IssuesLetter

Electrical Energy Security: Policies for a Resilient Network

Part II

April 2002

For the third time in a generation, our nation is focusing attention on the thorny questions of national energy security. This time, however, it isn't just concern about fuel shortages and price spikes; it is also about the potential impacts of deliberate attacks on energy facilities, including the nations power plants and electric grids. Regulators and other public officials must now assess and seek to limit the effect of these new risks, while keeping an eye on the enduring goals of utility management, including power system costs, reliability, and environmental impacts.

In the companion Issuesletter, Assessing Security Risks, we discuss how electrical energy security involves a web of interconnected elements, from the security of individual power plants to gas pipeline supply routes and the architecture of regional transmission grids. In this Issuesletter we highlight policies for regulators and utilities to improve the security of the nations power systems not by building fortresses around large, fragile facilities and trying to defend thousands of miles of long-distance transmission lines but by strategically evolving a more resilient electric network.

What is a Resilient Network?

In the resilient network, physical security is not an added feature, bolted on after power plants and transmission lines are built. Rather it is an integral element of system planning and network architecture with four central features:

1. Inherent deterrence. The resilient network has few critical facilities facilities which, if lost or damaged, would lead to widespread, cascading impacts. It deters attack by offering very few effective targets.

2. Focused protection of critical features. Some electric system facilities (e.g., regional operations centers or key transformer sites) are critical to grid operations, and their loss could have widespread effects. Other facilities (e.g., large hydro stations or nuclear power plants) may not be critical to the grid but are potential threats to the public if damaged or used as weapons. In the resilient network, both types of facilities are few in number, well-protected, and their essential grid functions are supported by back-up facilities.

3. Accent on distributed resources. Widespread use of distributed resources can lower stresses on the electric grid and lower the grids reliance on remote central stations and long transmission links. Just as desktop computers and local area networks have

moderated the central role of mainframe computers, distributed electric resources can lessen the number of hours and the number of facilities where the loss of strategic assets would cause widespread outages or cascading failures.

Energy Security and Grid Security

The topic of this Issuesletter security of the power grid is a subset of a much larger issue, national energy security. Arguably, the greatest threats to the nations energy security are our growing petroleum demands, the risk that dangerous energy facilities will be used as weapons against society, and the long-term risks associated with environmental harms. Blackouts due to grid failures, deliberate or accidental, can also be extremely costly and disruptive. This Issuesletter focuses on policies to protect against such failures and to lessen the safety and environmental risks associated with operation of the electric system. It does not address the larger issues of national energy security.

4. Graceful failure and recovery. The resilient network is designed not to make component failures impossible but to permit failures to occur without catastrophic effects on the essential functions of the system. Thus, when elements of the electric network fail, whether through accident, storm damage, or deliberate attack, the effects of that failure can be minimized in scope and duration. Increased use of efficiency, load management, and distributed generation will limit the effect of individual failures.

The good news is that many of the technologies and policies needed to build the resilient network already exist. The strategies needed to make our electric grids more reliable last summer are largely the same strategies that could make grids more secure today. Fortunately, unlike many new policies the nation will be asked to adopt in response to security concerns, policies supporting increased resilience will not add to the nations total electric bill. In fact, they will save billions of dollars for American families and businesses.

Regulatory Challenges

Regulators do not create power systems; they structure the economic and regulatory environment so utilities and other investors can provide electric facilities and services to meet customer needs and public goals. Power companies, independent generators, and pipeline companies are expected to spend well over one hundred billion dollars on new energy infrastructure in the coming decade. What regulatory reforms are needed to drive this investment in ways that produce a more resilient network?

At the outset, it will be helpful for regulators to appreciate some of the structural and institutional conflicts that complicate regulatory policymaking for electric energy security.

Generation capitalism vs. security socialism. In today's increasingly competitive wholesale power markets, private investors make most decisions about the size, location,

and fuel sources of the nations new power stations. However, the security of the grid and the fuel supply is a matter of broad public concern, and security failures have very large public risk and cost consequences. Investors do not base their decisions on these public concerns. Rather it is generally the government and public, not the generators, who bear those costs and risks.

