THE NATIONAL ACADEMIES

MEETING IN BRIEF

Improving Power System Resilience in the 21st Century

Resilient America Roundtable

July 24-25, 2014

The National Research Council (NRC), with the Electric Power Research Institute (EPRI) and the National Association of Regulatory Utility Commissioners (NARUC), held a symposium on July 24-25, 2014, to explore ways to strengthen America's power grid to withstand or recover from a wide range of natural and man-made disruptions. The symposium was designed to provide a foundation for a larger workshop on power system resiliency to be held in 2015 and, informs the work of the Resilient America Roundtable's community-based pilot projects.

Welcoming remarks were given by **M. Granger Morgan,** co-chair of the Resilient America Roundtable, and **Lauren Alexander Augustine**, NRC director of the Program on Risk, Resilience and Extreme Events. "As we travel around the country talking about resilience", said Augustine, "the first thing community leaders say during and after any disaster is 'get the lights on'". Electric power is critical to a wide range of social services and disaster recovery, continued Morgan. The objective of this symposium is to identify strategies that could be used to improve the resilience of transmission and distribution systems, and to speed their restoration after disasters; and to provide a list of topics and good practices (rather than formal recommendations) to enrich dialogue between decision makers and power suppliers.

Resilience is defined as "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events," (National Academies, 2012)[1], with a focus here on the services that are provided by the power system (in contrast to solely grid reliability). The workshop's first day focused on the high-voltage transmission system; the second day focused on the distribution system.

IMPROVING THE RESILIENCE OF HIGH-VOLTAGE ELECTRIC POWER TRANSMISSION SYSTEMS

A number of things can be done to protect the transmission system, Morgan offered. Transmission lines consist of a set of towers held up by tension between the wires; on the ends are anchor towers. If a disruption occurs, a domino effect can result and many towers will break. There are ways to increase the system's resilience, such as designing stronger conductors and more robust towers to withstand natural hazards, and walls that protect against human intrusion. But the system cannot be made completely resilient, he cautioned, and actions are needed to speed restoration.

---

[1] National Academies. 2012. *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press. http://www.nap.edu/catalog/13457/disaster-resilience-a-national-imperative.

Extreme Weather

W. Terry Boston of PJM cited the occurrence of "wild card" disasters—high-impact, low-frequency events such as the Fukushima Daiichi nuclear disaster, Derechos, and Superstorm Sandy, all of which have occurred in recent years. Boston shared PJM's definition of resiliency (Figure 1), derived from work he did as part of the National Infrastructure Advisory Council, noting that the key to resiliency is understanding that we cannot prevent disruptions, but we can "plan for, ride through, and recover from each event, and learn during the process."

Superstorm Sandy caused approximately 8.5 million customer power outages. Boston explained that from the transmission side, PJM's biggest problem was with high voltage and having to take lines out of service to prevent major equipment damage, but balance was restored fairly quickly; disruptions to the distribution system were the primary cause of the outages. From an emergency planning perspective, challenges arose in managing and deploying over 65,000 people from around the country who arrived to help restore power.

In addition to extreme weather, Boston pointed to threats from space weather and cyberattacks. In 1989, PJM experienced a large space weather event that disabled transformers at the Salem Nuclear Plant. Despite that event, he noted, space weather has not resulted in major problems, and it's hard to know "what's hype and what's real." Boston indicated that issues with cybersecurity are more immediate, noting that PJM had a peak number of 8,900 hits in November 2013, of which 4,090 were documented attempts to attack their system. The probability of cyberattacks is increasing, he said, and PJM has tripled its budget and increased capabilities for defending their systems.

At Southern Company, **William O. Ball's** job is to plan, design, construct, maintain, and operate the transmission grid in the South. "But my real job is to keep the lights on," he said. Southern Company takes an all-hazards approach to resilience, exploring all possible ways the system can be compromised, and seeks to develop cost-effective solutions that increase the resilience of the overall system. We operate vertically integrated utilities, which helps to avoid siloed thinking focused solely on generation or transmission or distribution solutions. Balancing the cost of service vs. building resilience is challenging, he added; maintaining balance means using solutions that protect against multiple scenarios.

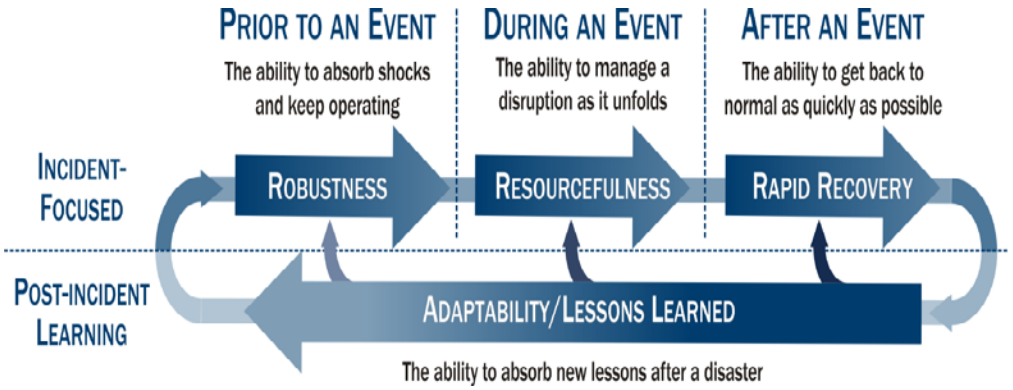

FIGURE 1: The sequence of events of the resilience construct.
SOURCE: National Infrastructure Advisory Council, 2010. Framework for Establishing Critical Infrastructure Goals: Final Report and Recommendations[2].

