2015 September 10

Written testimony from Prof. M. Granger Morgan prepared for the 2015 September 10 hearing on "Examining the Vulnerabilities of America's Power Supply" before the Committee on Science, Space and Technology Subcommittee on Oversight and Subcommittee on Energy of the U.S. House of Representatives.

Thank you for the opportunity to provide my thoughts on this important topic.

I hold the position of Hamerschlag University Professor of Engineering at Carnegie Mellon University where I have appointments in three different academic units:

- The Department of Engineering and Public Policy
- The Department of Electrical and Computer Engineering
- The H. John Heinz III College.

At Carnegie Mellon I co-direct, with Professor Jay Apt, our Electricity Industry Center (see: www.cmu.edu/electricity). I am a member of the Advisory Board for the DoE Office of Electricity. Last month I rotated off of the council of the Electric Power Research Institute (EPRI) on which I have served three times and chaired for several years. As a member of the National Academy of Sciences I served as chair of the National Academies' study *Terrorism and the Electric Power Delivery System* (NRC, 2012). Since the publication of that report I have also organized and chaired two meetings on issues of power system resilience at the National Academies. Video recordings of both of these two-day events are available on line:

- Workshop run by the NRC Board on Energy and Environmental Systems on the Resiliency of the Electric Power Delivery System in Response to Terrorism and Natural Disasters. See: http://sites.nationalacademies.org/deps/BEES/DEPS_081081
- Expert meeting run by the NRC Resilient America Round Table on Improving Power System Resilience in the 21st Century. See: http://sites.nationalacademies.org/PGA/ResilientAmerica/PGA_146736

At the Academies I serve as co-chair of the Resilient America Round Table (See: http://sites.nationalacademies.org/PGA/RESILIENTAMERICA/). I am a Fellow of the IEEE, of the Society for Risk Analysis and of the AAAS.

Unlike food and water, none of us consume electricity directly. Rather, we consume the services that electricity makes possible. Those services have become ever more critical to the safe, effective and productive functioning of our lives as individuals, to our society, and hence also to our national security.

Most of the blackouts we experience are not the result of disruptions of the bulk power system. Rather, they result from more local events such as thunderstorms and vehicles crashing into utility poles. However, regional blackouts of the bulk power system do occur, sometimes as a result of errors made by system operators, sometimes as a result of

damage caused by natural events. The power system is inherently vulnerable because it is spread out all across the landscape.

Figure 1 (reproduced from NRC, 2012) shows that the distribution of larger outages in the U.S. bulk power system displays a "fat tail" – that is larger outages are much more common than one might expect from a simple statistical model. Because of restructuring of the electric power industry, which has resulted in using the high-voltage transmission system in ways for which it was not originally designed, today that system operates under stress, with the result that it has a reduced ability to absorb disruptions.

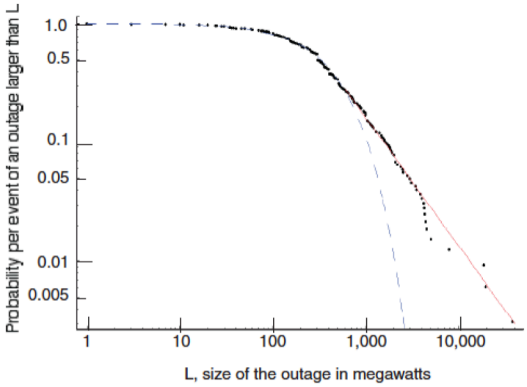

Figure 1: Relative frequency of electrical outages in the United States between 1984 and 2000. Of the 533 transmission or generation events shown, 324 involved a power loss of >1 MW (average of once every 19 days), and 46 involved a power loss of >1,000 MW (average of 3 per year). Dots indicate actual outage events. The dashed line is an exponential (Weibull) distribution fit to the failures below 800 MW loss. The solid line is a power law fit to the NERC data over 500 MW loss. SOURCE: Data compiled by NERC DAWG, plotted by Jay Apt, Carnegie Mellon University, 2006. Reproduced from NRC (2012).

