By Peter M. Curtis

Peter Curtis is the president of Power Management Concepts, LLC, in Woodbury, NY, and an associate professor at New York Institute of Technology.

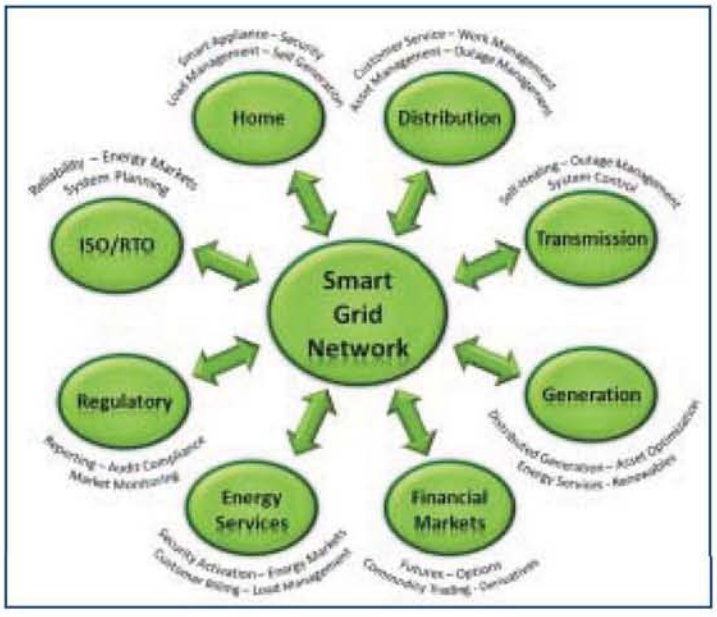
A Phased Approach to Smart Grid Technology

Improving energy security, efficiency, and reliability by planning

Over the coming months facility managers will be finalizing their energy, operation/maintenance, and construction budgets. Perhaps this is a good time to include a budget line item for a Smart Grid pilot project and reap the benefits of energy security, efficiency, and reliability, all leading to financial savings and environmental stewardship.

As we know, recently there has been considerable discussion, debate, and deliberation about the Smart Grid—the convergence of digital and power distribution technologies. Many experts believe that the use of automation, communication, and computers will improve the production, distribution, and consumption of electricity, with the by-product being improved reliability and efficiency. The Department of Energy's Office of Electricity Delivery and Energy Reliability is heading this effort to modernize our nation's electric grid. The office has created a Smart Grid Task Force responsible for coordinating standards development, research, and energy policy programs.

Our electric infrastructure was designed and built before we developed modern power distribution standards. Essentially, the Smart Grid will be a vast network that will join millions of new devices with the trillions already connected to the Web in order to meet our need for energy security, reliability, and efficiency. End users will be able to better monitor and control their energy use as well as sell excess electricity generated by their own renewable resources.



Smart Meters are state-of-the-art electric meters that let energy consumers monitor and reduce energy use, which will in turn increase reliability and encourage energy efficiency by facilitating smarter end-user technologies. Millions of dollars are being allocated for smart meters in utility capital budgets, and the House of Representatives has approved federal funds to help implement and expand the programs. Some utilities have already taken the first steps by launching Smart Metering pilot programs.

Envisioned Smart Grid technologies include:

- Smart electrical devices that report electricity consumption and implement usage policies.
- Advanced control systems used by utilities to analyze and manage the grid, allowing them to offer flexible rates that vary depending on the time of use or times when available capacity exceeds demand. Consumers may also use some of these control systems to view and adjust electricity usage.
- A two-way communication network that connects the smart devices and the users to the control systems. One example is the Automated Metering and Information System (AMIS) developed by Siemens. AMIS registers the rate of electricity consumption of each individual utility customer and sends detailed data to both the utility and the user.

The transformation to a digitally based electric distribution and transmission system will need to address added security risks. Some types of smart meters and other points in the Smart Grid's communications system can be hacked, which increases the risk of massive blackouts.

The utility industry recognizes that a hacker armed with as little as $500 worth of computer equipment and a background in electronics and software engineering can exploit these vulnerabilities. Furthermore, recent reports state that spies have been mapping the U.S. utility infrastructure and hacking into its computers, planting software that could

Continued from page xx

be used to disrupt it. Another recent incident that points to the vulnerability of critical infrastructures is the cutting of communication lines in Silicon Valley that disabled phones and internet connections.

It is impossible to police millions of miles of electrical cables, so intelligent systems will be vital for monitoring and securing the Smart Grid.

It is impossible to police millions of miles of electrical cables, so intelligent systems will be vital for monitoring and securing the Smart Grid. Some experts say that implementing a grid that can sense what is happening within it will enable system operators to know when someone is trying to tamper with it. Automation will allow the grid to self-heal by automatically bypassing failures to continue to supply power to consumers. This would make the grid more resilient to both deliberate attacks and natural disasters.

Mother Nature must also be considered. For example, periods of high sunspot activity produce a "solar wind," which is the spray of atomic nuclei, electrons, and other particles that blow off the sun's surface at about 1 million miles per hour. The intensity and frequency of these solar storms peak approximately every 11 years. Larger magnetic storms can disrupt satellites, induce currents in transmission lines that can melt transformers, and disrupt communications on the Earth's surface. On March 13th, 1989, solar flares knocked out 21,500 megawatts of electrical power in Quebec, Canada, leaving 6 million people in the dark. That night, temperatures were as low as 19°F. In the worst-case, these same storms could cause cascading failures that might affect close to 300 million people in the United States alone.

We are obviously on the threshold of another major technology revolution, and the mission critical industry must be prepared to take full advantage. To do this, our facilities must be made Smart Grid ready. The time is now to start budgeting for pilot projects and the installation of the necessary infrastructure. Building a robust and secure Smart Grid will be a monumental challenge, and in reality it may take decades for it to evolve. ■