NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

AMI-SEC
ASAP

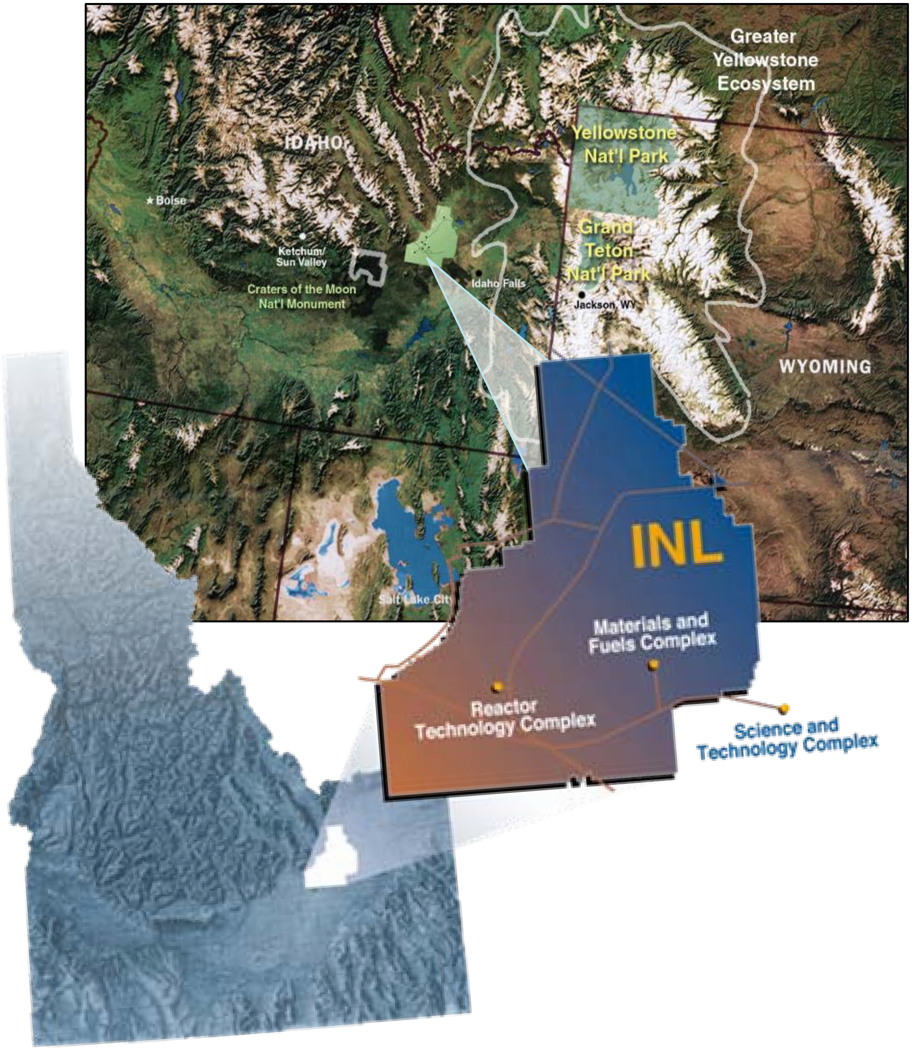
Gary Finco, Idaho National Laboratory

January 8, 2009

The Idaho National Laboratory

A DOE National Laboratory located in Idaho

- ***Facilities located in Idaho Falls and on the 890 square mile reservation located 40 miles away***
- ***Work force of 3,300 people ~ 7,000 total employees with all contractors***
- ***Historically focused on nuclear reactor research***
  - ***Operated by Battelle***



INL Idaho National Laboratory

SCADA/PCS Test Bed

Control Systems

- ***Multiple Vendor participation***
- ***Fully functional SCADA/EMS systems***
- ***Fully functional DCS and PCS systems***
- ***Inter-systems (ICCP) communication capability***
- ***Real world configuration capability***
- ***Remote testing capability***