In this testimony, I address three topics:

1) strategies to avoid physical disruption of the power system;
2) strategies to speed the process of putting the system back together after physical disruption; and
3 strategies to assure the continued provision of critical social services when grid electricity is not available.

1. Strategies to avoid physical disruption of the power system.

From time-to-time Mother Nature produces events that can cause significant damage to the power system. Hurricanes and associated storm surge, wildfires, tornadoes, floods, earthquakes, tsunamis, ice storms and space weather can all cause serious physical damage and widespread hardship.

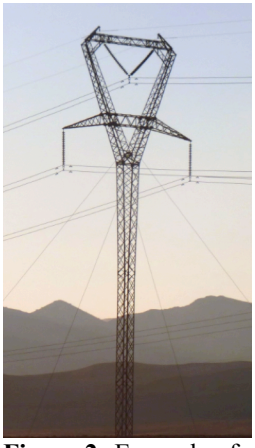

Figure 2: Example of a guyed transmission tower. Such towers can be less expensive but subject to "domino collapse." Image from Wikimedia.

However, while such events are inevitable, there are a variety of things that system designers and operators can do to make the power system more robust and thus minimize the damage they cause and the resulting adverse consequences. For brevity I offer just two examples.

It is less costly to build high-voltage transmission lines in such a way that guyed towers are partly supported by the power cables themselves (Figure 2). However, if a single tower collapses, because of a heavy load of ice, an earthquake, a hurricane, tsunami, or terrorist act, then many other towers many also fall in what is often termed a "domino collapse." By spending a bit more money and periodically inserting towers that are strong enough to be self-supporting, damage

can be limited. For example, in California regulations require that every tenth transmission tower must be stronger so that an earthquake will not trigger such a collapse.

Because the power system is spread out across the landscape it is inherently vulnerable to both natural and intentional physical damage. Large substations are especially vulnerable. They contain high-voltage transformers, circuit breakers, and other large equipment, that if damaged can be very difficult and expensive to replace. Many transformers involve custom designs. It can take many months to secure replacements. Moving these large and extremely heavy devices also poses big challenges. Recent years have witnessed efforts to increase the resilience of such systems, for example by shock mounting equipment in earthquake prone areas, taking greater precaution against intrusion by wildfire, etc.

Fortunately, the U.S. has not experienced any large coordinated terrorist attacks on the power system (see pages 9-15 of NRC 2012 for a discussion of why that might be and when and to whom the system might be an attractive target). However, deliberate attacks on power systems have been common in some parts of the world. In North America, modest attacks have been carried out by vandals, environmental absolutists, Canadian First Nation groups concerned about facilities on traditional lands, and disgruntled former employees.

If a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high voltage power transformers. Such transformers are expensive, hard to replace, and often sit out in the open surrounded by only a chain-link fence. A 1990 OTA report noted that the bulk power system is vulnerable to "saboteurs with explosives or just high-power rifles."

Unlike the 1990 OTA report, in the National Academies' report on *Terrorism and the Electric Power Delivery System* that I chaired, we were careful *not* to be explicit about means by which an attack might be carried out. However, after the 2013 rifle attack on the substation in Metcalf, CA, such caution is probably no longer needed. A terrorist organization that wanted to cause massive disruption to the U.S. power system could order rifles and armor piercing bullets on the Internet, place sharpshooters in the back of station wagons like the 2002 Washington snipers, and from a distance put holes in a carefully selected set of critical high-voltage power transformers.

Replacing chain-link fences with opaque and more robust enclosures around substations can reduce vulnerability and increase system resilience. There are many similar strategies that can be adopted to make power systems more robust in the face of both natural and terrorist events. A description of some of these can be found in Chapter 6 of the NRC report *Terrorism and the Electric Power Delivery System* (NRC, 2012).

