IssuesLetter

Electrical Energy Security: Assessing Security Risks

Part I

April 2002

Among the many issues facing utility regulators there are two, often competing ones: What does it take to keep the lights on? And what does it take to keep rates at a reasonable level? Ongoing changes in the electric industry have challenged the ability of regulators to adequately address these questions. Assuring that system security risks are understood and addressed only adds to the challenge. Can we afford the security costs required to protect a system designed with large, remote generation and an associated transmission network? Alternatively, can we migrate to a more robust system with greater security that relies more on distributed resources and energy efficiency?

Closely related to these questions is a third concern, that of environmental consequences. Can security goals be met with resources that minimize adverse environmental impacts?

In this first of two Issuesletters discussing security-related questions, we examine the nature of security risks to the nations electric infrastructure. In the companion Issuesletter, Electrical Energy Security: Policies for a Resilient Network, we suggest regulatory approaches and policies to support a more resilient electric network.

What We Mean By Security Risk

The term security can take on different meanings depending upon the context. There are risks associated with intentional disruption of the system (sabotage), and there are operational risks of the system (whether from physical failure of the plant, human error, or market-based instability). Both can pose short- and long-term national security risks for the electric grid. For example, in the very long run, we face security risks associated with the potential loss of low-lying land areas to greenhouse gas-induced oceanic flooding. Both types of risk and the methods for mitigating them are driven by the existing resource mix and the resources yet to be added to the system. In addition, any plan to address security must assess the consequences of a security failure. For instance, catastrophic failure of a nuclear plant carries serious consequences not associated with sabotage of a wind farm, even though it may be easier to attack the wind farm. We discuss here the security risk characteristics of different technology choices.

We have already experienced the effects of making decisions based on risk. For example, as a nation we have essentially abandoned oil as a backup fuel for both economic and environmental reasons. The new generation of combustion turbines will not run on oil which means that oil is no longer an option for a growing percentage of our generation

supply. As a result, we are ever more dependent on the gas supply network, a network with its own set of security risks, which carries more energy than the electric system. With the gas basket carrying more and more of our eggs, there is perhaps already more risk concentration than prudent risk management would dictate.

As utilities and regulators come to grips with todays realities, one crucial conclusion stands out the nations electric infrastructure will be made more secure by investing in a resilient network architecture. Energy security (and relieving pressure on the grid) will come from a network with much more energy efficiency and distributed resources than it will from building fortresses around large, fragile facilities and trying to defend thousands of miles of transmission lines and gas pipelines. The good news is that many of the technologies and policies needed to build this resilient network already exist. Strategies that made our electric grid more reliable in the summer of 2001 will make the grid more secure in 2002 and beyond.

Historical Measures of System Operation

The electric grid has generally been constructed and operated under a standard to maintain uninterrupted operations, even with the loss of the largest single resource on the system (generation, a substation, or a transmission line). This is the N minus 1standard, where N represents the sub-parts of the whole system and minus 1 represents the loss of the largest single resource (contingency) on the system. This is an operational engineering standard, set by engineering criteria. Traditionally, both operators of the system and regulators came to view this standard as being the same as an assessment of the risk of system failure, since it was deemed highly unlikely that more than one part of the system would fail at the same time. From an operational standpoint, this is likely to continue to be the criterion.

However, the underlying assumption does not hold true in the face of multiple external forces, whether intentional acts of sabotage or the confluence of independent events. For example, in 2001, California had an N minus 3 (or worse) condition: the loss of the El Paso natural gas pipeline (accidental explosion), a significant reduction in hydro imports from the Northwest (drought), and unscheduled outages from other generators. Such events, as well as concern over sabotage, raise the questions of whether all is being done to reduce the risk profile of the electric grid or, more importantly, whether we are making the most cost-effective and prudent choices to reduce the risk profile.

Many Dimensions of Security

The events of September 11 have changed our view of energy security. Whether from terrorist attack, natural disaster or equipment failure, the interconnected nature of our electric system creates a broad array of risks. The electric grid offers a soft underbelly at nearly every turn, thus raising serious security risks, with potentially costly solutions.

