



INL provides large-scale, independent, end-to-end testing of next-generation communications infrastructure.



Idaho's Communication Test Bed

Our nation's reliance on wireless and Internet technology is rapidly evolving as more corporations are making wireless integration and convergence a top business priority. Similarly, military systems worldwide are rapidly embracing next-generation commercial technologies to accelerate network-centric capabilities and provide enhanced situational awareness.

While handheld devices such as laptops, Blackberrys, and cell phones once had limited mobility and range, they are rapidly incorporating new and multiple protocols such as Wi-Fi, broadband cellular (3G), and Bluetooth on a single platform to increase their effectiveness and agility.

Worldwide there is exponential growth in public Wi-Fi access points, and new wireless protocols such as WiMAX and 3G cellular continue to evolve and expand the range and speed of these devices. Additionally, critical infrastructure networks, previously isolated or connected with dedicated wireline circuits, are incorporating Zigbee for wireless sensor networks, wireless LANs for maintenance functions, and cellular or Internet based backhaul to manage control centers.

Yet with all the buildup surrounding wireless technology, few understand the complexities surrounding wireless protocols and security, the risks of converged network infrastructures, the

need for interoperability of communication systems, or mitigation measures to safely use and improve new technologies in both commercial and military environments.

Located on 890 square miles of federally owned and managed landscape, INL's communications test bed provides much cleaner frequency spectrum with little radio-frequency or background interference from urban congestion or military test sites. Over the last 50 years hundreds of millions of dollars in infrastructure has been placed at INL, allowing the laboratory to function like its own small city, or series of telecommunications and Internet service providers.

Continued next page

The Energy of Innovation



Continued from previous page

Securing Communications Systems

Building on INL's technical capabilities and critical infrastructure protection mission, INL engineers and researchers have the ability to perform vulnerability and risk assessments, tool development, and interdependency modeling and simulation for improving security while restricting access to proprietary data.

As a federal funded national laboratory, INL also works closely with customers from the departments of Defense, Energy and Homeland Security to define their testing needs for interoperability, standards verification, priority access signaling, and other critical infrastructure concerns. This cooperative effort provides wireless carriers, vendors and government agencies with "one-stop shopping" for an integrated test environment. Capabilities also exist to examine the interdependencies that exist between communications equipment and other critical infrastructure sectors such as electrical, Internet and computing, and manufacturing and industrial control systems.

INL is authorized by the National Telecommunications and Information Administration to operate as an experimental radio station. Combined with its geographic isolation, INL can test a wide variety of existing and emerging wireless systems with a view toward science or technology development.

Our test beds are enhanced by our technically experienced research and development, engineering, and critical infrastructure protection staff whose capabilities include telecommunications design, systems deployment and integration, simulation research, high-performance computing, cyber security and process control systems. The combined assets and expertise provide an ideal location for independent, real-world performance and vulnerability testing.

As the use of wireless and communications technology increases, new security protocols, independent verification and validation, interoperability testing, and tool development will be essential for supporting the long-term survivability of critical infrastructures, personal communications devices, and nationwide control networks.

Assets:

- Both lab and full-scale networks
- Two independent fiber loops (170 and 65 mile)
- Mountaintop RF facilities
- Ground-based towers and facilities
- Mobile trailers and towers
- Anechoic chamber and RF test labs
- RF propagation and network simulation

Services:

- Lab evaluation and testing
- Full-scale range testing
- Independent Validation & Verification
- Test plan/procedure development

- Range scenario/exercise development
- Vulnerability Assessments/Testing
- Performance, robustness, interoperability testing
- System integration
- Application/device testing

Technologies:

- Cellular test bed (multiple systems)
- Wireless Personal Area Networks (Bluetooth, Zigbee, etc.)
- Wireless Local Area Networks (Wi-Fi, 802.11)
- Wireless Metropolitan Area Networks (WiMAX)
- Voice over IP
- PSTN Simulators and SS7 Switches
- Wireless Local Loop
- Fiber Optic, SONET, ATM, DWDM
- Antenna Test Range
- Smart Antennas (software adaptable)
- Land Mobile Radio (Push to Talk)
- Radio Paging Networks
- Emergency responder operations/priority services
- Software-defined radios
- Variety of HF, VHF, UHF communications systems
- Point-to-Point and Point-to-Multipoint systems
- Analog and Digital Microwave
- Ad Hoc, Mesh, and Self Forming Networks
- Aerial Communications Links
- Satellite Systems
- NARDA RF safety certifications and measurements

For more information

Derek Hesse
(208) 526-9405
Derek.Hesse@inl.gov

Lynda Brighton
(208) 526-3908
Lynda.Brighton@inl.gov

**A U.S. Department of Energy
National Laboratory**

