

[**Richard Schlesinger**](https://www.energycentral.com/member/profile/55798)

Principal, Alpine Communications

**Protecting The Grid**



* Posted on February 27, 2018

* 376 views

* [start a discussion](https://www.energycentral.com/c/iu/protecting-grid#comment-form)

* [report](https://www.energycentral.com/user/login)

* follow

The electric grid is arguably the biggest machine in the world, the greatest engineering feat of the past hundred years, with over 200,000 miles of high-voltage transmission lines, more than 55,000 substations and 5.5 million miles of local distribution cables.  It’s one of those human accomplishments so successful as to become virtually invisible.  But, the grid today is hardly the grid that Thomas Edison envisioned when he launched the first one, the Pearl Street Station, in 1882 in lower Manhattan; vastly larger and infinitely more complex, it’s the product of constant evolution.  And the very structure of the grid is evolving; while for the most part it still distributes power from central sources to end-users within a certain locale, it is increasingly incorporating local nodes of distributed generation incorporating interruptible renewable sources, some local, others centrally located.  As the grid evolves, so, too, do the threats to which it is vulnerable.

Because of its vast physical structure, the grid is an obvious target for physical attack for everyone from criminals to foreign terrorists to say nothing of its vulnerability to natural disasters.  Because it is so widely dispersed, often in unpopulated and isolated places, physically protecting all of its assets is prohibitively expensive and logistically extremely difficult.  Still, comparing the industry’s response to Hurricane Matthew in 2017, versus its response to Hurricane Sandy in 2012, indicates how far the industry has come in preparing for inevitable natural disasters.  One example: Florida Power & Light personnel assisting Consolidated Edison discovered the importance of flood monitors at substations.  FP&L used that technique in 2017 when Hurricane Matthew hit to assess when to de-energize substations, which helped minimize damage and speed restoration of service.  Another crucial lesson was the importance of developing a framework in advance of disaster for coordinating the efforts by state and local authorities to expedite the movement of crews and equipment both in “pass through” states and in the immediate vicinity of storm damage.

But while natural disasters, to say nothing of squirrels, will always pose a threat to the integrity of the grid, the most serious threat today is probably its vulnerability to cyberattack.  That became frighteningly obvious in December, 2015, when grid control operators in Ukraine watched as their cursors moved independently across their screens and took about 30 substations offline.  Almost a quarter-million people lost power; even the operators were suddenly left in the dark as hackers shut down their uninterruptible power supplies.  It was a carefully planned attack after months of study by the hackers of the infrastructure and of the operators’ credentials.  Whether the culprit was Russia, as Ukraine has alleged, or another party, it was very well planned and well funded and probably involved a number of different units.

The stability of the grid, especially in this age of renewable and distributed generation, depends increasingly on its interconnectivity, and that interconnectivity is achieved through a vast network of computer devices and controls.  This proliferation of internet connected nodes creates almost endless opportunities to penetrate to the heart of the grid.  Thus, while there have been significant efforts to protect the center of the grid, with security standards at generating and major distribution centers, the periphery has received much less attention.  And that periphery is almost infinite, because it includes virtually every point where the “internet of things” connects with the distribution system.    Every smart meter, every internet-connected television, refrigerator and thermostat and each Siri- or Alexa-enabled device, becomes a possible entry point where sinister forces can penetrate from the periphery to the very center of the grid.  In other words, there is a very weak layer of protection between the critical infrastructure providers and their own customers.

Furthermore, there is often a weak layer of protection within the central facilities themselves.  Control of central facilities used to be through manual and electrical equipment, with individuals, watching meters, charged with physically throwing the right switches to respond to fluctuations in the supply and demand for electricity.  These functions, literally in the hands of highly trained and experienced workers, are increasingly being performed through devices with IP addresses and even automatically by computers driven by sophisticated algorithms.  Without serious barriers between networks and the components of those networks, there are almost infinite opportunities to penetrate, with malicious intent,  from the perimeter to the center of the system, with possibly catastrophic results.

Concern about the vulnerability of the grid to cyberattack is not new.  Former CIA Director James Woolsey has been warning about it for years.  DARPA, the Defense Advanced Research Projects Agency, has been working on how to thwart a cyber attack, although Woolsey and others have also warned that the grid is vulnerable to an atmospheric nuclear explosion, which would cause a high-magnitude, short duration pulse that would cripple the grid.  But these DARPA studies, which won’t be complete until 2020, focus on massive, centrally planned attacks.  The threat of attackers entering through the widely dispersed internet of things is far more difficult to address.  A number of government agencies, including  the Energy Department, the Homeland Security Department and FERC, are addressing the broad issue of cybersecurity through at least 27 separate programs.  But it will take more than just government rules and regulation.  Protecting the grid has become a crucial issue that requires broad cooperation among federal, state and local governments and the many individual private and public entities of which it is composed.  It’s a daunting task, but one that we ignore at our very real peril.