Many aspects of security are public goods, where benefits are provided to everyone, including those who do not pay for them. For example, long-term investments in renewable energy will reduce the risk to the public of pipeline interruptions and central station outages. Yet if the security benefits of renewables, while shared by all, are paid for by a few, investments in renewables will continue to fall short of our collective needs. Regulatory reforms are needed to assure that private investment decisions reflect the networks security needs.

Conflicting policy paradigms. Improving electric energy security requires increased coordination and strategic decision-making both within the power sector and between the power sector and the government. However, integrated resource planning the principal tool developed by the industry to consider and weigh complex policy objectives like energy security is neither conducted by most utilities nor supervised by most regulators. And larger-scale coordination among utilities has occurred only rarely. Toady's market-based regulatory environment does not provide an easy opportunity to conduct the kind of coordinated analysis needed to advance network security.

The Regulators First Focus: How Much for Security? And Who Pays?

Our nations view of energy security has changed since September 11, 2001. Already there are proposals for significant new investments to upgrade the security of the existing grid, to protect vulnerable facilities, and to ensure that new facilities and systems are built to higher standards. While no reliable cost estimates are available, one can easily foresee total costs for enhanced grid security that rival the stranded costs faced by utilities over the past several years. Regulators need to confront these proposals with two key financial questions: Is this the least-cost option for enhanced energy security? And who should be required to pick up the tab?

Advocates for particular projects are likely to say the costs are justified on security grounds. It is up to regulators to insist upon a process to uncover less expensive and/or more reliable alternatives. When the public is asked to pay for expensive security upgrades, we should use a competitive, technology-neutral approach to permit the most economic and effective strategies to emerge on their own merits. (See box, The Efficient Reliability Rule.)

Who pays for enhanced security is also critical. During the time of vertically-integrated franchises, security costs, like other utility costs, were passed on to ratepayers and governed by state rate-design policies. But we are now in a period of rapidly-expanding generation competition, at least at the wholesale level. Effective competition among generators and distributed resources requires each resource to bear the costs of its own

operation. Security costs, like other generation costs, should be assigned to the cost-causer.

Failure to assign costs appropriately will undermine competitive markets while raising the real cost of electric power to the economy. For example, no one doubts that added security at nuclear power plants is in the public interest, but hiding those costs by assigning them to the National Guard or the defense budget will distort electricity markets, subsidize some consumers at public expense, and displace less expensive alternatives. Moreover, when comparing power supply choices, utility managers, investors, and regulators should take into account the risk that future security costs will ultimately be assigned to higher-risk supply chains and facilities. Our national experience in a number of contexts, from asbestos and black lung disease to PCBs and tobacco, teaches us that it is unwise to assume that the social costs of private activities can be externalized indefinitely.

The Efficient Reliability Rule

Proposed security upgrades and reliability investment decisions that will, by administrative action, impose substantial costs on consumers and other market participants should first be tested by the following standard:

Before socializing the costs of a proposed reliability-enhancing investment through tariff, uplift, or other cost-sharing requirement, the state PUC, FERC, and the relevant RTO should first require a finding that:

1. The relevant market is fully open to demand-side as well as supply-side resources;

2. The proposed investment or standard is the lowest cost, reasonably-available means to correct a remaining market failure; and

3. Benefits from the investment or standard will be widespread and thus appropriate for support through broad-based funding.

To ensure that these standards are met, proposed investments should be tested in an open season bid process that is genuinely open to competitive applications from supply, wires, and demand-side resource providers.

Learning from Experience: Low-Cost Options for Reliability and Security

What are the least-costly ways of improving reliability and security? The power outages, rolling blackouts, and price spikes of the past three years provide useful lessons about what is needed to build a more resilient electric grid in the face of deliberate security threats as well as unplanned reliability problems.