[2] National Infrastructure Advisory Council, 2010. Framework for Establishing Critical Infrastructure Goals: Final Report and Recommendations. From the report, "Robustness includes the measures that are put in place prior to an event; resourcefulness includes the measures taken as a crisis unfolds; rapid recovery includes the measures taken immediately after an event to bring things back to normal; and adaptability includes the post-incident measures and lessons learned that are absorbed throughout the system." http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.

Ball pointed to the importance of preparation and exercising of recovery plans. He cautioned that it's unwise to depend solely on past experiences for guidance on future events because people can't imagine a scenario worse than what they've already experienced. Having strong, trusting relationships in place before an event is key; while local, state, and federal partnerships are all important, local partnerships are the most important. Authority should be delegated as close to the site of the disruption as possible, since central coordination often slows down the response.

Dan Ton of the U.S. Department of Energy's Office of Electricity and Energy Reliability discussed the suitability of microgrids to support efforts to improve resiliency of power delivery systems. Ton defined resilience as the capacity to absorb shocks and keep operating, to manage a disruption as it unfolds, and to get back to normal as quickly as possible. Advanced microgrid concepts and technologies can correspond to these stages, he proposed, and during all three it is important that the microgrid operates interactively with the distribution system.

Ton explained that a microgrid is a group of interconnected loads and distributed energy resources that act as a single controllable entity with respect to the grid; it can operate in both grid-connected and "island" modes. The ability to intentionally separate parts of the system prevents cascading blackouts and reduces the time required to restore power. An advanced microgrid includes a fully functional energy management system and interacts with the power delivery system.

Ton's office is developing advanced microgrid system design and control functionalities that community's can implement to support their resilience objectives, decision support tools for a centralized energy system, and tools for power system restoration. With the growing threat of severe weather events, Ton noted, the value of microgrids in protecting the national electrical grid from power outages is increasingly important. Advanced microgrids contain essential elements of large-scale grids, have the capacity to interact with, connect to, and disconnect other grids, and can help to mitigate the economic impacts of power disruption. DOE partners with states to deploy microgrids, said Ton; the long-term vision is full integration of microgrids at multiple levels, from distribution to transmission, nationwide. These technologies will result in a self-healing power system that can better serve the well-being and development of the American people and economy.

Paul Parfomak, Congressional Research Service, noted that although resiliency is not driven by physical security, following recent attacks such as the 2013 attack in Metcalf, California against a critical transformer substation, physical grid security is an increasing concern in Congress and industry. Congress has expressed concern to the Federal Energy Regulatory Commission (FERC), held hearings about grid security, and proposed legislation to bolster FERC's ability to protect the grid. The electric sector augmented ongoing initiatives to increase physical security, including information sharing, security exercises, and programs to replace and restore critical spares. Mandatory physical security standards for high-voltage transmission systems were developed and adopted by the North American Electric Reliability Corporation (NERC), a not-for-profit international regulatory authority focused on ensuring reliability of the bulk power system in North America. Companies adopted new measures to protect high-voltage critical assets at a cost of hundreds of millions of dollars.

Parfomak listed ways to physically secure high-voltage substations, including protecting critical information, conducting surveillance and monitoring, using better locks and vehicle barriers, and installing hardened walls and taller fences. Substation designs can be modified to be less vulnerable, for example by separating single-phase units in case a fire occurs. The question isn't so much *how* to protect substations but *how much,* he added: How much can you justify the costs of improving security under uncertainty? Debate also concerns the proper roles of regulators and industry. The federal government no longer thinks that voluntary physical security measures are adequate, and measures are now being mandated.

Solar Weather

The next panel explored strategies to assess and improve transmission system resilience to solar weather. **Ron Turner** of Analytic Services, a not-for-profit company that advises government, discussed how space weather and solar storms could affect the power grid. Of most concern are coronal mass ejections—large plasma clouds directed from the sun toward Earth that impact the Earth's magnetic field, creating a geomagnetic disturbance that can affect the power grid through ground-induced currents (GIC). Coronal mass ejections typically take three days

to reach Earth but can arrive in as little as 12 hours. Depending on how they align with Earth's magnetic field, there can be little or significant impact. A solar storm caused a power grid outage in Quebec in 1989, and during a major storm in 1859, the Carrington Event, telegraph shacks caught on fire from induced current in the wires.

