

## DOE, NIST aim to secure smart grid

Smarter electric grid brings security challenges along with the promise of a leaner, greener energy supply

- By [William Jackson](#)
- Jun 11, 2009

The smart grid that the Energy Department and electricity industry are building promises to be a more intelligent, more efficient system that will support a new generation of renewable energy sources. But it will also bring new challenges in ensuring the security of the grid itself and the information systems that will connect with it and control it.

"To be clear, the smart grid is both a means to enhancing grid security as well as a potential vulnerability," Patricia Hoffman, acting assistant secretary at DOE's Office of Electricity Delivery and Energy Reliability, recently told a Senate panel.

Engineers and regulators have an opportunity to ensure that developers standardize security in the new infrastructure from the beginning, which would make the grid not only smarter but also more secure than the aging system the country now uses.

Because the reliability of the nation's electrical power supply is a matter of national security, Congress is working to establish proper oversight of the grid's cybersecurity while DOE and the National Institute of Standards and Technology hammer out technical standards and specifications.

The House and Senate are considering bills that would define the roles of agencies, including the Homeland Security Department and the Federal Energy Regulatory Commission (FERC), in evaluating threats and vulnerabilities to the grid's information technology systems and enforcing security requirements. Differences between the bills include DHS' role in protecting the electricity infrastructure and how quickly regulators would be able to mandate responses to emerging threats. Rep. Bennie Thompson (D-Miss.), chairman of the Homeland Security Committee, sponsored one of the bills and said he expects to see action on them this year.

"I am absolutely convinced that, at the end of the debate, everyone will be on the same sheet of music," Thompson said. "Our goal is to complete it during our legislative calendar this year."

Meanwhile, NIST is defining the technical standards for grid interoperability and security, with research and development support and \$10 million from DOE. NIST must work quickly to create those standards because the American Recovery and Reinvestment Act provides \$4.5 billion for smart-grid R&D, and vendors are eager to start working on smart-grid technologies.

In May, NIST identified an initial batch of 16 existing technical standards for the interoperability and security of control systems. The agency's work is the first step in a three-phase program to develop key technical standards for an intelligent power distribution grid by the end of the year.

"We are working with a sense of urgency to expedite the development of standards critical to ensuring a reliable and robust smart grid," NIST Deputy Director Patrick Gallagher said.

In cooperation with utilities, equipment suppliers, consumers and standards organizations, NIST plans to further refine the list of existing standards for the smart grid, then develop the remaining standards needed to fill in gaps, and finally develop a program for testing and certification to ensure that smart-grid equipment and systems comply with the standards.

The smart-grid program was established under the Energy Independence and Security Act of 2007. It aims to use intelligent networking and automation to better control the flow and delivery of electricity to consumers. DOE, which is the overall lead for the program, called it "a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between."

The act gave NIST the job of developing a framework of standards and protocols to ensure interoperability and security. Final standards will be approved by FERC, which has regulatory authority over the interstate industry under the Energy Policy Act of 2005.

The Obama administration has identified the smart-grid program as an important element of the economic recovery program because of its potential for creating jobs, contributing to energy independence and curbing greenhouse gas emissions.

Furthermore, bringing new technology into the power distribution system is necessary to improve efficiency and reliability and enable the incorporation of new sources of power, said Katherine Hamilton, president of the industry group GridWise Alliance.

"The smart grid is a means, not an end in itself," Hamilton said. "We don't care what the technology is, we just want a smarter grid for the public good."

A more reliable system is needed that can respond to and recover quickly from problems, such as the power outage that darkened a large portion of the northeastern United States in 2003. "It took them a year to figure out how it happened," Hamilton said. That inability to respond to disruptions in near real time could put the country's security at risk.

In addition to being more resilient and reliable, power systems must become more efficient. Power generation and transmission facilities are built to accommodate peak demand plus 15 percent. "Most of the time, about 50 percent of the capacity is not being used," Hamilton said. "It's just sitting there."

Bringing renewable power sources, such as solar and wind, into the current system might not help much and could make the situation worse. They are fundamentally different from traditional energy sources — such as coal, gas, nuclear power and hydroelectricity — because they are more variable and difficult to control.

"You can't have all of that power just coming online," she said. "Utilities have to be able to get it on their lines and dispatch it when they need it." That will require greater real-time visibility into the system and more refined control over it.

Supply and demand must be balanced across the system, which is not a new idea. "The mechanics have been there forever," Hamilton said. "The issue now is how do you automate it and get more information?"

The technology is already emerging. One tool, a wide area measurement system (WAMS), uses detailed measurements of voltages in the power grid, Hoffman told the Senate Energy and Natural Resources Committee.

"The data is synchronized with timing signals from Global Positioning System satellites," Hoffman said. "The real-time information available from WAMS allows operators to detect and mitigate a disturbance before it can spread and enables greater utilization of the grid by operating closer to its limits while maintaining reliability."

On the customer side, Powerit Solutions, of Seattle, provides intelligent demand-control systems for industrial users.

Potential savings draw customers to Powerit Solutions' energy control systems, said Bob Zak, the company's president. Industrial users consume 28 percent of the country's electricity, which offers opportunities for savings, he added. Industrial users are charged a surcharge for peak energy use.

"That demand charge can contribute 30 percent of the total energy bill," Zak said.

By monitoring total power use at the meter level and analyzing how individual systems and devices use that power, the automated system can spot peaks approaching. The system's algorithms can make decisions about the most efficient way to reduce consumption and smooth the flow without interrupting critical processes.

