Options To Reduce Vulnerability

The preceding chapters have established that U.S. electric power systems, while capable of absorbing considerable damage without interrupting service, are vulnerable to attacks by saboteurs and, to a lesser extent, to massive natural disasters. Damage could occur that exceeds normal utility contingency planning, resulting in widespread, severe power shortages and rolling blackouts that would be extremely expensive and disruptive, and could continue for many months.

The risk that massive damage will occur is not high, but neither is it negligible. International terrorist groups appear to have the capability of mounting a crippling assault, and at some point, they or domestic extremists may see a motivation. Earthquakes and hurricanes more severe than have yet been experienced in the United States are inevitable. Eventually one will cause unprecedented damage to an electric power system, although the random nature of such disasters makes the resulting disruption very uncertain.

Various measures can be taken to reduce vulnerability disruption if damage does occur. The North American Electric Reliability Council has recognized that threats exist, and some utilities have taken action, as discussed in the previous chapter. However, such actions are voluntary on the part of individual utilities. It can be easy to ignore low-risk events, even if they are of high consequence, especially when protective measures are costly.

Given the unpredictability of these types of disruptions and the uncertainty of their costs, it is not possible for a cost/benefit analysis to determine how much protection is worthwhile. The desirability of further measures is a matter of judgment more than analysis, as is the potential role of the government in stimulating greater protection.

This chapter describes the measures that could be useful in reducing the risk. This can be done by:

1. preventing or minimizing damage to the system;
2. minimizing the consequences of any damage that does occur; and
3. assuring that recovery can be accomplished as rapidly as possible.

In addition, the evolution of the electric power system can be guided toward inherently less vulnerable technologies and patterns. Table 6 lists the specific steps.

These measures are presented independently of how they would be implemented or who would pay for them. The following chapter discusses consistent policy packages of these measures that could be undertaken depending on the judgment of the decisionmaker as to the severity of the problem. The packages address the issues of implementation.

PREVENTING DAMAGE TO THE SYSTEM

While it is not possible to protect energy facilities completely, it is possible to deter attacks and limit damage. Measures to reduce vulnerability include both physical changes or additions to electric power facilities and institutional measures. Physical changes include constructing walls or berms around critical facilities and adding monitoring devices to detect unauthorized entry. Some changes may be prohibitively expensive, while others may involve minimal expense.

The transmission network is the part of the power system of greatest concern because it is highly vulnerable to attack, and the consequences can be great. The lines themselves are essentially impossible to protect because they extend over many thousands of miles, often in sparsely populated areas. However, lines can usually be repaired quickly with equipment and materials that utilities keep on hand.

Substations are the part of the transmission system with the most serious combination of vulnerability and potential consequences. Unguarded and unprotected substations in remote areas are as vulnerable as lines, but damaged equipment could take months to replace. The loss of even one key substation could effectively isolate a substantial part of the regional generation capacity from the load centers, posing the risk of long-term power shortages.

Table 6-Options To Reduce Vulnerability

A. Preventing damage
1. Harden key substations-protect critical equipment within walls or below grade, separate key peices of equipment such as transformers, toughen the equipment itself to resist damage, etc.
2. Surveillance (remote monitoring) around key facilities (coupled with rapid-response forces).
3. Maintain guards at key substations.
4. Improve coordination with law enforcement agencies to provide threat information and coordinate responses.
B. Limiting consequences
1. Improve emergency planning and procedures for handling power flow instability after major disasters and ensure that operators are trained to implement these contingency plans.
2. Modify the physical system-improve control centers and protective devices, greater redundancy of key equipment, increased reserve margin, etc.
3. Increase spinning reserves.
C. Speeding recovery
1. Contingency planning for restoration of service, including identification of potential spares and resolution of legal uncertainties.
2. Clarify legal/institutional framework for sharing reserve equipment.
3. Stockpile critical equipment (transformers) or any specialized material (e.g., various types of copper wire) needed to manufacture this equipment.
4. Assure availability of adequate transportation for a stockpile of very heavy equipment by maintaining database or rail/barge equipment and adapting Schnabel cars to fit all transformers if necessary.
5. Monitor domestic manufacturing capability to assure adequate repair and manufacture of key equipment in times of emergency.
D. General reduction of vulnerability
1. Emphasize inherently less vulnerable technologies and designs where practical, including pole-type transmission lines, underground transmission cables, and standardized equipment.
2. Move toward an inherently less vulnerable bulk power system (e.g., smaller generators near loads) as new facilities are planned and constructed.