Efficiency and load management -- untapped reservoirs are very large

The National Energy Plan states that, at recent rates of customer load growth, we will need to build more than 390,000 MW (the equivalent of nine new Californias) of new generating capacity by 2020, along with the gas pipelines, power lines, and fuel supplies to support them. However, numerous studies show that between 30 and 50 percent of this demand growth could be avoided by cost-effective investments in energy efficiency, load management, and distributed generation. Demand-side programs run by hundreds of electric utilities over the past two decades delivered almost 30,000 MW of demand reduction at a cost of 2 to 3 cents per kWh saved, before they were ramped down in the move to restructuring. Californias recent experience is especially instructive. Following the blackouts and price spikes of 2000-2001, in the summer of 2001 the state and its utilities launched an intensive conservation and load management effort. In just a few months, overall electric consumption was cut by six percent, and peak load was reduced by an average of 10 percent in the summer peak season.

Customer-based resources can lower grid costs and improve security

At peak load periods, when supplies in the electric system are tight, and power lines are reaching their limits, there is real reliability value to lightening the load on the system. Any reduction in total system demand during peak periods provides reliability advantages, but actions in load areas remote from generation are especially valuable. Demand reductions and distributed generation provide more available capacity to absorb any unexpected shock, ranging from the routine, innocent failure of a transformer to a maintenance mistake at a power plant to an intentional disruption of power supply.

Distributed generation, in particular, carries an additional positive attribute because it allows the grid to separate into smaller islands during a system failure. Distributed generation can provide a network of small power sources in urban areas and supplement traditional central station units, which will (at least for the currently foreseeable future) still provide the bulk of our power supply. In the future, all of these resources might be linked by a smart network of web-based and wireless controllers responding to load and market conditions. However, grid reliability and security can be enhanced today, even without a high degree of real-time integration, simply by the gradual displacement of large and remote power sources with smaller resources closer to load.

The times when demand-side and distributed resources will be most effective in addressing security concerns are also the times of greatest financial value. In most power systems, 10 percent of installed capacity is needed only one percent of the hours in a year. During those few hours, wholesale market prices are at their highest, reserve margins are at their lowest, and the grid is most vulnerable to unplanned disruptions. Distributed resources can deliver greater reliability and security, while lowering power costs.

Renewables reduce fuel supply and cost risks

American consumers are all too familiar with the steep rises in fossil fuel prices that can follow periodic disruptions in global or local energy markets. But price is not the only potential problem. For example, nuclear power is subject to the risk that problems at one facility will require operating changes throughout the fleet. The rapid expansion of gas-fired generation puts considerable pressure on the nations natural gas delivery system, creating new points of vulnerability. Because electric generators cannot store large quantities of gas, pipeline interruptions also directly affect electric system reliability. For example, an explosion on the El Paso pipeline in Carlsbad, New Mexico, early in 2001 took electric generation off line in California and helped trigger rolling blackouts. In New England, where 10,000 MW of new electric generation are now being added, 77 percent of the regions pipeline capacity may be committed to power generation, and the potential loss of compression in the regions pipelines will soon become the largest single contingency that reliability planners must face. There, as elsewhere in the nation, the overall level and pace of gas-fired additions to the grid stresses the capabilities of the gas delivery system and exposes the electric system to new pipeline and gas supply risks. The resilient network should diversify and lessen fuel supply risks by actively promoting investments in demand management and renewable sources of supply.

Making the Right Choices Policies for the Resilient Network

So what can regulators do to tap the value of efficiency, load management, and distributed generation at millions of locations on the grid? A number of policy and market reforms are needed, from the structure of wholesale regional markets to distribution utility planning and customer incentives for load response and energy efficiency.

1. Require utilities to analyze the reliability benefits of lighter loads and more distributed resources

The key to the resilient network is a design architecture based on lighter loads and more distributed resources. As a first step, regulators should require utility engineers to model regional and local grids at different load levels and identify the critical facilities (power plants, transmission links, and key substations and control centers) whose loss would cause serious reliability problems in a city or region. Three different types of critical grid facilities should be identified: a) those few key facilities that must be actively secured against deliberate attack; b) those that can be supported by strategic investments in power supply or transmission (for example, adding power lines to change a radial system into a more stable network.); and c) those that can be rendered less critical through investments in efficiency, load management, and distributed resources. Limited security budgets should be focused very strategically. (See Box, What About Protecting Key Facilities?)