From wellhead to mine mouth to meter, the electric grid and gas pipelines are accessible and vulnerable to saboteurs and are also subject to physical failure. There are no reliable

cost estimates of what would be required to protect all electric facilities from any possible attack or failure. However, the magnitude of costs to increase protection through partial measures, such as redundant power lines, could rival the stranded costs faced by utilities over the past several years. Addressing this means state regulators should aggressively assess a full array of alternatives to achieve societys required security goals and strategies.

> Every effort should be made to define security goals in technology-neutral terms allowing the most economic and effective strategies to emerge on their own merits.

Assessing Security Risks

There are a variety of issues to consider when developing the most effective and cost-efficient method to meet security goals. Multiple dimensions need to be assessed, including on-site security for physical plant, proximity to load, fuel-associated risks, consequential costs, facility size, geographic issues, technological vulnerability, and the time horizon for risk avoidance.

Table 1, summarizes the security risk characteristics discussed below for different technology choices and reveals that two key technology groups should play a significant role in improving electric system security distributed generation and energy efficiency.

Table 1: Security Risks by Technology

Facility Type	Site Risk	Proximity Risks	Fuel Risk	Consequential Cost Risk	Size Risk	Geographical Risk	Technological & Multi-Systems Risk
Large Remote Generation	High	High	High	High	High	Low	High
Large Local Generation	High	Medium	High	High	High	Low	High
Transmission	High	High	N/A	High	High	Medium to High	High
Distribution	Medium	Low	N/A	Low	Medium	Low	High
Distributed Fuel-Based Generation	Low	Low	High	Low to Medium	Low	Low	Low
Remote Renewable Resources	Low	Medium to High	None	Low	Low	Low	Low to Medium
Distributed Renewable Resources	Low	Low	None	Low	Low	Low	Low to Medium
Energy Efficiency/DSM	Negative	Negative	Negative	Negative	Negative	Negative	Negative

Site Security Risks. Each type of resource carries its own site security risks. A nuclear unit, because of the magnitude of environmental damage that might result from an accident or attack, requires extreme security precautions that are likely to be very expensive.

Distributed Generation (DG) and energy efficient technologies such as Combined Heat and Power (CHP), on the other hand, because of their small size and customer-premise locations, will be easier to secure and less catastrophic to the economy should they fail. They are less visible to would-be attackers and are much smaller in scale. Individually, each small plant has a low impact on the grid, and they are often located within more secure areas.

Distributed renewable resources are a subset of DG and carry a low-risk profile for each wind turbine, biomass plant or solar array. They are more difficult to attack (many small targets vs. a few big ones) and a less attractive target.

Proximity of Resource to Load. Resources close to the loads they serve are less dependent on other parts of the system and thus are inherently more secure; resources placed at the load, especially on customer premises, avoid certain risks altogether. This means that every transmission line, substation, or distribution system feeder that can be avoided is a risk avoided or reduced.

A 300-mile long transmission line from Palo Verde in Arizona to California presents a far higher risk profile than a 10-mile line from a suburban Philadelphia generator to downtown loads, although both are easily accessible to saboteurs. One is remote, the other is not. One is long, the other is not. Moreover, it is much more expensive to provide the 300-mile transmission line with a redundant alternative path than it is to duplicate the 10-mile line, and alternative paths carry much the same security exposure as the primary path.

Greater proximity of generation to load also increases the ability of the system to effectively island itself in the case of system failure.

Fuel Delivery and Storage Risks. Support systems like fuel delivery and storage need to be considered when assessing the security profile of a resource. For example, a baseload coal unit dependent on train deliveries is subject to risks associated with the railroad system, while distributed PV systems avoid comparable risks.

Supply resources carry varying degrees of fuel source risk. Natural gas as a fuel has clear risks associated with pipeline delivery. A recent study found that the partial loss of a major gas pipeline compressor station could result in the disruption of a number of power plants in the Northeast. (See Steady-State Analysis of New Englands Interstate Pipeline Delivery Capability, Richard Levitan, Levitan Associates, Inc., presentation to the NEPOOL Participants Committee, January 5, 2001). Likewise, California has already experienced the effects of the loss of a natural gas pipeline for an extended period of

time. Wind and solar, though, have virtually no security risk from a fuel standpoint. While both have obvious intermittency risks, in the aggregate, they have a fairly stable and predictable level of fuel availability, and the fuel sources are not vulnerable to the acts of outside agents.