SOURCE: Office of Technology Assessment, 1990.

Harden Key Facilities

Most substations are enclosed with nothing more formidable than a chain-link fence. Improved fences and gates could delay an attack while guards are summoned by perimeter monitoring systems. However, no fence will delay experienced, dedicated adversaries for more than a few seconds. Hence there seems little purpose in constructing very expensive perimeter barriers unless police or armed guards are stationed at or close to the site. Moderately reinforced fences, perhaps anchored at the bottom and incorporating rolls of barbed tape, would provide some protection against opportunistic saboteurs and vandals, especially if coupled with perimeter alarms.

Protective barriers-walls or berms-could be built around the transformers to preclude damage from off-site rifle fire. Barriers might be particularly valuable in substations at generating plants. Unsophisticated saboteurs might prefer to avoid approaching generating stations too closely because they are manned and often guarded, but appropriate walls would prevent easy attack from a distance. Walls would not stop a saboteur willing to climb the fence and attack from close range, but deterring less aggressive attacks could still prevent the loss of a billion-dollar generating station. Barriers would also limit the damage that could be caused by one large bomb, forcing the saboteurs to plan a more elaborate, risky attack.

The cost of hardening a particular facility depends on the site characteristics and the type of protection required. For example, a sheet metal wall (or building) will hide equipment from view. That might help against vandals, but it would provide no protection against a saboteur with a high-power rifle who knows the equipment is inside and will simply spray the wall with many bullets. A heavier wall, perhaps made of reinforced concrete that can stop rifle fire, would be considerably more expensive. If the surrounding terrain provides high-vantage points, the wall would have to be commensurately high. While no general rule is proposed, crash-resistant fences and a concrete wall would add perhaps $100,000 to $200,000,[1] a few percent of the multimillion-dollar facility cost. Some measures, such as walls, would make installation and maintenance of equipment more difficult. These costs should be included when evaluating the desirability of adding protection.

[1]Derived from The U.S. Army Corps of Engineers, "Security Engineering W@," August 1987, and Sandia National Laboratories, "Access Delay," Sand 87-1926,1989. App. A of the ACE manual lists several vehicle barriers including ditches (about $4/foot), concrete-filled posts ($50/foot), reinforced fences (about $40/foot), etc. For example, a 4-acre site would have a fence of about 2,000 feet. Assuming a ditch on 75 percent and filled posts on the rest, the cost would be $31,000, plus a crash gate at $13,000. In addition, a fence designed to delay attackers on foot, perhaps rolls of barbed tape attached to a standard chain-link fence, would cost about $6/foot, or $12,000. Such a fence would be little deterrence to a well-equipped adversary. More formidable barriers would cost over $20/foot. An 8-inch thick concrete wall around thtransformer would cost $13.50 per square foot. A three-phase transformer might involve a three-sided wall of about 25 feet per side plus an additional 75-foot straight wall to shield the opening while allowing access in case the transformer has to be removed. The wall might be 25 feet high, for a total of 3,750 square feet which would cost about $50,000. The grand total for the example is $106,000.

Utilities in most parts of the country generally have not designed their facilities to be earthquake-resistant, except for nuclear powerplants, yet several regions besides the west coast are vulnerable. Generating stations are particularly vulnerable to earthquakes unless adequately designed and constructed. The central Mississippi valley, the southern Appalachians, and an area centered around Indiana are particularly vulnerable to major earthquakes but are much less prepared than California. Review and appropriate upgrading of existing facilities, and application of appropriate seismic standards to new construction, could avert a major loss of generating capacity.

Surveillance

Equipment can be installed at unmanned, key facilities to detect intruders. Intrusion detection systems include sensors, alarm communication systems, and possibly video equipment to assess the cause of an alarm. Perimeter alarms and motion detectors would alert utility headquarters or police/military units which could instigate rapid, armed response. A rapid response could interrupt an attack and that possibility might deter an attack by a group sophisticated enough to recognize the problem. To be of greatest value, a detection system should be coupled with some sort of physical protection of the main substation components, to reduce the possibility of off-site attack.