Even though there have been large storms over the last 150 years, it's difficult to quantify the risk, said Turner; NERC and the scientific community have ongoing efforts to quantify storm frequency and impact. Forecasters can provide short-term warnings – 6 to 12 hours in advance – for solar storms but not multiday forecasts. Geospace is monitored with satellites, and currently we have a robust architecture. However, Turner cautioned, many of the observational instruments used are degraded, drifting out of range, or past their expiration date.

John Kappenman, Solar Storm Consultants, drew upon experience studying and analyzing data related to the impacts of solar storms on the power grid to invite discussion about open questions, vulnerabilities, and opportunities to develop ways to address these hazards. From his analysis, the March 1989 Quebec solar storm and resulting blackout did not represent a worst-case scenario, which he said could be 4 to 10 times greater. The US's power grid was developed without considering vulnerability to solar storms, and between the1950s to 2000, the grid grew by a factor of 10 and went to higher operating voltages, escalating the system's vulnerability. If the worst-case scenario solar storm unfolds, unprecedented blackouts could occur, and the potential exists for widespread catastrophic permanent damage to key grid assets.

IEEE survey data on transformer failures from 1980 to 1994 correlate highly with important geomagnetic storms during that period, and this correlation suggests that solar storms may be a major cause of transformer problems. Kappenman expressed concern about how vulnerability is currently being assessed, noting that FERC's proposed standards and models do not include the most robust baseline data. He concluded by raising mitigation options, such as building transformers to be GIC tolerant or resistant, or developing blocking devices to keep GIC out of the system, but cautioned that the effectiveness of these options is not well known.

Mark McGranaghan, Electric Power Research Institute (EPRI), offered an overview of the institute's research and development activities around geomagnetic disturbance (GMD), and how it relates to grid resiliency. Research ranges from understanding how to model the system and assess the vulnerability to evaluation of the performance of mitigation measures. McGranaghan stated that industry takes the threat of solar storms very seriously, and there are ongoing efforts to understand and address the risks. EPRI works with NERC, and brings utilities to the table to participate in research. He noted several areas where more work is needed, including risk-based planning and assessment, monitoring and modeling, and a better understanding of harmonics. It is important to develop models that can assess the potential for voltage limits to be exceeded, taking the whole grid down. One of the accomplishments of the group is providing tools to industry so they can do analysis—a big success story in terms of research.

Transformer modeling is a key area, and work is needed to understand whether the models are right in terms of how they saturate and whether a transformer will survive during an event. Monitoring is also critical, he emphasized. Since the late 1980s the Sunburst Network has monitored GIC around the world to characterize and help model these events. DOE is monitoring actual magnetic fields. Individual utilities are monitoring currents, harmonics and reactive power, and transformer vibration, allowing for much better characterization of what is happening in a system. McGranaghan stated that it is critical to take an integrated approach, which leads to risk based planning. He emphasized that all aspects of research are important, including forecasting, operations, equipment design and specifications, and locations that may need neutral blocking devices to protect the transformers. Part of the research, he added, is evaluation of the performance of different devices and their potential for application, as well as education and training.

Emanuel Bernabeu, of Dominion Virginia Power, offered a utilities perspective on how to create a resilient power system with respect to GMD. He defined resilience as the ability to reduce the magnitude and/or duration of a disruptive event. Four key words resonate with resilience – anticipate, absorb, adapt and recover – and Dominion approaches GMD with respect to each of these concepts. Three problems are associated with GMD: the DC current can create hot spots within transformers, harmonics can result within the system, and transformers will consume more reactive power, which can cause voltage problems.

Dominion's mitigation methodology is based on three pillars: modeling, equipment hardening, and situational awareness and operating procedures. Modeling to identify the flows of GIC is the first and perhaps the most important step, he said. The company also models harmonic flows and uses thermal models to predict temperature rise. Not every transformer gets impacted in the same way; the analysis lets them identify critical locations, and provides a guide for investment in time and effort. The second pillar is equipment hardening. Following the 1989 storm—when significant mis-operations of their protection schemes for capacitor banks occurred—Dominion changed its philosophy of protection; it is now immune to harmonics and imbalance in the network.

The third pillar is situational awareness and operating procedures. Dominion receives alerts from NOAA and has an extensive suite of real-time information that includes GIC monitors that measure the DC current. The company uses forecast information to prepare the system for large events, he explained, and real-time information to direct needed actions; the operator can adjust the system's topology to change the risk exposure of different assets.

Cybersecurity

The third panel focused on protection of the grid from cyberattacks. **William H. Sanders**, the University of Illinois, articulated the challenge as "providing trustworthy grid operation in possibly hostile environments." A trustworthy system does what it's supposed to and nothing else, said Sanders, quoting a 1999 NRC study, *Trust in Cyberspace*. In other words, while achieving the mission, it's important to ensure that there aren't unintended consequences.

