



## Raising The Bar On Security In The Utility Industry

An Energy Department lab is testing software that could make it faster and easier for utilities to identify problems that could lead to outages.

By Martin J. Garvey, [InformationWeek](#)

Dec. 22, 2004

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=56200120>

Testing of new software planned to take place at a lab in Idaho could result in a leap in cybersecurity for the utility industry.

Founded in August, the U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory (INEEL) has as its mission testing systems that ultimately should help electric utilities and system operators across the country protect their infrastructure, operations, and apps from real-world and cyberenemies and hackers. Its technology mirrors real-world utility infrastructures, including [Scada](#) (Supervisory Control and Data Acquisition) systems, and wireless technology and processes.

ABB Ltd., a leading control systems and emergency-management system vendor in the utility industry, is an early participant in the INEEL tests. The vendor recently paid TecSys Development Inc.--whose ConsoleWorks central console-monitoring product gives customers a single view of IT systems, along with alarms and suggested processes to avert downtime and potential security problems--to support ABB's emergency-management software in its roster of supported products. Supported products include Cisco routers, HP's HP-UX operating system, and Oracle's relational database-management system.

When ABB's EMS is part of the ConsoleWorks roster, utility operators could attain a single console view of both the IT side of the house and the operational side. For example, a view of a change in a router could be the early warning of some intrusion. Following the deal between ABB and TecSys, INEEL has begun conducting some early tests of ConsoleWorks, while it awaits funding from Washington.

If the testing goes successfully, the bundled offering has important implications for the industry, says Jim Davidson, consultant technical specialist at INEEL. "From a central source we could monitor the beginning of an attack at the router or firewall level," says Davidson. "Ultimately, we'll test, but we can't certify anything, but we'll report back to utilities, vendors, and users for fixes. Our goal: Teach them how to be more secure."

An independent energy analyst is working this week to help the DOE in its quest to protect the U.S. industry from cyberattacks to the power grid. Joe Weiss, at Kema Inc., is documenting worldwide damage to utility-control systems. "The highest probability comes from viruses and worms, but next comes corporate IT installing the latest version of antivirus software," Weiss says. "Loading the latest version of antivirus software on HP-UX or Solaris could slow down the operation, thus shutting down multiple real-time control systems."



Copyright © 2004 [CMP Media LLC](#)