A wide variety of intrusion sensors have been developed, ranging from buried pressure sensors to electric field disturbance detectors to fence-motion detectors. None is perfect. All sensors have some probability of failing to detect an intrusion, depending on such specific factors as the installation conditions, weather and geographic conditions. and sensitivity of the sensors. Sensors also may trigger nuisance alarms-i.e., alarms caused by spurious factors such as animals, weather (e.g., wind or rain), background noise, or failure of the sensor itself. Intrusion detection systems may include a closed-circuit television system for remote assessment of the cause of alarms. A detection intrusion system at a substation with a 2,000-foot perimeter would cost on the order of $125,000.[2]

At remote sites surveillance would be less useful because the response would take too long. Saboteurs can cross almost any barrier, leave explosives to destroy critical substation components, and depart within a few minutes. If several teams operate simultaneously at different sites, a utility may know a major attack is in progress but be helpless to do anything about it.

Even at remote sites, however, surveillance systems still would serve two major purposes. Detecting and monitoring unauthorized entry would permit the utility to investigate and presumably discover and disarm timed explosives. Thus the potential damage that one or a few saboteurs can accomplish would be limited to only one or two sites before utilities would have guards out. In addition, some forms of surveillance, such as remote TV cameras, may provide crucial evidence for an investigation even if an attack is successful.

A related issue is employee training to recognize and respond to sabotage threats. Reporting suspicious behavior near key facilities may uncover plans for an attack. **Alternatively,** recognition that sabotage and not natural causes has led to damage may lead to the preservation of evidence.

Guards

Detection and delay will do little to stop a serious saboteur if a human response is unavailable to intervene. A heavily armed response to an actual attack is most appropriate to police or military forces (see below), but private guards can deter some attacks.

Currently, armed guards are used at all nuclear powerplants. As a matter of routine, nuclear plant licensees must develop physical security plans, which include the training and use of guards. A well-trained, armed, and dedicated onsite security force is one of the major elements of a nuclear powerplant security system. Guards are also used at non-nuclear powerplants to monitor employees and visitors and vehicle traffic and for perimeter surveillance. The training and use of guards at powerplants vary by utility. Guards generally are not used at substations.

[2]Ibid. App. A of the ACE manual lists perimeter detector costs ranging from $20/foot for fence motion detectors to $40/foot for infrared systems. For a 2,000-foot perimeter this totals $40,000 to $80,000. A basic control panel would cost around $10,000, including the control unit, power supply, and communication module. AC(7I'V system costs around $30/foot adding another $60,000 to the surveillance package. Personnel to monitor the system would add an operating cost.

The deterrent value of guards depends on their numbers, training, capabilities, and orders as well as on the capabilities and motivations of their potential adversaries and the physical characteristics of the site. Opportunistic saboteurs and vandals may be deterred by even a single, unarmed guard. Ruthless terrorists with the resources to mount a well-planned, violent attack essentially could ignore any force less than a well-trained and motivated group of armed guards. Barriers and surveillance equipment can greatly increase the effectiveness of guards.

Guards are employed in different situations for a variety of reasons: to prevent or detect intrusion, vandalism, and theft; to control people and vehicle traffic; and to enforce rules, regulations, and policies. Although, private security guards perform some functions similar to public law enforcement officers, often wear uniforms and badges, and occasionally carry weapons,[3] their legal authority differs in many significant respects from that of public officers. In general, private security guards have no more formal authority than other civilians in the United States. A private security guard has only that authority which his employer possesses: the employer's basic right to protect persons and property is transferred to the security officer.[4]

Most guards are not armed and can do little directly to halt an attack in progress. Guards are in a much better position to detect suspicious behavior and report it to management or authorities. The ability of local law enforcement to mobilize rapidly in the event of an attack would be critical. In this situation, communication among local law enforcement officials, contract security firms, and the Federal Bureau of Investigation is essential.

The typical training period for most security guards is less than 2 working days. Many guards, including some who are armed, receive less than 2 hours of training. Most guard personnel aren't cognizant of their legal powers or authority. However, this situation may be changing. Because demands on security guards and the potential for legal liability have been increasing in recent years, a growing number of companies and schools are providing security training.[5] The extent and cost of training security personnel employed at electric utility facilities vary by company and by site depending on the degree of risk aversion acceptable to management.[6]

A utility's decision to use guards at a facility would have to address a number of issues: the kind of security coverage needed and costs; the effectiveness of guards in deterring different kinds of attacks; whether to employ in-house security personnel or contract out for guard services on a temporary or permanent basis.

Because many substations are located in remote areas, a related question is how long would it take for contract guards, if not stationed at the site, to arrive after a warning has been received. The rate of deployment would depend on a number of factors, including the circumstances of the event, and the location and resources of the contract security firm.