We need a combined approach, proposed Sanders, that uses approaches from classical cybersecurity that are optimized for grid characteristics, but that recognizes protection won't be perfect. Sanders identified several challenges, including the importance of understanding the relationship between the grid's cyber and physical infrastructure, the need to create a reliable computing base throughout a system that could be geographically distributed and exposed, the challenge of scale, considering the numbers of devices and business entities and the large potential attack surface of the grid, and how to detect and make sense of the potentially large number of events.

We need to think carefully about responses to cyberattacks, cautioned Sanders. When a resilient system is built, in that it adapts to a cyber or combined cyber and physical attack, can an attacker use that quality to drive the system to an unsafe state? To understand if progress is being made, he suggested the development of "a science of cybersecurity and trust assessment", using metrics to understand tradeoffs for different proposed solutions, technical needs, and interdependencies.

Paul Hines, the University of Vermont's School of Engineering, discussed the connection between power and cyber networks. Large blackouts are costly and are often caused by cascading events, he said. Because grid failures spread widely, a small number of broken parts can quickly become a very large blackout. He identified three important questions: a) how does increased coupling between a power and communications network impact vulnerability? b) How can we understand and reduce large-scale blackout risk once there is a model of how blackouts spread? c) How can we model power failures? In approaching power failure modeling, Hines cautioned that different models yield different results in terms of identifying areas of greatest vulnerability; results will differ when using a topological vs. power vs. cascading failure model. Using the wrong model can yield the wrong answer, and theoretical graph models can be very misleading.

Vulnerability is hard to predict, Hines emphasized. Increasing the coupling between the cyber and physical network can make the grid more robust or more vulnerable, depending on the design. The failure of any single component will not cause a large blackout, but when things fail in combination, blackouts can occur. Hines and his colleagues are working to identify critical components—pieces of a network that, when they fail at the same time as other components, add a lot of risk to the system.

Selecting Effective and Cost Effective Transmission System Resilience Building Strategies

The day's final panel explored how society might decide which resilience-building options and strategies to adopt, how to pay for them, how to improve coordination among relevant players, and how legal and regulatory obstacles could be alleviated. Consultant **Ellen Lapson** drew upon years of experience working with resilience in the context of

financing entities in the utility industry and companies in infrastructure ownership.

Lapson identified two key questions in making improvements to build more resilience into the power system: a) How will "the best" approaches be determined, considering all available possibilities and the likelihood that improvements will require capital investment and/or increase operating expenses, and b) if society mandates a need for greater resiliency, who is responsible to pay for and implement these improvements? Among the likely candidates for supplying funds, are utilities, regional transmission organizations, consumers and manufacturers, and other companies within the sector; the only parties positioned to bring large quantities of investment are rate-regulated utility companies.

The process by which utility regulatory commissions and organizations decide what types of resources to invest in is based on open disclosure at public forums and regulatory proceedings, said Lapson. She raised the question of whether, with regard to resilience, the process might require more information to be divulged about vulnerabilities than is safe. It could take 5 years to complete the process and fix a problem, while a terrorist could act within months of the information being disclosed. If the risk is real, she said, we need to streamline or alter the processes of transparency so that sensitive information is not publicized through an unauthorized leak.

One option for accelerating the adoption of new approaches, Lapson suggested, is to galvanize the natural interest of major industry players. She challenged the view that utilities are not suited to implement microgrids, noting that rate regulated investor owned utilities are eager to find new investment opportunities, as they now serve a market that is not growing; microgrids could be a real opportunity to take an unconventional approach. Lastly, she emphasized the importance of focusing on the needs of research and development, and finding actionable solutions to these issues.

Paul Stockton, former Assistant Secretary of Defense for Homeland Defense, was responsible for ensuring mission assurance and continuity of operations at the Department of Defense (DOD). Following Superstorm Sandy, he led DOD support to FEMA and affected states. Stockton cited NARUC's definition of resilience, the robustness and recovery characteristics of utility infrastructure and operations that avoid or minimize interruptions of service during an extraordinary and hazardous event, and emphasized the need to prepare for "black sky days," —utterly unlike blue sky days for which the grid is optimized. These events are much worse than major outages.

Stockton outlined the problems of cost recovery related to investments in resilience. The bulk power system requires utilities to demonstrate that investments are used and useful. What is a prudent investment against uncertain hazards and events that are impossible to assess but will have enormous effects on public health and safety, and national security? What is cost effective, and how do you assess cost effectiveness using traditional tools? Stockton stressed the importance of equity issues and, given the emergence of distributed energy generation, fairly distributing the cost of maintaining a reliable bulk power system.

Patrick Hogan of Pacific Gas & Electric Company, serving 15 million customers in Northern California, defined resilience as understanding risks, designing systems to mitigate their impact, and ultimately, restoring service when an event occurs. In California, they are working to change ratemaking proceedings, the formal regulatory process by which prices are set. Typically, during rate making, the utility presents information to the commission on key risks it faces, and agreement is reached on the priorities. The next step involves discussing what to do about that risk, and the cost of mitigating or avoiding it. There's a tradeoff in terms of investments to harden the system, he noted, and investments in power restoration capabilities.