2. Strategies to speed the process of putting the power system back together after physical disruption.

The electricity industry has an excellent track record in restoring damaged portions of the system after natural disasters, such as hurricanes. There are standing arrangements for

cooperation between firms and line crews from other companies who are often dispatched from many hundreds of miles away to aid in recovery.

Many of the preparations and strategies that power companies make to deal with natural hazards are equally applicable to deal with the physical disruption that might be caused by terrorist events. Chapter 7 of the NRC report *Terrorism and the Electric Power Delivery System* (NRC, 2012) discusses strategies for system recovery at some length.

As noted above, if a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high voltage power transformers. As the Department of Energy explained in its recent Quadrennial Energy Review (QER, 2015):

> LPTs [large power transformers] can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of 1 year or more. In addition, due to their size and weight, moving LPTs presents logistical challenges requiring specialized equipment, permits, and procedures…
>
> The loss of critical LPTs can result in disruptions to electricity services over a large area. Such a loss could be due to the customized nature of the components and the associated manufacturing requirements, as well as physical attacks (such as the Metcalf incident), natural hazards (such as geomagnetic disturbances…), or extreme weather (such as floods, salt water corrosion, and sudden heat waves). In the Metcalf attack on a substation in California, "multiple individuals outside the substation reportedly shot at the [high-voltage] transformer radiators … causing them to leak cooling oil, overheat, and become inoperative."…
>
> The United States has never experienced simultaneous failures of multiple high-voltage transformers, but such an event poses both security and reliability concerns. The Edison Electric Institute, seeking to manage such vulnerabilities, has established a Spare Transformer Equipment Program, enabling utilities to stockpile and share spare transformers and parts. The inventory under this program is not large enough, however, to respond to a large, coordinated attack. Transformer design variations and the logistical challenges associated with their movement pose additional challenges to maximizing the effectiveness of the program. A National Research Council study referring to this effort noted that "... The industry has made some progress toward building an inventory of spares, but these efforts could be overwhelmed by a large attack" and that "it alone is not sufficient to address the vulnerabilities that the United States faces in the event of a large physical attack."…

Paul Parfomak, a specialist in energy and infrastructure policy at the Congressional Research Service has prepared an excellent report on this topic, which the Committee staff has kindly shared with me. Rather than summarize, below I reproduce the abstract of that report (CRS, 2015) and urge the committee to give the full report a very careful reading.

> The U.S. electric power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations. High voltage (HV) transformer units make up less than 3% of U.S. transformers, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes, HV transformers are critical to the nation's electric grid. HV transformers are also the most vulnerable to damage from malicious acts.
>
> For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures. There has been

some level of physical security investment and an increasing refinement of voluntary security practices across the electric power sector for at least the last 15 years. However, recent grid security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have changed the way grid security is viewed and have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security efforts by utilities and regulators.

On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by the North American Electric Reliability Corporation (NERC). The new standards require certain transmission owners "to address physical security risks and vulnerabilities related to the reliable operation" of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks. Legislative proposals would expand federal efforts to prevent or recover from a physical attack on the U.S. grid. These include the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243).

There is widespread agreement among government agencies, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the actual risk of a multi-HV transformer attack remains an open question. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, recovery from HV transformer attacks, and the overall resiliency of the grid. Maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

Our National Academies report on *Terrorism and the Electric Power System* (NRC, 2012) recommended that the Department of Homeland Security and the Department of Energy develop a stockpile of emergency replacement transformers, an idea first studied years ago by EPRI. While still very large, these transformers would be somewhat easier to move. However they would not be as efficient as the devices they were replacing and so would provide only temporary service during the many months it would take to manufacture, move and install permanent replacements. Between 2012 and 2014, DHS demonstrated this idea (NYT, 2012). Attachment 1 describes the program. While this demonstration is clearly useful, there is an urgent need to move beyond demonstration to implementing a stockpile.