A utility's decision to employ guards as a security measure also raises a number of institutional issues. One issue is whether the government should grant police powers to utility security personnel. Advantages include increased authority and reduced liability risk. Potential disadvantages include abuse of authority (e.g., unnecessary arrests) and the legal implications of such abuse.[7]

Another issue is who should pay for the additional security. Normally, utility commissions allow utilities to recover security costs. Before additional security measures are taken, utilities and utility commissions will have to agree on what constitutes a valid need and is in the interest of the consumer.

Coordination With Law Enforcement Agencies

Ongoing communication among utilities and Federal, State, and local law enforcement agencies, is essential to reducing vulnerability. Clear lines of communication provide two main benefits. First, they enable law enforcement agencies to warn a

[3]Joseph Arwaddy, Burns International Security Services, Inc., personal communication Jan. 23, 1990. According to Arwaddy, less than 2 percent of security work involves armed personnel.

[4]Charles Schnabolk, *Physical Security: Practices and Technology* (Woburn, MA: Butterworth Publishers, 1983), p. 55.

[5]Ibid.

[6]Arwaddy, op. cit., footnote 3.

[7]Norman D. Bates, "Special Police Powers: Pros and Cons," *Security Management,* August 1989, vol. 33, No. 8, p. 54.

utility of a potential attack, should they learn of such circumstances. Second, they allow the utility and the law enforcement agencies to coordinate armed response plans when attacks occur or seem imminent. If utilities are forewarned that an attack is likely, they can take preventive measures such as temporarily increasing spinning reserves or stationing guards at important facilities.

The North American Electric Reliability Council (NERC) has recommended that utilities establish communications with the local FBI office. Regular information exchanges with local law enforcement agencies should also be pursued. These are steps that all utilities could employ at low cost. A utility's decision to establish a liaison with the FBI is purely voluntary, although most generally implement NERC's recommendations. The Federal Government might consider requiring the FBI to maintain communications with utilities.

If an attack is detected, whether by guards or remote surveillance, very rapid, armed response may be required to prevent damage. Such responses must be planned and tested beforehand. Considerable coordination will be required to assure that the appropriate forces are available, know what is required, and will be alerted promptly. The forces could be local or State police, or, as is already being planned for facilities vital to national security, U.S. military forces. If no response forces are available in a useful time-frame (a matter of very few minutes), increased hardening and permanent armed guards are the only options for minimizing damage.

Under some conditions, it might be necessary to temporarily station armed guards, such as the National Guard, at electric power facilities. These troops could be deployed much faster and more effectively if contingency plans have been prepared and studied beforehand.

LIMITING THE CONSEQUENCES

If damage cannot be prevented, the next best thing is to ensure that impacts on customers are as low as possible. Utilities have already installed protective devices on the transmission networks such that it is unlikely that blackouts would cascade beyond the directly affected region. Other steps can be taken that would further reduce the extent of the impacts.

Improve Emergency Planning and Procedures

The behavior of a transmission system following simultaneous destruction of several key facilities cannot be predicted with complete accuracy. It depends on the circumstances on the system at the time as well as on the pattern of destruction. Considerable contingency planning under a variety of conditions is necessary to ensure that the best responses are identified. In cases where there is some warning, operators can revise the pattern of generation and transmission so that more failures can be accommodated. In addition, operators will be required to make quick judgments after damage occurs. Training in recognizing and responding to multiple, simultaneous losses, which no utility has yet experienced, will help operators control instabilities and keep as much power flowing as possible. The Pacific Gas & Electric Co. has credited its drills and planning with minimizing disruption after the 1989 Loma Prieta earthquake.

Modify the Physical System

Transmission networks are generally designed with reserve capacity to accommodate equipment failure and maintenance requirements, and allow for unpredictable developments in loads and resources. One or two equipment failures should cause no significant problems for the customers. Transmission networks could be designed to ride out virtually any conceivable attack, but that would require prohibitively expensive redundancy of equipment, including spare lines in separate corridors. However, some upgrading would limit the extent of the blackout in case of the loss of several key facilities. Analysis of the bulk power system following postulated severe damage can identify potential constraints to keeping at least some of the system operating. Some of the improvements that might prove worthwhile are upgraded control centers, greater redundancy at certain substations, more protection devices and interconnections, upgraded lines, improved communications, etc. The Electric Power Research Institute is developing highly sophisticated computer systems that could analyze and respond to abnormal fault conditions, thereby limiting disruption.

One counter trend should be noted. Loads on transmissions lines are increasing as utilities find opportunities for economic transfers of power.

