Smart Grid security a growing concern

Because the grid is 'smarter,' it's also more vulnerable to attacks

By Richard L. Nailen, *EA* Engineering Editor

As electric utility systems become "smarter," they are also becoming increasingly vulnerable to disruptive attacks. Communication and interaction are the essentials of Smart Grid operations. Monitoring and control of system demand; control of substation facilities; energy interchange between utilities; loading of generating stations—all these functions must contribute to enhanced system reliability and efficiency. Each of them relies on high-speed electronic transmission of data between multiple locations. (See Figure 1, below.)

Unfortunately, as credit card and Internet users are learning all too well, the transmission of this data invites the attention of hackers

Unfortunately, as credit card and Internet users are learning all too well, the transmission of this data invites the attention of hackers with a variety of motives to access and "game" the system. Widespread changes in utility structure, separating generation from transmission and distribution functions, have introduced new complications. (See Figure 2, next page.)

Cybersecurity has therefore become a prime concern for utility management. Residential electric customers are also among those worried about unauthorized access to,

Please turn to next page

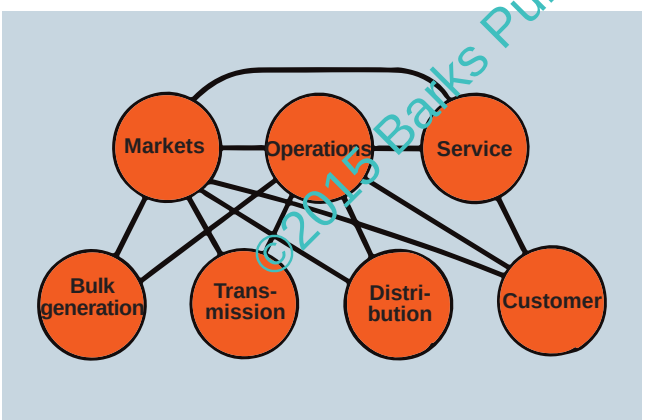

Figure 1. Communication and control linkages are crucial to electric utility operations.

SMART GRID continued from previous page

and tampering with, the information flow between their Smart Meters and the utility. In 2010, the U.S. Dept. of Energy announced a $30 million investment to "address cyber security issues" facing the domestic grid. Hacking the Smart Grid command and control network was then being seen globally as "the preferred method of future terrorist attacks."

As John McDonald of GE Energy Management has pointed out, grid communications years ago involved only "point-to-point" proprietary systems, so that an outsider break-in was confined to one section. New installations, however, "have moved to network communications . . . using industry standard communications protocols" instead of proprietary links. Hackers now can cause widespread disruption.

Many ways of dealing with this threat are being investigated. Although everyone agrees on the need, no universal solution has yet appeared. Security experts are looking for "encryption and cryptographic hashes," "more efficient algorithms," and "stronger access controls." "Security patches" must be "tested under field conditions and deployed as quickly as possible to prevent and detect the introduction and propagation of malware." Internet experience has shown that as new viruses or other unwanted network disruptions are discovered and blocked, others soon take their places. In 2013, an antivirus service provider reported that in the previous year "new malware sample discoveries had increased 50%."