Innovative approaches to build resilience are being explored, such as how stationary and mobile storage might support microgrids, aid solar power during times of cloud cover, and serve as emergency backup. He noted the importance of collaboration among stakeholders; which is founded upon a common framework for prioritizing and funding investments, policy makers and energy regulators working together on priorities and accountability, and creating forums for taking in and reflecting community and stakeholder input.

IMPROVING THE RESILIENCE OF ELECTRIC POWER DISTRIBUTION SYSTEMS

Colette Honorable, chair of the Arkansas Public Service Commission and president of NARUC, said that economic regulators are broadening the way they think about resilience and reliability, and about the associated interdependencies. NARUC advocates

a risk-based approach that promotes industry on the front lines, and equips regulators with tools to respond in new and different ways to new and different proposals. Economic regulators are interested in considering alternative ratemaking techniques, whether trackers, surcharges, or other cost effective methods that are prudent in the public interest. We all share the same goal, Honorable concluded, ensuring safe, reliable, and affordable utility service for the people that we serve.

Extreme Weather

Panel one explored strategies to increase resilience and speed restoration of distribution systems in the event of severe weather. **Jeffrey Williams** of Entergy, a utility headquartered in New Orleans that provides electricity to 2.8 million customers in Gulf Coast states, said that after Katrina, so much of their infrastructure was damaged that Entergy had to take its company, Entergy New Orleans, into bankruptcy to bring it back; there were no customers to bring in revenue. The power infrastructure loss ($1.5 billion) was less than 1 percent of the total damage ($150 billion) that communities suffered—a fact that made Entergy aware that the larger risk was the sustainability of their customer base.

Entergy is seeing many more billion-dollar loss events. In taking a risk perspective, the company undertook a study to map assets and commissioned Swiss Re to do probabilistic loss modeling. Results demonstrated that by 2030 damages from the 100-year storm, previously at $150 billion, would rise to $200 billion, and the "100-year" storm would happen once every 40 years. Entergy tested the cost-effectiveness of 50 different adaptation measures. The current system does not support a proactive approach, said Williams, funds become available after a disaster occurs; it is difficult to invest a dollar today for an uncertain benefit in the future, although that is a much better approach.

Williams posed the question, "what can you do to become more resilient?" First, get prepared. Entergy has hardened its transmission distribution system using concrete and steel construction, accelerated vegetation management, and elevated substations. The company conducts drills under various scenarios and engages in mutual assistance agreements with other utilities. He emphasized the importance of working with community members; Entergy held 12 blue ribbon resilient community leadership forums in the Gulf to talk about where the community is vulnerable, what individuals are doing to promote their resilience, and how Entergy and the community can work together. It also held two technical conferences with customers to evaluate hardening options to reduce economic losses.

David Owens, Edison Electric Institute (EEI) recounted his experience following Superstorm Sandy, and outlined what has evolved into a "really outstanding partnership" between industry and government. Since 1955, a voluntary agreement between all electric companies has been in place; whenever a major event occurs, unaffected companies seek to provide assistance to neighboring utilities. Superstorm Sandy severely tested this structure, he stated. Tom Kuhn, President of EEI, realized a need to coordinate with government in addition to their industry, and engaged a process to work closely with the Department of Energy.

After Sandy, President Obama removed the red tape to help industry mobilize and respond quickly, and requested that a representative from each trade group take a post at FEMA—an assignment Owens took on for EEI. The response center was initially in chaos, said Owens, and they had to cope with problems as they came up, such as running out of fuel and getting Canadian relief crews over the border without the 2-day drug testing process. 8.5 million people were without electricity, and industry and government mobilized 67,000 people to aid in the restoration effort.

The level of cooperation between industry and government was tremendous, said Owens. Since then, EEI, industry, and government have engaged in discussion about how to improve response capabilities; all agree that an industry representative should be embedded in the government's emergency response center. EEI characterized Sandy as a national response event – affecting a significant portion of the population and multiple regions – requiring coordination of leadership from different companies to allocate resources in a safe, efficient, transparent and equitable way, to help provide oversight, and to coordinate with the federal government; EEI has taken on the role of central coordination. The energy industry is working on internal improvements, including creating a "national mutual assistance resource team" to coordinate the regional mutual assistance teams who aid one another during emergencies.

Craig Miller, who runs a research program at the National Rural Electric Cooperative Association

(NRECA), raised the question: Is the grid itself the right grid to be resilient? The grid was created in 1893 when the US started building large generating plants, big turbines with lots of angular momentum that sent out tremendous power at high voltage. The grid was uncontrolled from 1893 to about 1983, but over the past 30 years the nation has moved toward active control.