Increasing competition in the electric power industry could further increase these loads.[8] Unless construction keeps pace with the increasing loads, the result will be smaller reserve margins. The greater the reserve margin, the more opportunities utilities would have to bypass damaged facilities. Thus increasing efficiency of use of the transmission system could conflict with reliability of service, especially under the kind of extraordinary conditions considered in this report.

Increase Spinning Reserves

When a major failure of generating or transmission capacity occurs, utilities must have replacement capacity available immediately. Since generators take some time to warm up before they can start delivering power, reserve capacity must be kept on-line. Usually this means several generators are operated sufficiently below full load so that any anticipated outage can be accommodated by an increase in their power level. The usual reserve is at least equivalent to the largest single unit or transmission line in operation, in accordance with customary planning for the possible loss of any one piece of equipment.

If multiple facilities are sabotaged simultaneously, the available spinning reserve is likely to be inadequate. Operators will not be able to find adequate replacements for the isolated generators, and many areas will lose power, at least until other units can be started which may require several hours. Under such conditions, increased spinning reserve levels could significantly reduce the disruption, depending on the patterns of damage and the remaining available capacity. Utilities are prepared to increase spinning reserves temporarily if they are aware of a specific threat against them such as sabotage or major storms. Maintaining higher levels routinely would protect against unexpected attacks.

If additional generating capacity is available, operating it as spinning reserve is not very expensive. The additional fuel and labor costs are modest. Some parts of the country currently have excess capacity which may be used for spinning reserves, although load growth is slowly reducing that surplus to historically normal levels. During certain periods, such as extreme peak hours or when multiple units are undergoing maintenance, surplus capacity is not available for increased spinning reserves. Increasing spinning reserves during those periods could require expensive new construction.

SPEEDING RECOVERY

Once the system has been stabilized, operators try to restore power as quickly as possible. Even after severe damage, power to parts of the system usually can be restored within a few hours by isolating the damage and resetting circuit breakers. Restoration to full service and reliability depends on at least temporary repair of the damage. The measures here are intended to eliminate constraints to both near- and long-term recovery.

The benefits of expedited restoration can be extremely large, even if no power outages occur. For example, for each day that a large coal-generating unit is idled, a utility must spend on the order of $1 million for replacement power.[9]

Contingency Planning

As in the two previous sections, advance planning and analysis is vital to minimizing problems. If utilities have already analyzed the problems, they should be able to act more efficiently. For instance, few operators have ever had to blackstart a generator or deal with an entire region of mismatched generation and transmission capacity and loads. Planning can also help with longer term problems such as where to get replacement transformers and how to get them to the site. NERC has started to inventory transformers in order to facilitate emergency borrowing. Completion of this task, such that the operators of all key facilities know where to look to borrow critical equipment, could save precious time in an emergency.

Clarify the Legal/Institutional Framework for Sharing

Utilities routinely loan equipment and crews to help restore another utility's power after an emergency, when this can be done without jeopardizing their own operations. However, utilities normally maintain spare large transformers only to the extent that they are needed to permit maintenance and

[8] U.S. Congress, Office of Technology Assessment, *Electric Power Wheeling and Dealing: Technological Considerations for Increasing Competition,* **OTA-E-409 (Washington, DC: U.S. Government Printing Office, May 1989).**

[9] See ch. 4 for a discussion of the cost of disabled units.

replace failures. If these spares are loaned, the owner is risking its own system reliability. From a national perspective, it is better to risk reliability in one area than to keep another area blacked out, but utilities cannot be expected to willingly sacrifice their own reliability for the national interest. In addition to their own economic interests, they may be concerned that they will be sued by their customers who suffer blackouts because backup equipment has been loaned out.

The Defense Production Act and other national emergency laws already permit the government to requisition equipment (with just compensation) needed in case of a threat to the national security, for instance if a key defense facility is blacked out in time of war. There is no general power to intervene in a major economic emergency that has no national security implications, but the legal situation that would pertain is complicated.[10] State governments can guarantee such transfers within their own boundaries, and utilities can make their own voluntary arrangements including indemnification. However, a national policy establishing a mechanism to determine priorities and protect economic interests may be needed to expedite action and in cases where the equipment would be shipped across jurisdictions.

Stockpile Critical Equipment

Rapid restoration of a system damaged by the loss of several large transformers requires finding and installing at least temporary replacements. Many utilities keep some spare transformers in case of equipment failure. At least one utility keeps spare Generation Step Up (GSU) transformers for each plant because of past problems with GSU reliability.[11] However, these spares are typically kept at the substation site, near the operating transformers, where a saboteur could readily destroy them along with the operating transformers. If a utility is unable to obtain spares, whether from its own system or from another utility, the only other option is to order a replacement from a manufacturer. Custom-designed units may require a year or more to manufacture.