2. Support increased efficiency and encourage demand response in power markets

A host of policy options are available to utilities and policymakers to accelerate cost-effective demand management. The most important options are: building codes and appliance efficiency standards; system benefit charges, utility efficiency programs, and other sources of funding for efficient end-use technology; demand-side bidding, price-responsive load and other tools for enhanced demand response in regional power markets; ratemaking plans for utilities that eliminate the utility's profit incentive to promote sales (most promising are performance-based plans using revenue caps in place of price caps); and rate designs for retail sales that encourage customers to shift consumption away from high-cost power periods when reliability is usually most at risk.

3. Adopt rules that simplify distributed generation interconnections and allow distributed resources to displace more expensive T&D upgrades

Distributed resources can improve reliability and forestall very expensive upgrades at the substation and local distribution level. Utility and environmental regulators now possess a number of effective tools to support increased investment in cost-effective distributed generation. The most important are interconnection standards and distribution utility policies such as distribution-level planning, targeted efficiency programs, distributed resources development zones, and de-averaged buy-back rates that reveal the full value of distributed resources in different locations. Improved wholesale market rules should permit small generators to compete with central station units to provide energy, capacity, and ancillary services in wholesale power markets. Output-based environmental standards are also needed to promote fair competition among distributed generators without degrading local environments.

What About Protecting Key Facilities?

No matter how the electric system is designed, there will be a need to protect critical grid facilities (e.g., a key substation, the loss of which would blackout a city; or a system operations center) and those energy facilities (e.g. nuclear power plants, large hydro sites) that pose risks to the public if sabotaged. Each of these facilities will require protection, and we will have to try provide it. How well this can be done is subject to debate. The fact that it will be expensive seems a foregone conclusion.

An important objective should be to design a system that has fewer of these critical points and for fewer hours of the year, and every effort should be made to avoid creating new facilities requiring expensive security protection.

System redundancy is an expensive option that should be pursued sparingly, although it may be cost-effective in some circumstances. New England, for example, has kept in place its pre-ISO control centers as backup facilities to the NE-ISO, which can be called on if the ISO control center in Holyoke is lost.

4. Adopt policies that diversify fuel supply risks

Overdependence on fossil fuels generally, and on natural gas in particular, increases both security and price risks. A conscious strategy of diversified resources adding meaningful proportions of renewables, combined heat and power, and high-efficiency combined cycle generation to the electric grid will make the power grid more resilient and improve the nations energy security. Renewable portfolio standards, system benefit charges, and green power options are some of the best options available to regulators.

In addition, it appears that the vast majority of electric customers will be served by traditional franchises or default service providers for some time. For these customers, regulators need to ensure a balanced resource mix through utility resource planning or portfolio management that meets long-term public goals, including price stability, environmental quality, and energy security.

Conclusion

The strategies supporting the resilient network address the nations need for improved grid security. They will lower the number of hours when and the number of physical locations where the grid is close to capacity and the loss of a critical link or facility would have significant consequences for a city or region. But it is also important to see these policies as a no regrets security strategy. Resources devoted to the resilient network will have additional multiple benefits: enhanced reliability to survive heat storms and other weather events; significantly lower capital costs; reduced environmental impacts; and lower stresses on the entire network from distant generators to the neighborhood substation and distribution line. Underinvestment in the resilient network will waste the nations scarce capital on hard assets that are more expensive to run and protect.

References

Cowart, R. 2001. Efficient Reliability: The Critical Role of Demand-Side Resources in Power Systems and Markets, National Association of Regulatory Utility Commissioners, June 2001. http://www.raponline.org/Pages/Reli.htm

Regulatory Assistance Project, 2001. Distributed Resource Policy Series: http://www.rapmaine.org/Pages/Disco/distribution.html