As noted above and in Parfomak's report, the Edison Electric Institute and others have worked to better coordinate the modest existing stocks of spare transformers, but those stocks are not sufficient. DOE recently released a request for information to gather input on setting up a transformer reserve, and eight private energy companies have launched "Grid Assurance," an independent organization that will stockpile transformers and other critical equipment.

A variety of technical and operational actions exist that can be taken now to reduce the vulnerability of the bulk power system. While power companies are moving to implement many of them, it is also true that the risks faced by most individual facilities are relatively small. In some cases, it is not reasonable to expect private firms to make investments that, while they may carry considerable collective social benefit, yield little immediate benefit to the firms that are involved. Congress would do well to work on identifying strategies to change those incentives.

In addition, research could produce additional and perhaps more cost-effective strategies to increase system resilience. The Office of Electricity of the U.S. Department of Energy, and the several DoE National Labs they support through their programs, are, in my view, doing very good work. They have considerably greater technical expertise than DHS to address the key issues of grid security in parallel with the issues of grid modernization, and, in my view, should be given a more leading role in that area. That office has operated with modest funding for many years and could benefit from increased support.

At the level of more basic power-systems research, the National Science Foundation (sometimes in collaboration with DOE) has funded several research center activities including PSERC (http://pserc.wisc.edu/home/index.aspx) and CURENT (http://curent.utk.edu). Such collaborative academic research makes valuable contributions to improving the resilience and security of the power system and should be encouraged.

3. Strategies to assure the continued provision of critical social services when grid electricity is not available.

For many years the power engineering community focused exclusively on the problem of assuring the continued operation of the bulk power system. While that is clearly very important, it is also important to work on developing strategies to assure the continued provision of critical social services in the event of serious power outages (Talukdar et al., 2003; IEEE, 2004; Ch8 in NRC, 2012).

Since occasional power outages are inevitable, and blackout from terrorist attack is possible, the nation should take steps to assure that critical social services can continue to operate when the power goes out. Key strategies include:

- LED traffic signals with solar cell and battery back-up so that traffic does not snarl and block emergency vehicles in key transportation corridors. Such systems are commercially available.[1]
- More systematic and reliable use of back-up generators.

Figure 3: Example of an advanced CHP system developed by Dean Kamen of DEKA Research and Development. (Photo by G. Morgan.)

[1] Battery back-up LED traffic lights are now in use in a number of states (e.g., CA) and cities (e.g., NYC). Trickle charge LED chargers are less common but also commercially available.

On both of these see Apt and Lave (2004).

- Cell phone and other communication systems that will remain intact and continue to operate, not just for hours but for days.

The development of modern "smart grid technology" and of distribute resources, such as conventional and advanced (Figure 3) natural gas fired combined heat and power generators, provide the technology that can be used to support the creation of islands of reliable power to support critical social services when, for whatever reason, grid power becomes unavailable.

Narayanan and Morgan (2012) have elaborated strategies that show how this might be done (Figure 4). Because many utilities are already installing distribution automation, smart meters, and other needed technology, their analysis of the incremental cost to implement such a system:

> …suggests that at least a few regions might find it reasonable to invest in a system of the type we have outlined to secure critical social services in the event of a large, long-duration outage… Clearly, no electric utility will make these investments on its own. However, if a public utility commission (PUC) concluded that installing such capabilities constituted a prudent investment, then in regulated distribution companies non-depreciated capital costs and operation costs could be recovered through the rate base with the approval of the regulator. Alternatively, local, county, or state government might choose to fund the project with tax revenue, contracting with the local distribution utility and other parties to implement the changes.