A secure source of emergency transformers could cut many months off replacement time. Such a source could be a stockpile of the most commonly used types of transformers, available to any utility in an emergency, or it could be individual backup units for each vital substation. In either case, the units would have to be stored in a secure location, perhaps at military installations.

Backups for each substation would effectively solve the problem of long-term blackouts, but at a high price. The effectiveness of a common stockpile in reducing vulnerability depends on several factors relating to the nature of the destruction, the physical characteristics of the system, the availability of spares from other sources, and the number and type of spares in the stockpile.

The wide variety of transformers in use complicates the development of a stockpile. The major criteria are the input and output voltages and the power level. There is also a wide choice of less crucial factors such as insulation level and tolerable range of voltages.

Because voltages on transmission and distribution systems are standardized, there are only a few common and important combinations of step-down voltages. Six to eight key combinations of voltages could be identified for developing model transmission transformers. While there are many other voltage combinations and functions of transformers, those factors would not be the key consideration in an emergency.

GSU transformers present a more challenging stockpiling problem. Because generator output voltages are designed to maximize operating efficiency and not according to standardized values, voltages range from 12 to 30 kV.[12] A stockpile of GSU transformers would have to make use of the ability of generating units to produce a small range of output voltages (±5 percent of nominal), although with a slight loss of efficiency.[13] Also, ABB transformer engineers have suggested that it should be possible to design transformers to work with a variety of input voltages, in which case most 345-kV transformers could be backed up by two separate models and most 500-kV transformers by three to

[10] Robert Poling, Congressional Research Service, personal communication Feb. 12, 1990.

[11] Bernard Pasternack, American Electric Power, personal communication, October 1989.

[12] U.S. Congress, Office of Technology Assessment, op. cit., footnote 8, p. 91.

[13] D.G. Fink and H.W. Beatty (eds.), *Standard Handbook for Electrical Engineers* (New York, NY: McGraw-Hill, 1978), p. 7-34.

four common single-phase models.[14] Assuming similar numbers for 230- and 765-kV units, a stockpile of GSU transformers could be based on a total of around one dozen models. Another variable is the physical configuration. The bus from the generator carries an extremely high current so the losses can be high. Therefore, the substation and GSU are designed to minimize the distance this current has to travel, which may call for a custom-designed connector.

Power ratings, insulation levels, and impedances for both GSU and transmission transformers would have to be selected based on a trade-off of costs and expected application, and efficiencies would be suboptimal. Around 20 transformer models would cover most critical applications. However, a stockpile would almost certainly require more than one set (three single-phase or one three-phase transformer) of transformers of each model. For example, if saboteurs disabled four or more sets of transformers, it is probable that at least two of the sets would have the same voltage combinations and would be replaced by the same model. The number of units of each model would have to be selected based on an assessment of the likelihood of serious sabotage.

Stockpiling raw materials for the manufacture of transformers may be another way to reduce production time in case of an emergency. The customary practice is to design the transformers frost and then order the materials because of the customized nature of the product and costs. Copper, for example, is special-ordered for each transformer (the copper wire is rectangular, not cylindrical, with particular width and height) and takes about 10 to 16 weeks on order. Core steel, porcelain, load-tap-changers (LTCs) are similarly special-ordered. If existing designs and stockpiled materials are used, new transformers can be produced in less than 6 months (in contrast to normal procurement of over 12 months).

Additional spare transformers would be expensive. A set of extra-high-voltage transformers costs on the order of $2 to $5 million. If all important substations are to be backed by duplicate transformers, the capital cost could range up to many hundreds of millions of dollars, depending on the definition of important. Common transformers would have to be designed for use in a variety of applications, so they are unlikely to fall at the low end of the cost range. This is particularly true for the GSUs, which would require a mechanism to accommodate a range of input voltages. Assuming a stockpile of 40 transformer sets (two of each model), the capital cost would be on the order of $100 to $200 million. Building and maintaining storage facilities would add to the cost.

The suboptimal characteristics of common transformers would also result in substantial indirect costs. To match the voltage capability of a nonoptimized GSU, the generator would need to operate at other than its optimal voltage output, resulting in slightly degraded efficiency. Further, the transformer's generic characteristics could result in significant efficiency losses, for example if it is oversized for the generator and as a result operates at partial load. Assuming a combined efficiency loss of 1 percent, the cost at a 500-MW coal plant would be on the order of $2 million during the year required to obtain a custom-ordered replacement transformer. Presumably, however, this cost would be much less than the cost of not having a stockpiled transformer when it is needed.

