U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

Cyber Security: A Top Smart Grid Priority for America's Electric Cooperatives

The Cyber Security Challenge

Those organizations investing in smart grid technologies, tools, and techniques face a significant challenge: the very act of installing information and communications systems could provide access to hackers and cyber terrorists. These bad actors could retrieve unauthorized data, damage equipment, or shut down segments of the electric grid. To address such attacks, the U.S. Department of Energy (DOE) requires that every smart grid project supported by the American Recovery and Reinvestment Act of 2009 submit a comprehensive cyber security plan. The project must receive DOE approval of this cyber security plan before implementing new smart grid systems. In their Smart Grid Demonstration Project, "Enhanced Demand and Distribution Management," the National Rural Electric Cooperative Association (NRECA) and their Cooperative Research Network (CRN) have taken on the cyber security challenge.

Cyber security for smart grid projects has never before been addressed in a systematic way. Implementing these new technologies, tools, and techniques safely calls for "how-to" manuals that provide step-by-step directions for addressing vulnerabilities and protecting components and systems from deliberate attacks or user errors. The need is especially challenging for electric cooperatives that have relatively small staffs and little cyber security expertise. In recognition of this need, the NRECA-CRN cyber security team has developed tools for power companies to make their smart grids more secure—and these tools are available today.

The NRECA-CRN Smart Grid Demonstration Project

NRECA is a trade association serving the collective interests of the nation's electric rural cooperatives and their consumers. CRN is the research arm of NRECA. The NRECA-CRN Smart Grid Demonstration Project

involves 24 of member rural cooperatives who are members of NRECA, reaching across 12 states, and approximately 729,000 consumers. The project is replacing aging equipment with state-of-the-art devices

to help keep electric service reliable, affordable and secure. Mark Stallons, President and CEO of Owen Electric Cooperative, a participating rural cooperative in Owenton, Kentucky, says, "We expect to need additional power plants and transmission in our region sometime during the next five years. [These upgrades] should help delay those decisions by reducing demand."

Drivers for Cyber Security

When DOE issued the announcement in June 2009 that they would fund selected smart grid projects, the Department specified certain cyber security requirements. At that time, some cyber security guidance was available from the North American Electric Reliability Corporation, and since then further guidance has been issued by the National Institute of Standards and Technology. In trying to address the DOE requirements, the NRECA-CRN project team met with each participating cooperative to determine how to translate that guidance to suit the various cooperatives' particular needs. "This guidance is fine, but can you provide something more appropriate for electric distribution? And written in plain English for our engineers to implement?" was the general response from the participating rural cooperatives, according to Craig Miller, NRECA-CRN's project manager.

NRECA-CRN Cyber Security Tools

So Craig and his team went to work and produced a cyber security guidance manual and supporting templates. These cyber security guidance tools are among the first of their kind. The manual and supporting templates start with a broad perspective, asking questions about management oversight for cyber security, and then take users through a series of structured inquiries about the details associated with specific components such as smart meters and distribution automation equipment.

The NRECA-CRN project involves more than 250,000 smart grid components. Demand management devices for the project include smart meters, in-home displays, thermal storage

NRECA-CRN Smart Grid Demonstration Project: Facts and Figures

- Total budget: $67,864,292
- Federal Share: $33,932,146

- 229,214 smart meters
- 15,600 load control switches
- 6,333 in-home displays, web portals
- 611 smart feeder switching components
- 334 conservation voltage reduction devices
- 166 advanced volt/VAR controllers
- 160 thermal storage devices
- 22 SCADA systems and components
- 3 meter data management systems

devices, and a communications infrastructure that incorporates meter data management systems

and wireless towers. This equipment helps consumers to better manage their bills and keep their electricity affordable. Distribution automation devices for the project include smart feeder switches, conservation voltage regulators, volt/VAR controllers, and advanced SCADA systems. This equipment enables power companies to identify faults quicker and speed restoration times following outages, improving the reliability of electric service.

In procuring these components, the NRECA-CRN team provided their vendors with a list of cyber security questions about the protections built into the equipment. The NRECA-CRN team was surprised by the wide range of responses, which highlighted the newness of cyber security requirements in the electric power industry. Ms. Robbin Christianson, Director of NRECA-CRN Program Operations and Business Management, notes, "Some of the vendors clearly understood the requirements and had appropriate responses about the safeguards in place, while others seemed unclear about the questions and provided little or no response." Clearly, cyber security tools were needed to overcome a lack of experience and expertise and move vendors and power company engineers up the learning curve as rapidly as possible.

Putting the Tools to Use

On May ??, NRECA-CRN announced the release of their cyber security tools along with plans to make them available: [link to announcement]. In keeping with NRECA-CRN's knowledge-sharing mission, all rural cooperatives will have access to these tools, as will any power company who agrees to share how they have used and/or improved upon the materials. NRECA-CRN's Executive Director, Ed Torrero, points out, "These materials mark the first broad approach to advancing cyber security at the distribution level, and participating rural cooperatives and others have the opportunity to use these tools to fit their local situations, boost their security posture, and meet evolving federal and industry standards." Reflecting on the widespread interest in cyber security for the smarter grid, Mr. Torrero adds, "In addition to requests for assistance from investor-owned utilities and municipal electric systems in the U.S., we have taken calls from administrators in England, Italy, and India."

With these tools and others like them, power companies can pose common questions to vendors about the cyber security of their equipment. As a result, Ms. Christianson hopes, "They'll all get it," and the market will respond accordingly. The ultimate aim is to have appropriate cyber protections built into equipment design from the start, making the smart grid more secure in the most cost effective manner possible.

Other Lessons Learned from the NRECA-CRN Project

The planning stage for the NRECA-CRN project is nearing completion, yet the project already reports rapid progress on implementation. In April and May of this year, about $14 million is being spent on equipment purchases and installations, and the NRECA-CRN team expects nearly all the project's smart grid components to have been purchased and installed by the end of 2011.

The NRECA-CRN project is demonstrating the value of spending time on proper planning. The team's strategy is to have communications hardware and data management software in place before equipment is purchased so that, after installation, the components will be ready for immediate use. This preparation is essential, according to Mr. Miller, because "smart grid systems generate tens of thousands more bits of data than conventional systems. Without in-place and operating communications and data handling systems, rural cooperatives would be overwhelmed with the volume of data and probably would need to implement costly engineering solutions just at the point when the equipment needs to be working and performing needed smart grid functions."

The project team's approach is showing the advantages of careful planning and just-in-time implementation strategies. Moreover, the cyber security advancements produced by NRECA-CRN raise the bar for other DOE smart grid project recipients and provide potential solutions for them and the rest of the electric power industry. DOE looks forward to further contributions from the NRECA-CRN project.

Learn More

The American Recovery and Reinvestment Act of 2009 provided DOE with $4.5 billion to fund projects that modernize the Nation's electricity infrastructure. For more information visit www.smartgrid.gov or www.oe.energy.gov. There are five recent reports available for download:

- *Smart Grid Investment Grant Progress Report*, July 2012
- *Demand Reductions from the Application of Advanced Metering Infrastructure, Time-Based Rates, and Customer Systems – Initial Results*, December 2012
- *Operations and Maintenance Savings from the Application of Advanced Metering Infrastructure – Initial Results*, December 2012
- *Reliability Improvements from the Application of Distribution Automation Technologies and Systems – Initial Results*, December 2012
- *Application of Automated Controls for Voltage and Reactive Power Management – Initial Results*, December 2012