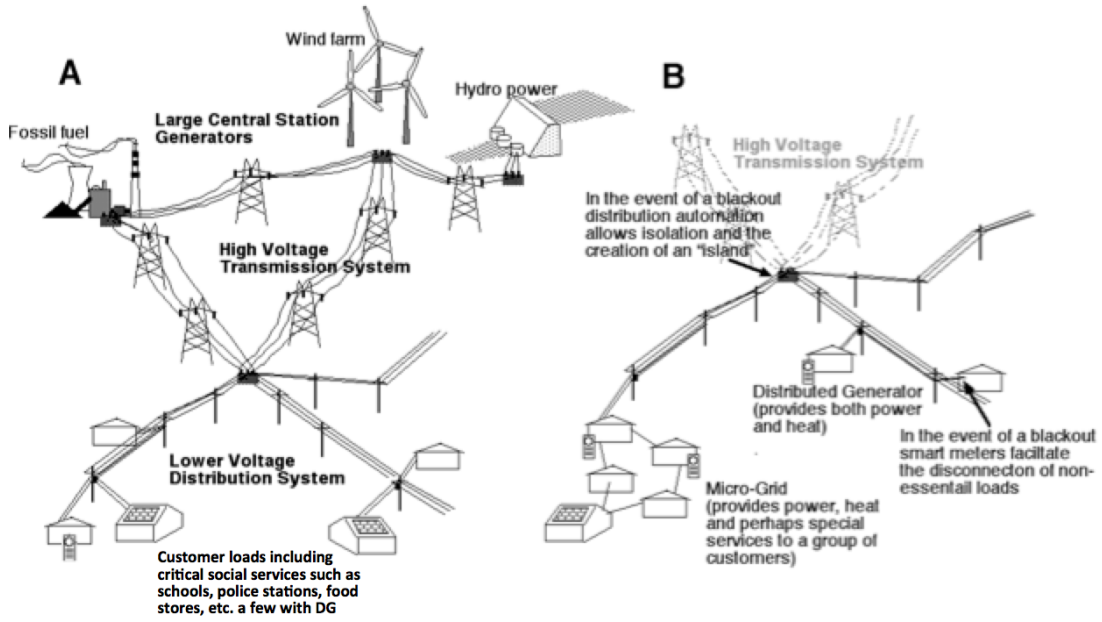

Figure 4: Left, simplified illustration of the electric power transmission and distribution system under normal operation. Right, simplified illustration of the islanded distribution system during a large, long-duration blackout in which DG units serve local critical social services. Smart meters have disconnected loads that are not critical. Feeders have been reconfigured to form an isolated "island" using distribution automation and added low-power fault-handling equipment. Figure modified from Narayanan and Morgan (2012).

Some of the issues involved in promoting the wider development and adoption of micro-grids, and systems of the sort discussed by Narayanan and Morgan (2012), fall under the

limitations imposed by state laws that grant "exclusive service territories" to legacy utilities (making it difficult to build even small privately operated micro-grid systems) and under the responsibilities of state public utility commissions. However, there are also roles the Federal government can play. In this connection, the National Academies' report on terrorism and the grid made the following recommendations:

> **Recommendation 8.1** The Department of Homeland Security and/or the Department of Energy should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private participants, including public and private parties providing law enforcement, water, gas, sewerage, health care, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration (> several weeks) and large geographic extent (over several states) since such outages would require a response different from those needed to deal with shorter-duration events (hours to a few days).
>
> **Recommendation 8.2** Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts.
>
> **Recommendation 8.3** State and local regions should use the tools provided by DHS as discussed in Recommendation 8.2 to undertake assessments of regional and local vulnerability to long-term outages, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities.
>
> **Recommendation 8.4** Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities.
>
> **Recommendation 8.5** Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency.
>
> **Recommendation 8.6** DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private

> sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans.

With the exception of some limited work in the area of Recommendation 8.6, I am unaware of any actions that have been taken to follow up on these recommendations.

References:

Apt, Jay and Lester Lave, "Blackouts Are Inevitable: Coping, Not Prevention, Should Be the Primary Goal, " *Washington Post*, August 10, 2004; Page A19, available on line at: http://www.washingtonpost.com/wp-dyn/articles/A52952-2004Aug9.html

CRS 2015. "Physical Security of the US Power Grid: High-voltage transformers substations, " Report 7-5700/R43604 prepared by Paul W. Parfomak, Specialist in Energy and Infrastructure Policy, 36pp.