There would also be costs associated with transporting the transformer from storage to the damaged site. Both the time required and the cost depend on the location of the stockpile and the damaged site. Also, because a common stockpiled transformer would not be perfectly matched to the specific site requirements, it would probably be replaced by a new or repaired transformer, and returned to the stockpile, doubling transport costs. Overall however, the cost of transport is a small fraction of the capital cost of a transformer.[15]

A decision to establish a stockpile would have to address issues of how many units and of what design, where to store them, under what conditions to release the equipment, and how to transport it. Priorities for the use of stockpiled equipment should more than one utility have a need may also need resolution.

Payment for the stockpile is another critical issue. Spares are typically held as an essential part of the

[14]Lex Curtis, Manager of Technical Support, Westinghouse/ABB (now ABB), personal communication, July 27, 1989.

[15]Hilton Peel, Manager of operations, Virginia Electric Power CO., personal communication% July 19, 1989.

operation of a system and are included in the rate base.[16] Currently, neither utilities nor State utility commissions have found compelling reasons to stockpile critical components beyond normal spares. To develop a stockpile paid for by utilities and their customers, both the utility and the utility commission must agree that the expenditures are a valid cost of business in the interest of consumers.

Assure Adequate Transportation Capability

Moving large transformers is difficult under any condition. Frequently, bridges have to be temporarily braced and overpasses removed. Under emergency conditions, transportation could be a serious constraint. The contingency planning discussed above should identify the transportation problems that could slow delivery of transformers to key facilities (or removal from other facilities for use as replacements). Utilities can move to eliminate as many of these problems as possible. For instance, if the rail lines that brought in the transformers have closed, alternative routes could be developed.

If transformers are stockpiled and many are required at once, transportation equipment itself may be a constraint. Large transformers are moved on specialized rail cars called Schnabel Cars. There are only 13 in the country (plus 1 in Canada), and some handle only one type of transformer or are limited in capacity. A serious stockpiling effort should be accompanied by a program to ensure that sufficient Schnabel Cars will be available. This might involve the production and stockpiling of the cars, or just the conversion of all existing cars to handle all transformers. If only single-phase transformers are stockpiled, conventional transportation equipment is probably adequate.

Monitor Domestic Manufacturing Capability

U.S. manufacturing capability of transmission equipment, particularly the large transformers, has declined and imports have risen. The use of imported equipment per se is not a problem if it is the least expensive, best quality equipment available. However, some utilities are concerned that in an emergency, they will have less leverage with foreign companies to assure expedited manufacture of critically needed transformers, and that equipment will take longer to deliver from abroad. Repair of damaged transformers also would be delayed if they had to be shipped abroad and back. At this time, it is not possible to determine what would have to be done to maintain the U.S. industry, or how great would be the value during emergencies. However, the situation would appear to warrant continued attention and analysis by the Department of Energy and the Department of Commerce. National security concerns may dictate the maintenance of some minimum capability even if it is not justified economically under normal conditions. Alternatively, the incentive for stockpiling may increase if supply from abroad can't be considered to be as expeditious.

GENERAL REDUCTION OF VULNERABILITY

The measures discussed above could be implemented specifically to reduce the vulnerability of existing bulk power systems. Other measures have not been listed because they would be far too expensive to retrofit. However, as the system grows, new construction is required that might emphasize different approaches. Vulnerability to massive destruction has never been a design parameter in electric power systems (except for nuclear powerplants). Making it a parameter could guide the evolution of future systems toward inherently less vulnerable technologies and configurations. Vulnerability is not likely to be the key factor in most cases, but it could swing an otherwise close decision.

Less *Vulnerable Technologies*

Existing equipment has not been designed to resist sabotage. It is possible that alternative transmission towers, insulators, transformers, etc., could be more resistant than current practice. The Electric Power Research Institute, equipment manufacturers, and DOE might be encouraged to study how to do this. In some cases, alternative designs may be available now that would be less vulnerable even though that was not one of the design criteria.

For example, underground cables are less noticeable and less accessible than overhead lines. Therefore they are less likely to be targets of casual saboteurs, and somewhat harder to attack for serious terrorists. They also avoid drawing attention to substations. Underground cables should also be more resistant to major natural disasters, since they

[16] Ibid.

are not exposed to wind, flying objects, or collapsing towers. However, underground cables are much more expensive to manufacture and install. Furthermore, maintenance and repair, though needed less frequently, are more difficult and expensive. If cables were destroyed, whether by saboteurs or earthquakes, replacement would take considerably longer than for overhead lines.