"The challenge is how to reduce the consumption in response to changes in the grid without killing the business," Zak said. "There are limitations on how far you can drive this down. We are not eliminating the peaks entirely. There will always be moments of highest usage."

But the technology is good enough at predicting peaks and controlling use by individual systems to reduce surcharges for peak demand by 10 percent to 40 percent, which can yield savings of as much as 12 percent on an organization's electricity bill, he said.

However, incorporating automation across a nationwide grid — from the generator to the consumer — is a daunting task. A primary requirement is interoperability standards.

In March, NIST named George Arnold, the agency's deputy director of technology services, to be director of smart-grid activities. Arnold, who formerly worked for Bell Laboratories and was chairman of the American National Standards Institute, said the

aggressive timeline for producing a suite of technical standards by year's end is doable because much of the work has already been done. NIST's job will be to prioritize needs and identify existing standards to meet them, he added.

In the first phase of the program, NIST awarded a \$1.3 million contract to the Electric Power Research Institute, of Palo Alto, Calif., to help develop an interim report on a smart-grid architecture and standards road map. Officials expect the interim road map to be ready this summer.

In the meantime, Hoffman said DOE has been working with industry for several years to improve the cybersecurity of the existing grid. Specifically, DOE has:

- Identified cyber vulnerabilities in energy control systems and helped harden systems to mitigate the risks.
- Developed more secure means of communications between field devices and control systems.
- Created tools to help utilities assess their security posture.
- Developed modeling and simulation tools to estimate the effects of cyberattacks on the power grid.
- Provided training for industry to help defend against cyberattacks.

In 2005, DOE began working with DHS and the Canadian government to create a security road map for North America's power systems.

"The road map vision states that in 10 years, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function," Hoffman told the Senate committee.

Through its national laboratories, DOE is working with industry groups and universities to develop cybersecurity tools to meet that goal. Its test bed is assessing supervisory control and data acquisition and energy management systems for the electric, oil and gas industries and has produced 11 hardened control-system designs now being deployed. Another DOE effort is the development of security audit files that can be incorporated into network-scanning tools to assess the security settings of control systems against optimal configurations.

"Given that large control systems can have over 1,000 security settings, [that approach] can help a utility enhance its security posture while saving time and money," Hoffman said.

But the regulatory framework for power grid security is far from adequate, a FERC official said.

Although FERC has the authority to regulate grid security, "the commission does not have sufficient authority to provide effective protection for the grid against cyberattacks or other security threats to reliability," said Joseph McClelland, director of FERC's Office of Electric Reliability.

McClelland told the Senate Energy and Natural Resources Committee that the standards-setting process for electric grid security is cumbersome and time-consuming, that FERC has no authority over the content of the standards it enforces, and that it lacks the ability to protect sensitive information. Furthermore, FERC has authority only over the bulk power system in the lower 48 states, which excludes Alaska and Hawaii, and it does not cover distribution systems in many major metropolitan areas, such as New York, that are not part of the bulk power system.

Part of the problem is that the Energy Policy Act splits the development and enforcement of security standards into two jobs. The North American Electric Reliability Corp. (NERC) creates the standards that FERC enforces. The standards are developed in cooperation with industry and other stakeholders, with plenty of time for public comment.

"Although inclusive, the process is relatively slow, cumbersome and unpredictable," McClelland said.

FERC cannot alter or mandate security standards, although it can reject them and send them back to NERC for changes, which could add years to the process. McClelland said the first set of NERC standards, which FERC approved in 2008, are too lax and leave too much discretion to industry. The standards require companies to protect only critical cyber assets, and companies can identify those assets. Only 27 percent of electric utilities have identified their systems as having critical cyber assets, so the security requirements do not apply to nearly three-quarters of companies.

Strengthening the standards could take years under the current system, McClelland said. "It is not clear, even today, what percentage of critical assets and their associated critical cyber assets has been identified," he said. "It is clear, however, that this issue is serious and represents a significant gap in cybersecurity protection."

Strengthening the role of FERC in protecting the electric grid from cyberattack is one of the goals of the Critical Electric Infrastructure Protection Act (H.R. 2195), which Thompson introduced in April.

"This is another step not just in identifying vulnerabilities but in taking the necessary steps to correct them," Thompson said. FERC now can only suggest that generators and grid operators take immediate steps to enhance cybersecurity. "Our bill will give them the authority to require it. They will have the responsibility of seeing that security issues are corrected."

Thompson's bill has been referred to the Homeland Security Committee and the Energy and Commerce Committee, where a similar bill is pending — H.R. 2165, the Bulk Power System Protection Act of 2009, introduced by Rep. John Barrow (D-Ga.).

"We both agree that FERC is the entity that should have responsibility of securing" the grid, Thompson said. But in addition to giving FERC more immediate authority, his bill also would give DHS a leadership role in evaluating threats.

Furthermore, Thompson's bill would:

- Give FERC the authority to issue emergency orders to owners and operators of the electric grid after receiving information from DHS about a credible cyberattack.
- Require FERC to establish interim measures to protect against known cyber threats to critical electric infrastructure components in addition to existing mandatory standards.
- Require DHS to perform ongoing assessments of the cybersecurity vulnerability and threats to the critical electric infrastructure and provide recommendations for mitigating them.
- Require DHS to determine if outsiders have compromised the security of the federally owned critical electric infrastructure.

#### About the Author

William Jackson is a senior writer for GCN.



© 1996-2009 1105 Media, Inc. All Rights Reserved.