Miller asked what does the future grid look like? In considering how to make it more resilient, a metaphor often used is building castles—erecting big walls and protecting everything. NRECA believes the grid of the future is more like a ninja—agile and responsive to what is happening with more dynamic control. The future grid should incorporate advanced communications, advanced analytics, and data management that will evolve to handle an actively controlled grid. Given the large amount of cyber attacks on utilities each month, prescriptive cybersecurity that tries to anticipate and fend off every type of attack will not work; the next generation of cybersecurity has to be super reactive, identifying the fingerprints of a hack and reacting to it instantly.

Jay Apt, Carnegie Mellon University, presented data on the causes and duration of blackouts, including his own analysis of large blackouts between 1984 and 2009. Some involve system-related factors, and a few were from intentional attack, but most blackouts were caused by natural hazards.

It is likely restoration time can be reduced, he said, but unlikely that we can make the grid invulnerable. A different way of looking at it is through the concept of survivability, the ability of a system to fulfill its missions in a timely manner in the presence of attacks, failures, or accidents. To paraphrase, he said, "You are going to lose electricity. Get over it." In other words, use approaches that take pressure off of the grid. One approach is to use a distributed generation system that can move power to essential loads—e.g. police, gas stations, hospitals, and cell towers—and take nonessential loads offline. Another is to ensure that essential services have backup systems. There are many ways to maintain essential services when grid power is out and these ought to be part of the plans.

Cybersecurity

The next panel explored strategies to improve the resilience of the distribution system to cyber events. **Arthur House,** Connecticut Public Utilities Regulatory Authority, stated that the existing grid and distribution system are extremely vulnerable to cyber threats, and probably will continue to be vulnerable even with decentralization. The risk of a successful attack is significant, he stressed. Many natural hazard threats are predictable, and preparation is a question of practicing what you know is likely to happen. What will happen after or how to prepare for cyber threats is not well understood; there is no playbook for a cyberattack. There is also fear that a cyberattack would be launched simultaneously with a physical attack or a natural disaster.

Utilities generally employ cyber experts that understand cyber threats more than state regulators; regulators are in a new arena and they need to earn the trust of utilities. House proposed that solutions could be supported if utility commissions suspended the normal relationship between regulators and regulated, and discussed standards to strengthen the ability of utilities to defend against cyberattacks. Once standards are established, a third party could conduct audits to assess progress. Finally, the public should be briefed on the results so they understand the strengths in the system and are assured that weaknesses are being addressed.

Scott Baron, of National Grid, a public utility in the northeastern US and the United Kingdom, spoke about evolving cyber threats to the modern grid, and modernization efforts to make the grid more efficient, connected, automated, reliable, and capable of healing itself. National Grid's biggest concern is information technology embedded within operational technology. In a data center, substation, or control center, there is a "black box" containing a full-fledged PC with an operating system susceptible to hacking.

Managing threats means embedding security within grid modernization, which requires investment in a mature information security program. We need to partner with the company's business and operations departments to ensure that they understand the principles of information security and that we are supportive of their efforts, Baron said. We do not try to secure the business; we enable secure business. Public and private partnerships are needed to promote information sharing. Lastly, regulation should be embraced and supported, which can help give people within organizations leverage to implement cybersecurity programs.

Microgrids and Distribution Systems

The third panel focused on microgrids and distributed resources. **Erich Gunther,** of EnerNex, an electric and power engineering and consulting firm, discussed two microgrid projects—a utilities-side microgrid and a customer-side microgrid—to illustrate their differences.

The utility microgrid project, undertaken in response to Hurricane Irene and the 2012 snowstorm in Connecticut, was developed as a high-level micro design, a conceptual architecture that could be used as a pattern for utilities-side microgrids and related projects. The initial objective was to support critical facilities – e.g. police, fire stations, emergency response, and shelters – to ensure that energy and security were available for first responders, and to have situational awareness immediately after an event. An additional objective focuses on socioeconomic continuity after the immediate response, providing support to keep people and business in the community. Unlike customer-side microgrids, utility-side microgrids use the utility's expertise and discipline to maintain systems. However, challenges exist with how to recover costs, and in many states utilities can own the microgrid but not the generators.

EnerNex is also working on a customer-side microgrid for a corporate campus in Cupertino. The vision for the microgrid is to achieve business continuity with a system that pays for itself and supports environmental stewardship. The primary driver was the capability to be fully operational for 1-2 months following an earthquake. Given the high employee productivity and revenue generation, the business case for the microgrid was easy to make, unlike for a utility microgrid.

Gunther stated that utility side solutions could be very effective, taking advantage of the utility's expertise to provide safe, reliable power to their customers. The challenge is who benefits, who pays, and how that works into the rate case, since the current regulatory compact does not support investment to implement these systems. The customer side solution focuses on an individually tailored business case and provides energy security. Both of these systems are more complex than traditional approaches, are capital intensive, and require new skills and design tools to be implemented and operate effectively.