At present, underground cables usually are used only in heavily populated areas. In areas where land is very expensive, the narrower right-of-way needed by underground cables may more than makeup for the difference in equipment and installation cost. It is likely that there will be a growing trend toward underground cables because of increasing opposition to overhead lines, due in part to aesthetics (property values) and to increasing concern over the health effects of electric and magnetic fields associated with transmission lines.[17] Buried cables virtually eliminate electric fields and reduce magnetic fields. Reduced vulnerability could be an added incentive.

There would also be some advantages in moving toward greater standardization of key equipment, in particular the large transformers. Some of the potential benefits of standardization over the long term are increased opportunities for sharing during emergencies and some reduction in manufacturing time and cost. It would not be practical to retrofit existing facilities or change existing system voltages, but as new capacity is built, it could be guided toward a more limited family of voltages. However, some of the diversity found in our present system is a result of the diverse operating conditions that utilities face and their special needs. Each transformer carries a huge amount of power, and even a tiny loss of efficiency is very expensive. Hence standardization would impose serious additional operating costs if it sacrifices precise optimization for particular applications.

The transformers used in substations to reduce voltage from the transmission system to a distribution system are already standardized to a large extent in that there area limited number of combinations of voltages. If a stockpile were to be established (as discussed above), relatively few models would be required to backup most substations.

GSUs are less standardized than step-down transformers. They usually are designed, engineered, and manufactured to meet a utility's particular needs. It may be possible to design GSUs with multiple low-side voltage levels to fit a variety of generators, according to the National Electrical Manufacturers Association although that is not now done. These would cost more than standard transformers and probably result in less efficient generator and transformer operation.

Decentralized Generation

Until fairly recently, generating stations were growing in size and remoteness from the load centers because of economies of scale and difficulties in siting in densely populated areas. However, when large amounts of power are concentrated in a few generating and transmission facilities, the disruption that is caused by a few failures can be very large. Small generating plants are individually no less vulnerable than large plants (in fact they may be more so because fewer employees are stationed there), but the impact of their loss is less. Saboteurs would have to target more facilities to cause the same disruption. For example, destruction of electric power systems was never a major part of U.S. strategy in the Vietnam War, because most facilities were too small and scattered to be primary targets.[18] If, in addition, smaller plants can be sited close to load centers, the shorter transmission lines provide fewer opportunities for disruption.

To some degree, the trend toward larger plants has been reversed. No very large (over 1,000 MW) plants, either nuclear or coal, have been ordered for over a decade. Many co-generation plants have been constructed that are directly at a load center. Smaller plants offer benefits such as shorter construction times, better matches with uncertain load growth and greater operating flexibility. Reduced vulnerability does not appear to have been a significant factor in the choices that have been made to date.

It is not clear how far this new trend can continue. That may depend in part on how competition

[17] U.S. Congress, Office of Technology Assessment, *Biological Effects of Power Frequency Electric and Magnetic Fields—Background Paper*, OTA-BP-E-53 (Springfield, VA: National Technical Information Service, May 1989).

[18] Federal Emergency Management Agency, "Dispersed, Decentralized and Renewable Energy Sources: Alternatives to National Vulnerability and War," December 1980, p. 28.

changes the institutional structure of the industry[19] and on the relative costs of fuels (natural gas is particularly suitable for small plants). Economies of scale have not disappeared. They merely have been overwhelmed by other factors, some of which, such as high inflation and construction stretchouts, would not be expected to recur in the future.

A related issue is the use of transmission corridors and substations for multiple circuits. Utilities often try to maximize the use of corridors because it is economical to do so and increasingly difficult to establish new corridors. However, this concentration increases vulnerability. Utilities plan for common failures of adjacent facilities (e.g., a plane crashing in the corridor could bring down all the lines) but saboteurs could attack several multi-circuit corridors simultaneously with very great impact. The use of single-circuit corridors and substations, wherever practical, would reduce the impact of each attack commensurately.

Vulnerability considerations are not likely to be dominant if traditional approaches prove much more economical. However, under some conditions, it may be worthwhile to include vulnerability as a factor when siting and sizing new facilities. Further study of the relationship between decentralization, economics, and vulnerability may be warranted.

[19]For an analysis of the effects of competition, see U.S. Congress, Office of Technology Assessment, op. cit., footnote 8.