IEEE 2004. "The Unruly Power Grid," an article by Peter Fairley in *IEEE Spectrum*, August 2004, pp. 22-27.

Narayanan, Anu and M. Granger Morgan, "Sustaining Critical Social Services During Extended Regional Power Blackouts," *Risk Analysis*, *32*, 1183–1193, 2012.

NRC 2012. *Terrorism and the Electric Power Delivery System*, National Academies Press, 2012. 146pp. Available at: http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

NYT 2012. "A Drill to Replace Crucial Transformers…," an article in *The New York Times* by Matthew L. Wald, March 15, p. B4.

OTA 1990. *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage,* OTA-E-453, NTIS order #PB90-253287, 63pp. Available on many different web sites including: http://ota.fas.org/reports/9034.pdf

QER 2015. U.S. Department of Energy Quadrennial Energy Review: Energy transmission, storage and distribution infrastructure, 347pp.

Talukdar, Sarosh N., Jay Apt, Marija Ilic, Lester Lave and M. Granger Morgan, "Cascading Failures: Survival versus prevention," *The Electricity Journal*, 25-31, November 2003.

Attachment 1: One page description from the U.S. Department of Homeland Security of their recovery transformer demonstration program. The transformers were developed by ABB. See: http://www.abb.com/cawp/seitp202/9a9f00ef6e90dd00c1257a7e0042e142.aspx

DHS Science and Technology Directorate

Recovery Transformer

Extra high voltage transformers are the backbone of the electric grid but face many challenges, creating a potential vulnerability for the grid.

The United States electric grid is incredibly complex with more than 80,000 miles of extra-high voltage (EHV) transmission lines carrying electricity over long distances from generation stations to distribution networks. At critical nodes, EHV transformers either step up voltage for transportation across long distances or step down voltage prior to distribution to consumers. Ninety percent of consumed power passes through these critical pieces of equipment at some point on the transmission grid. If these transformers fail—especially in large numbers—the nation could face a major, potentially long term, blackout.

A damaged transformer at the Salem Nuclear Plant. (Metatech)

Many of the EHV transformers installed in the United States are approaching or exceeding the end of their design lifetimes (approximately 30 to 40 years), making them more vulnerable to failure. EHV transformers are huge, weighing hundreds of tons, making them difficult to transport. In some cases, specialized rail cars must be used (and there is a limited supply of these). Typically, it can take several months to transport and install a single EHV transformer due to the size and complexity of the equipment.

S&T develops new technology for the power grid, reduces time to recover by 75 percent or more

The Department of Homeland Security Science and Technology Directorate (S&T) partnered with the electric utility industry and the Office of Infrastructure Protection to initiate the Recovery Transformer (RecX) project. Through this project, S&T developed a prototype EHV transformer that drastically reduces the time to transport, install and

RecX in-grid deployment (Paul Wedig)

energize an EHV transformer to recover from outages associated with transformer failures from several months to less than one week, in the case of an emergency. S&T developed the RecX to be easier to transport (weighing approximately 60 tons versus hundreds of tons for traditional transformers) and quicker to install, reducing potential recovery time for transportation, installation, & energization of EHV transformers by more than 75 percent.

Together with industry partners, S&T successfully demonstrated the RecX prototype for one year ending in March 2013. The team transported a RecX from St. Louis to Houston, then installed, commissioned and energized it in less than a week, then monitored the RecX's performance over to validate its design and operational behavior. The RecX proved successful in an operational environment; it has the capability to reduce the impact of outages and increase the resiliency of the uniquely critical energy sector that directly effects not only functions across all other critical infrastructures but the nation's safety, prosperity, and well-being as well.

RecX Transportation (Paul Wedig)

Homeland Security
Science and Technology

To learn more about RecX, contact sandt.rsd@hq.dhs.gov.

2014-11-11