Unintended Consequential Security Costs. Many security strategies may incur unintended but consequential costs. The industrys prior efforts to increase reliability have led to the construction of a system that is heavily interdependent and therefore has higher related security risks than a less interconnected system. We now face the consequential costs of those past strategy decisions.

Consequential costs are similar in nature to the externalized environmental costs of the electric grid, with one extremely important distinction: some consequential security costs, such as redundant transmission, are not likely to be externalized (these costs will show up in the price of power), while others not traditionally associated with resource costs (e.g., the cost of national guard troops protecting nuclear plants or the cost of military operations protecting Middle East oil supplies) will be external to the price of the power. As an example, a decision to move away from remote, mine-mouth coal plants toward large-scale, urban combined cycle combustion turbines (CCCTs) will reduce the dependence on the transmission grid to move power to load centers but will create unintended security risks and related costs from increased dependence on natural gas pipeline delivery systems. Conversely, dependence on remote generation carries with it an increased reliance on transmission systems and large-scale control systems.

Size as a Security Consideration. As the size of a system component increases and proximity to load decreases, security risks increase. A 1000 MW nuclear unit presents much greater risk to the system than ten 100 MW CCCTs or 1000 one MW fuel cells. This is the effect of the N minus 1 standard. Each new resource addition will either enhance or aggravate this problem, depending upon how large the resource is and whether it, in turn, relies on a critically large component of the system.

Geography and Terrain. While all facilities are subject to some degree of natural disaster risk (earthquakes and storms), additional risks can occur because of geography. Transmission lines routed through mountains, forests, or deserts suffer from accessibility risks and exposure to severe climatic conditions (the Alaska oil pipeline) and other natural disaster risks (forest fires). In addition, the accessibility of these facilities makes them easier to attack.

Technological and Multi-Systems Vulnerability. The technological foundation for todays electric grid is increasingly more sophisticated. Recent advances in Supervisory Control and Data Acquisition systems and the proliferation of the Internet have yielded significant improvements in system operational reliability and efficiency. Everything from system dispatch to generation synchronization relies on these new technologies. These advances, however, open the system to new kinds of threats. Because the system is computer controlled and relies heavily on information transmitted either over the Internet or over the power lines themselves, the electric grid can potentially be brought down by

computer failure, computer hackers, program crashes, or inadvertent keystrokes.

In addition, the increased use of Independent System Operators, greater operational independence of the generating sector especially in availability and maintenance decisions and the presence of greater market volatility can combine to raise the risk characteristics of the system. The greater sophistication and increased interdependence of these disparate systems mean that there are new, non-engineering security risks that must be recognized. What resources we use from among transmission, generation (large and small), and efficiency, how they are added to the system, and how they affect one another will determine whether we increase or decrease these risks with each new resource addition.

Time Horizons

There are also time dimensions to security. The first assesses when security risks are greater, which is usually at times of system peak or stress, when the loss of key facilities would be more difficult to overcome. This is also the point when the least defensible segment of the system transmission represents one of the largest hazards on the system. Reducing the size and duration of peak periods through strategic efficiency investments can effectively reduce system vulnerability.

The second assesses the time horizon over which the system should be secured. Should the system be designed to withstand the loss of major components for a day, week, month, or year? As a general rule, as the time standard is lengthened, the costs will rise. For example, short-term security risks can be hedged with on-site fuel storage for non-renewable DG, but if the associated fuel delivery system is out of service, the value of the DG expires with its fuel supply. Increasing on-site fuel storage or hardening the fuel delivery system addresses this problem but only at an increased cost.

The explosion at the El Paso Natural Gas facility took a major gas pipeline in the Southwest out of service for several months. The only viable way to make the system invulnerable to this type of system failure is through redundancy (another pipeline, alternative fuels at the burner tip, or alternative power supplies) or through avoidance (become more efficient so the power is not needed).

Advantages and Challenges of Alternative Resources

Dispersed resources, such as DG and renewable energy, have the effect of reducing the concentration (magnitude of exposure) of security risks. Conservation and efficiency reduce reliance on higher risk portions of the system. Conversely, traditional wires and turbines solutions may hedge risk through duplication, but each such solution also duplicates the security risks associated with those technologies.