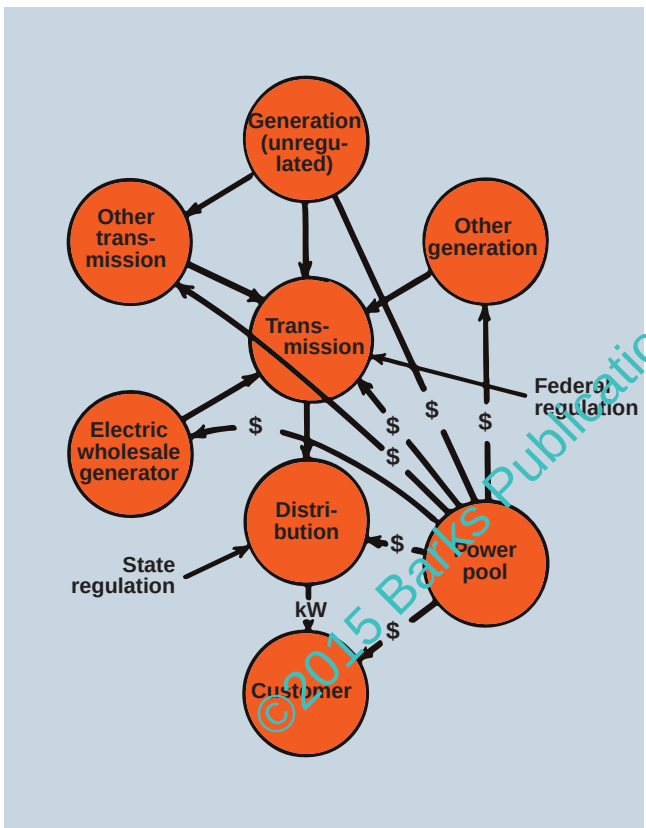

Figure 2. The once-simple model of a utility as one organization linking generation, transmission, and distribution has become far more complex, calling for additional layers of reliable communication.

A Google search for "grid cyber security" recently yielded nearly two million hits. International conferences on the subject have been held for several years in such widely separated locations as Germany and Singapore. A typical gathering in Amsterdam in January 2014 dealt with "End-to-End Cyber Security for the Smart Grid." Subjects covered included Emerging Hacker Trends, Security Architecture, SCADA Security, Standards Development, European Regulatory Landscapes, Critical Communications Security, and Control Center Security. The fifth "European Smart Grid Cyber Security" conference was held March 9-10 in London.

As if natural disasters like ice storms and hurricanes weren't enough, the rising price of copper has made utility service centers and substations increasingly attractive to copper thieves

According to a publication of the National Electrical Manufacturers Association, a break in the data transmission and control network not only risks utility service interruptions but also forces utility operators and equipment manufacturers to search for software and hardware patches than can heal the breach. Just sending out a line crew to put up a new pole, or string a new line, isn't a solution.

Besides the R&D time to find and fix problems, making such patches effective involves potential changes to the manufacturing process, product recalls, rebates, and possible lawsuits, as well as the public relations black eye (utilities don't need any more of those). And since the Smart Grid concept involves coordination between utilities that may be direct competitors, a common approach is essential for both the utilities and their state regulators.

Passed by the U.S. House of Representatives last year was the National Cybersecurity and Critical Infrastructure Protection Act of 2014, to amend the 2002 Homeland Security Act to deal with any cyber incident that "would jeopardize . . . the security, integrity, confidentiality, or availability of an information system or network . . . or any information stored on, processed on, or transiting such a system or network. . . ." Like much other legislative action during that election year, it languished in a Senate committee.

Utilities are confronted by other security threats as well. As if natural disasters like ice storms and hurricanes weren't enough, the rising price of copper has made utility service centers and substations increasingly attractive to copper thieves. Their periodic electrocution upon encountering a live circuit only adds to the problem. Equipment damage and area blackouts are a headache for system operators.

Vandals with other motives can cause even more damage, highlighted in 2013 by a 20-minute attack on a major utility substation in California. Unknown attackers using high-powered rifles fired on the 500 kV facility, knocking out 17 transformers by puncturing their tank walls so the oil coolant drained away. Repairs took a month. Just outside the station perimeter, the attackers were able to cut fiber optic cables to disrupt area cell phone and other telecom services. Similar attacks have occurred elsewhere in California and in Texas, Utah, and Arizona.

Any major disruption of electric service has always been costly for a utility, both financially and in public relations. As the Smart Grid is being advertised as a major improvement in grid efficiency and reliability, keeping it secure will be a greater challenge than ever before. **EA**