Richard Kidd, deputy assistant secretary for Energy and Sustainability of the U.S. Army, said the Army is the country's largest utility consumer. The Army views energy in three dimensions: soldiers, vehicles, and bases; in all three, the focus is on the integration of information technology and energy. New technologies are tested at home and abroad in combat theaters and domestic environments to reduce the vulnerability of the Army's energy supply chain, whether from war, weather events, or cyber or physical attacks. In addition, the Army engages in large-scale renewable energy projects.

Kidd outlined current projects to develop microgrids. At the individual level, the Army is developing technology that allows a soldier to become his or her own microgrid. Given the immense amount of battery-dependent equipment soldiers' carry, the Army seeks to enable soldiers to generate their own power. At a tactical level, the army has developed microgrids or hybrid energy systems to power combat stations, reducing the need to continuously supply generators. Finally, the Army is building installation microgrids at armed forces bases through the DOD effort, SPIDERS. At these sites, critical loads are identified and ways to service them from microgrids are tested. At Fort Carson, Colorado, the headquarters has been islanded and is serviced off a microgrid. Electric vehicle programs powered by microgrids are being installed at various sites. Lastly, Kidd noted that the Army has the capacity to partner with energy companies to support innovative solutions for energy security and renewable energy. In Hawaii, they provide Hawaiian Electric Companies (HECO) with land and long-term demand; in exchange HECO is building a microgrid to support Schofield Barracks.

Anu Narayana of Rand Corporation outlined work to develop a strategy for protecting essential critical services in the event of a long-term power outage over an extended region, and some known implementation barriers and associated costs. Narayana noted that grid failure is costly economically, and for health and safety. While hardening is important, what people really care about are the services from electricity. Narayana demonstrated a scenario in which there is a blacked out high-voltage transmission system and an islanded network of distributed generation units and customer loads with one point of connection to the main grid. The idea is to develop a strategy so a subset of critical services that depend on power can continue to operate.

Services kept in operation have to be suitable for a microgrid style operation, and not all services

have to be in operation all the time she noted; there could be load cycling that occurs within the self-selected island. For example, one police station in the region could be powered at full capacity at night and at half capacity during the day. Schools could operate in shifts. The community would make these decisions; rather than relying on one management strategy, every community would prioritize an approach that meets their needs.

The incremental cost on top of existing distribution automation infrastructure was found to be about $1.80 per month—less than 3 percent of the average monthly electric bill. However, legislative and regulatory barriers exist; in almost all states microgrid members are not able to share power through wires owned by utilities. In addition, there is little incentive for utilities to invest in these approaches. As a way forward, Narayana pointed to demonstration projects in Connecticut, and suggested that these types of projects can inspire confidence in the technology and address existing challenges to their use.

Chuck Agosta from Clark University shared his project to create a "nanogrid" on campus; one he hopes will eventually take over major buildings at the university. The project started with students' interest in charging their cell phones with solar energy, they began with a solar panel system that ran a bank of eight USB charging ports. The project grew in scope and there are now plans to convert three classrooms to a renewable energy nanogrid, with solar panels and a wind turbine built by students. The system will include storage capabilities so it is a semi-autonomous grid; there will be grid-tie to maintain reliability.

The local utility, National Grid, became very interested in this project because of its potential to boost energy efficiency. If the project can demonstrate its economic feasibility by finding ways over and above energy efficiency to get a good return on investment, more companies could be convinced to participate. Partly because of that, off-the-shelf components were used; technology that can be implemented right now. Lessons learned included recognition that some old technology will have to be left behind, for example traditional light fixtures do not work well with LED lighting, and there are advantages to concentrating electronics in one place. Lastly, interesting questions emerged about the interaction of the campus microgrid with National Grid and energy storage; there is potential to run the campus without additional energy from National Grid, but this presents topology questions that require further investigation.

Selecting Effective and Cost Effective Distribution System Resilience Building Strategies

Morgan posed the questions: If one was going to adopt strategies for making distribution systems more resilient, how should we decide which option to use? Who should use them? How might we best pay for them?

Diane Solomon, New Jersey Board of Public Utilities (NJBPU), recounted her experience following Superstorm Sandy, which impacted 71 percent of New Jersey's electric distribution systems, leaving 2.8 million without power. In the aftermath, there was a large cross-agency effort to build energy resilience of critical facilities throughout the state. NJBPU worked with the Office of Emergency Management, New Jersey Office of Homeland Security and Preparedness, and the Department of Environmental Protection; from a request for information, almost 800 resilient energy projects were identified in 425 municipalities, counties, and government agencies.

NJBPU collaborated with other state and federal agencies and the National Renewable Energy Lab to identify ways to enable critical facilities such as hospitals and wastewater treatment plants to operate without prolonged disruption. Potential approaches include combining distributed generation technologies with microgrid technologies, solar photovoltaic fuel cells, and combined cycle waste energy. The board also set up an energy resiliency bank to provide financial and technical assistance for projects to enhance resiliency with $200 million provided by a community development grant. Areas of focus include wastewater facilities and a microgrid that can island itself and operate the PATH trains to New York. Solomon closed with strategies to adopt in the wake of a storm like Sandy, noting the importance of communicating information to the public, measures that help locate problems quickly, and the need for transparency and partnership between local government and utilities.