Cyber Security Test Bed

An integral part of the SCADA/ Process Control Test Bed

- ***Supports control system security***
- ***Industry assessments***
- ***State of the art knowledge***

```
FILE*  fp;

foo=calloc(2048,1);

memset(foo, 'A', 2048);
bar=&foo[1024];
bar->prev_len=0xffffffff;
bar->next_len=0xfffffff0;
bar->prev_free=0xbfffff04;
bar->next_free=0xbfffff0f;

fp=fopen("exploit.bin", "w");
fwrite(foo, 2048, 1, fp);
fclose(fp);

return 0;
```

Next Generation Wireless Test Bed

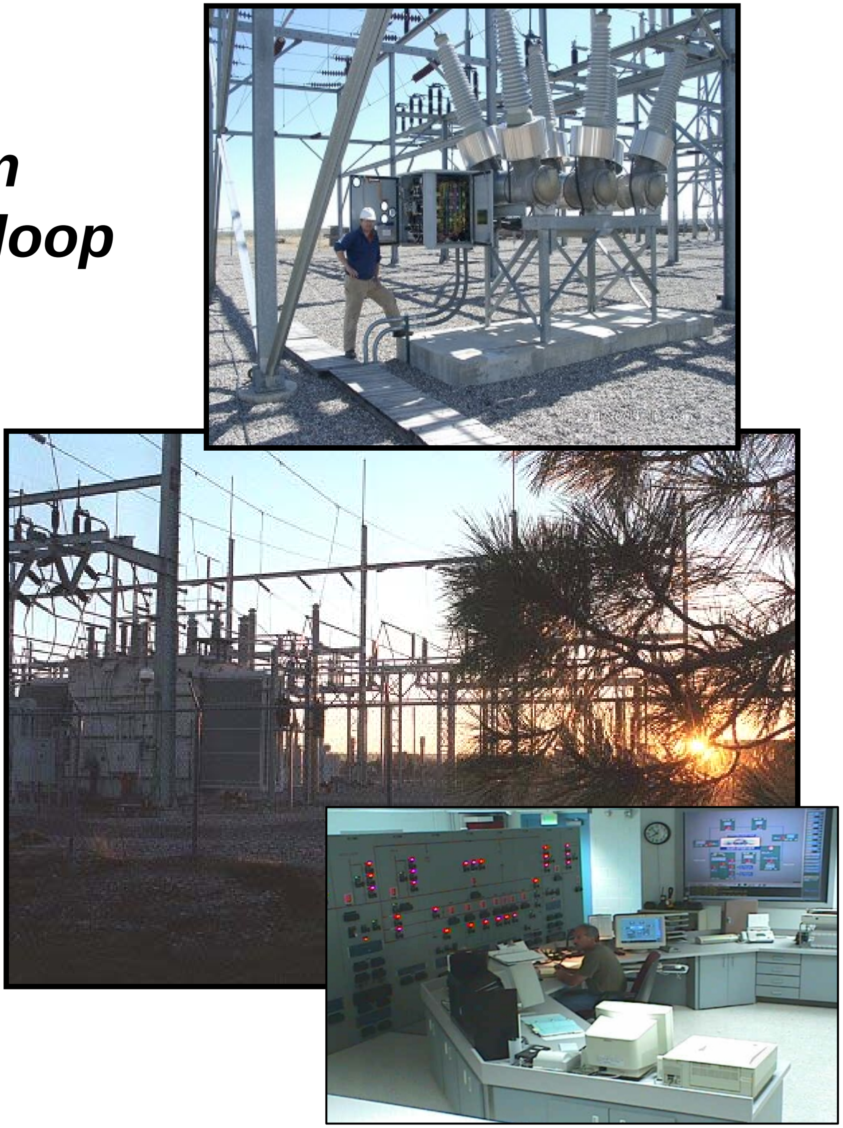
Operational since April 2003

- ***America's only "city sized" wireless test facility***
- ***9 Cell tower system operational; potential to expand***
- ***Testing next generation (3G/4G) wireless communication, wireless LANs and Land Mobile Radio systems***
- ***Access to commercial and government spectrums as NTIA experimental test station***
- ***Physically secure, interference free environment***
- ***Has supported IED jammer testing for USMC/Navy EOD***