Distributed generation can increase system security at competitive costs. Already DG should be as competitive as alternative generation at peak times, a key security period. If the prices for traditional resources reflect their true security enhancement costs,

economics should further induce DG selection. To be effective, however, DG must achieve higher penetration rates on the system. It will take a long-term policy commitment on the part of our nations leadership to capitalize on the potential of DG.

In the long run, DG could even replace large-scale, remote generation if comparable emission and efficiency levels can be achieved. In the near term, DG is likely to be used to manage peaks in the system, allowing large-scale units to provide base load energy. A balance between the two would spread security exposure across many locations, making any attack necessarily more difficult and, at the same time, less effective.

Any DG that can serve its host-customer during a system failure reduces security risk for that customer. However, because of the general safety design of interconnections, customer-owned DG will disconnect during system disturbance or failure. When operating during an emergency condition, however, its presence may help maintain sufficient system stability to avoid a failure in the first place. The disconnection phenomenon limits the value of DG in these circumstances but does not undermine its other security characteristics.

The Special Case of Nuclear Power

The Nuclear Regulatory Commission is charged with protecting the public from nuclear damage whether from accidents or acts of sabotage. It has used a design basis accident criterion for determining the construction, operations, and disaster response requirements for nuclear plants. While September 11 involved nothing nuclear, its implications for terrorist events are dramatic.

Vulnerability of nuclear plants to large aircraft must be reassessed, as well as assumptions about truck bombs, armed attack, and sabotage from within. Strict adherence to security requirements must be assured a change from previous times when power plants failed their security drills.

Ultimately, increased security with increased costs is sure to come. One significant cost of nuclear power already externalized to electricity costs is the Price-Anderson limit on liability for a catastrophic accident. Other costs that are likely to be external to the cost of nuclear power are military protection of facilities and perhaps even armaments. While most would concede there are national security interests at stake, the fact remains that societal costs are incurred and will be incurred for nuclear power that should be considered within the regulatory context.

Choices to increase or maintain nuclear power as an option should be weighed together with the cost (internalized or not) of related security requirements. Regulators remain at the crossroads of these decisions.

Renewable resources have special attractive attributes. Renewable resources are more modular, even when developed in a centralized situation. Most biomass and geothermal

plants are less than 100 MW. Wind turbines are physically separated and thus stand as separate risks. Fifty MW of wind turbines in one wind farm cover a large area. The loss of a single turbine has minimal impact on the system, and there is no fuel supply delivery system risk.

On the other hand, some renewable resources like PVs remain costly when compared to traditional resources. However, the cost gap is expected to continue to decrease, and, to the extent deployment is accelerated, the gap should close even faster. Fortunately, other renewable resources, such as biomass, small hydro, and wind can successfully compete with traditional resources. This is especially true if value (or cost) is assigned to the security attributes.

Energy efficiency. Energy not required or consumed has no security risk and may have even have a negative risk profile since lightening load reduces stress throughout the system and thus the security risk profile of the entire grid. Energy efficiency tends to be cost effective and can be implemented relatively quickly and in a targeted way to address specific local concerns. A proven and effective tool for embedding efficiency in our appliance stock is the use of manufacturing standards requiring the production of more efficient systems, equipment, and appliances.

Unfortunately, in many areas, especially where competition has been introduced, successful, utility-sponsored energy efficiency programs have been abandoned or reduced in the expectation that competitive markets would fill the need. Regardless of the status of retail electric competition, barriers to cost-effective energy efficiency remain. Regulators should revisit the issues surrounding energy efficiency programs and maximize the value that can be achieved. The potential benefits are very high, often dwarfing the costs.

Conclusion

The electric industry can pursue two paths. One is a continuation of the existing system architecture, with associated intensive and high-cost security requiring hardening assets that are difficult or impossible to adequately protect. The other path migrates toward a more robust system, with fewer high-intensity security requirements and with lower cost. It is the challenge of regulators and policymakers to put us on the path of achievable, effective security. The first step is to gain an understanding of the relationship between different technology choices and their impacts on security achievability and costs. The second step is to adopt policies to put the industry on the lower cost, higher security path as discussed in our companion Issuesletter, Electrical Energy Security: Policies for a Resilient Network.