Cheryl Roberto, Environmental Defense Fund, raised the questions, how might society decide which options to follow from a macro-economic sense? How should things be paid for? As a former regulator, she said that cost causation still makes sense. If pieces of the grid can be appropriately valued, there can be better flow of cost causation for tariffs. She pointed to an issue raised by Anu Narayana, that a barrier to

using microgrids was the inability to use power lines in a utility's grid. That should not be a problem, she stated; we should figure out the cost to that asset, and apply a tariff. Identify how to make use of the monopoly assets that are available for public benefit, put a proper economic price on it, and put it out there, said Roberto.

She raised questions of how to improve coordination between players and how to alleviate legal and regulatory obstacles. One approach may be to redefine utilities from a utility that delivers kilowatts as a commodity to a public benefit that provides an energy services platform. We want to see a nimble, resilient grid that allows all players to play in a neutral way, she concluded.

Miles Keogh from NARUC observed that technology is forcing a change on the system and the kinds of infrastructure and usage. NARUC gathers regulators, companies and consumer advocates to play a game called "rate-case monopoly," where players make choices about resilience investments, and then a disaster happens that is picked at random. Players have to live with the investments they've made. One of the "disasters" is that nothing bad happens and you invested in resilience building; what do you tell your governors and ratepayers? It was discovered that people find it very difficult to accommodate a sense that the sector is changing as they make investments, even if they are told it is changing. To address this challenge, Keogh said, there is a need to assimilate commonly used risk-management tools from other sectors, and build these tools into how utilities regulate and operate their systems.

Keogh raised the possibility that the value of the smart grid of tomorrow may not be power, but the data generated on the usage of kilowatts by millions of rate payers because of that data's predictive value and value for behavioral analytics. Although payment of electricity will not be eliminated, we will see whole new business models and revenue streams, which in turn will radically change regulation.

The final speaker, **Kevin Jones,** the Institute for Energy and the Environment at the Vermont School of Law, shared a project looking at smart grid technologies and policies with a focus on resilience, for example, with urban microgrids. To get utilities to invest in such projects, there need to be clear public policies and a way to ensure that utilities can recover the costs and expect reasonable returns, he said.

The first thing that needs to be done is to identify public policy objectives and benefits, and specific reliability criteria that should be met. For example, one approach is to identify critical facilities that need to operate during an emergency and develop a plan to preserve them. Alternatively, the goal might be maintaining similar outage statistics given the new spate of severe weather. Once goals are set, how to collect money to fund investments can be examined, Jones proposed; possibilities include recovering costs through planning tariffs or, if focused on maintaining critical facilities, through local charges.

Participants: W. Terry Boston, PJM; **Billy Ball**, Southern Company; **Dan Ton**, U.S. Department of Energy; **Paul W. Parfomak**, Congressional Research Service; **Ronald Turner**, Analytic Services Inc.; **John Kappenman**, Storm Analysis Consultants; **Mark F. McGranaghan**, Electric Power Research Institute; **Emanuel Bernabeu**, Dominion Virginia Power; **William H. Sanders**, University of Illinois at Urbana-Champaign; **Paul Hines**, University of Vermont; **Ellen Lapson**, Lapson Advisory; **Paul N. Stockton**, Sonecon, LLC; **Patrick Hogan**, PG&E; **Jeffrey Williams**, Entergy Corporation; **David K. Owens**, Edison Electric Institute; **Craig Miller**, NRECA; **Jay Apt**, Carnegie Mellon University; **Arthur House**, State of Connecticut Public Utilities Regulatory Authority; **Scott Baron**, National Grid; **Erich Gunther**, EnerNex; **Richard G. Kidd IV**, U.S. Army; **Anu Narayanan**, RAND Corporation; **Charles Agosta**, Clark University; **Dianne Solomon**, New Jersey Board of Public Utilities; **Cheryl Roberto**, Environmental Defense Fund; **Miles Keogh**, National Association of Regulatory Utility Commissioners; **Kevin Jones**, Vermont Law School.

Planning Committee: **M. Granger Morgan** (Chair), Carnegie Mellon University; **Erroll B. Davis, Jr.**, Atlanta Public Schools (Retired); **Colette D. Honorable**, Arkansas Public Service Commission; **Charles D. Gray**, National Association of Regulatory Utility Commissioners; **Mark F. McGranaghan**, Electric Power Research Institute.

NRC Staff: Lauren Alexander Augustine, Director, Program on Risk, Resilience, and Extreme Events; **John Holmes**, Associate Board Director, Board on Energy and Environmental Systems; **Sherrie Forrest**, Program Officer, Program on Risk, Resilience, and Extreme Events; **John Brown**, Program & Administrative Manager, Program on Risk, Resilience, and Extreme Events; **Jamie Biglow**, Senior Program Assistant, Program on Risk, Resilience, and Extreme Events.

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.
www.national-academies.org