Power Grid Test Bed

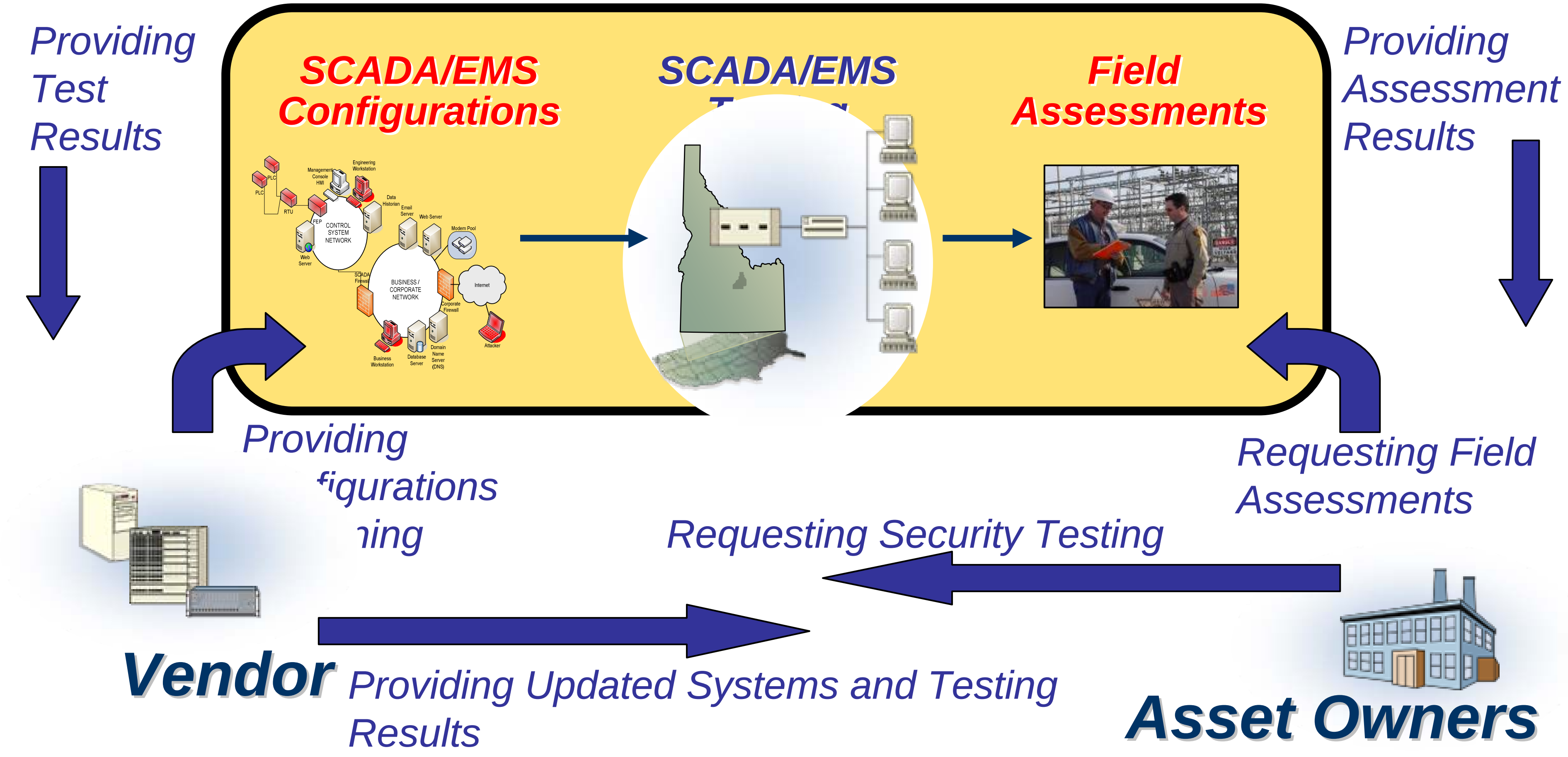
Various power grid test beds available:

- ***Secure power distribution system***
  - ***61 mi dual fed, 138kV power loop***
  - ***7 substations***
  - ***3 commercial feeds***
- ***Real-time grid monitoring and control through centralized SCADA operations center***
- ***Ability to isolate portions of grid for specialized testing***
- ***Protection & Restoration***
- ***Research***



Working Together to Deliver & Operate Secure Systems

National SCADA Test Bed



SCADA/EMS Configurations

SCADA/EMS

Field Assessments

Providing Test Results

Providing Assessment Results

Providing

figurations

ning

Requesting Field Assessments

Requesting Security Testing

Providing Updated Systems and Testing Results

Vendor

Asset Owners

Idaho National Laboratory

Purpose of the Tabletop analysis

The purpose of this document is to provide an overview of AMI component vendors, the products and services they provide, and an analysis of the pros and cons of the components features. The component focus is on the communications between the AMR meter and the utility or intermediate access point. The interest is in the type of communication, the data transferred, and the security measures employed to protect the transferred data. It is not intended to be all inclusive and there are many features and product details that are not addressed or included.

Tabletop analysis - Example

PRODUCT SPECIFICATIONS	Yes (Description)/No	Pro	Con
Has high reliability			
Uses standards	Yes C12.21 C12.22 GPRS TCP/IP, 900 MHz frequency hopping, 802.11S Zigbee,	Compatibility	
Remote meter reading	Yes	Ease of use, lower cost, and safety	Potential interception of meter data
Time stamping of the meter			
Real-time access to meter data	Yes	Ready access to current meter data to verify accuracy of billing, usage, and potential security breaches	Storage and bandwidth usage
15-minute data	Yes	Provide access to full-meter data and history for each 15-minute interval	Storage and bandwidth usage

Purpose of Procurement Language Document

The purpose of this document is to summarize security principles that should be considered when designing and procuring AMI systems products and services (software, meters, maintenance, and networks), and provide example language to incorporate into procurement specifications. The guidance is offered as a resource for informative use—it is not intended as a policy or standard.

Procurement Language Document - Example

Wireless Devices

Wireless communications allow connections to the AMI utility access points from the remote equipment (e.g. Meters and access points, pole top access).

Basis

Wireless communication is a cost effective method for building the AMI network infrastructure. Wireless technology provides communication from the meter to a local access point or pole top and then wireless or wired connections from the pole top will complete the AMI system communications.

Wireless communication signals are accessible to anyone in the world and are easy to discover via war dialing.

Language Guidance

AMI system equipment is installed with wireless devices enabled. Properly implementing wireless security settings (encryption, ….

Purpose of Recommended Testing Document

This document contains a list of tests and best practices that are recommended to be followed in order to fully test the wireless components of an AMI network implementation. They are not specific to any given wireless technology but are generic for wireless components that can be found in any wireless communications, regardless of the protocols or technology in use. For each specific wireless technology i.e. 802.11.x, ZigBee, Bluetooth, GSM, WiMax, etc. there may be other components and vulnerabilities that should be considered and tested. These are suggested starting points for any wireless network in order to provide for securing, installing and operating the wireless communication portion of an AMI system

Recommended Testing - Example

SPECIFIC TEST

Output power of transmitters
The AMI networks communications are designed with assumptions as to coverage and co channel interference which are based on several factors, including terrain, antenna gain and directionality and transmitter output power. For this reason, it is necessary to measure the output power of all transmitters.

Equipment
In order to measure the output power of the transmitters in all configurations, you will need a peak power meter with sensors that match the rated output power and the correct connectors that match the antenna port.