digital power group

A White Paper On

Critical Power

Sponsored by:

Cummins Power Generation

Danaher Power Solutions

eyp mcf
eyp mission critical facilities, inc.

EnerSys
Power/Full Solutions

POWERWARE

Schneider Electric

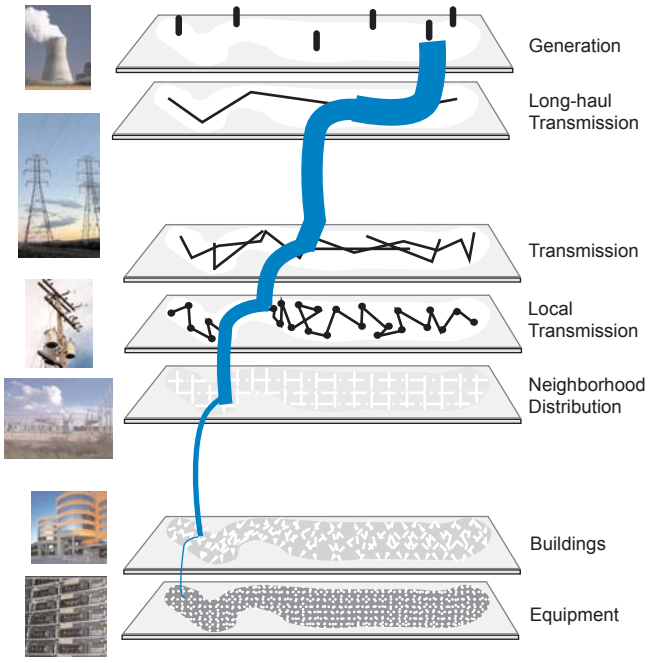
Critical Power

EXECUTIVE SUMMARY

Electricity occupies a uniquely important role in the infrastructure of modern society. A complete loss of power shuts down telephone switches, wireless cell towers, bank computers, E911 operator centers, police communication networks, hospital emergency rooms, air traffic control, street lights, and the electrically actuated valves and pumps that move water, oil, and gas, along with the dedicated, highly-specialized communications networks that control those physical networks. Familiar and pedestrian though electric power may seem, it is the first domino of critical infrastructure.

The public electric grid, however, is inherently vulnerable. Relatively small numbers of huge power plants are linked to millions of locations by hundreds of thousands of miles of exposed wires. Nearly all the high-voltage lines run above ground and traverse open country, and a handful of high-voltage lines serve entire metropolitan regions. And serious problems tend to propagate rapidly through the grid itself.

The Tiers of the Electric Grid



Derived from "Distributed Energy Resources Interconnection Systems," U.S. DOE NREL (September 2002).

Thus, while the public grid must certainly be hardened and protected, most of the responsibility for guaranteeing supplies of critical power at large numbers of discrete, private grids and critical nodes ultimately falls on the private sector, and on the lower tiers of the public sector —the counties, municipalities, and towns.

A New Profile for Grid-Outage Risks

Many essential services and businesses have critical power needs that have not been properly addressed, often because they have never been systematically assessed. And even enterprises that have prepared properly for *yesterday's* power-interruption risk profiles may well be unprepared for *today's*. The risk-of-failure profiles of the past reflect the rel-

atively benign threats of routine equipment failures, lightning strikes on power lines, and such small-scale hazards as squirrels chewing through insulators or cars colliding with utility poles. The possibility of deliberate attack on the grid, however, changes the risk profile fundamentally—that possibility sharply raises the risk of outages that last a long time and that extend over wide areas.

Even before 9/11, it had become clear that the digital economy requires a level of power reliability that the grid alone simply cannot deliver. Utilities have traditionally defined an "outage" as an interruption of 5 minutes or more. Digital hardware, by contrast, cannot tolerate power interruptions that last more than milliseconds. The challenge and the opportunity now is to deploy critical-power hardware that supplies exceptionally clean and reliable power to the critical nodes of the digital economy, and that guarantees operational continuity for the duration of the extended grid outages that deliberate assaults on the infrastructure might cause.

Backup generators, uninterruptible power supplies (UPS), and stand-by batteries are already widely deployed. About 80 GW of off-grid backup generating capacity already exist – an installed base equal to about 10 percent of the grid's capacity. Roughly 3 to 5 percent of the public grid's capacity is currently complemented and conditioned by UPS's – about 25 gigawatts (GW) of large UPS capacity in businesses and government buildings, and another 10 to 15 GW of capacity in smaller desktop-sized units located in both businesses and residences. And end users have, as well, installed over 30 million large stand-by batteries.

Until recently, the deployment of much of this hardware has been directed at power *quality*—smoothing out spikes and dips that last for only fractions of a second—or short-duration issues of power *reliability*—dealing with grid outages lasting from minutes up to an hour or so. In the new geopolitical environment, however, planners must address the possibility of more frequent grid outages that last for many hours, days, or even longer. Assuring *continuity* during extended outages requires a different approach, and a different level of investment in local power infrastructure.

Tiers of Power

Much of the critical-infrastructure literature refers to the grid as a single structure, and thus implicitly treats it as "critical" from end to end. But the first essential step in restoring power after a major outage is to isolate faults and carve up the grid into much smaller, autonomous islands. From the perspective of the most critical loads, the restoration of power begins at the bottom, with on-site power instantly cutting in to maintain the functionality of the command and control systems that are essential in coordinating the step-by-step restoration of the larger whole.

The hardening of the grid does certainly begin at the top tier, in the generation and transmission facilities. Much of modern grid's resilience is attributable to the simple fact that "interties" knit local or regional grids into a highly interconnected whole, so that any individual end user may receive power from many widely dispersed power plants. (This architecture also increases everyone's vulnerability to far away problems.)

Very large end users rely on similar "intertie" strategies — one-tier lower down in the grid — to help secure their specific critical-power needs. Substations, deeper in the network and closer to critical loads, can also serve as sites for deployment of distributed generating equipment. With the addition of its own generating capacity, the substation is "sub" no longer – it becomes a full-fledged "mini-station."

Report Authors

Mark P. Mills
Partner, Digital Power Group
Partner, Digital Power Capital

Peter Huber
Partner, Digital Power Group
Partner, Digital Power Capital
Senior Fellow, Manhattan Institute for Policy Research

Research Associates

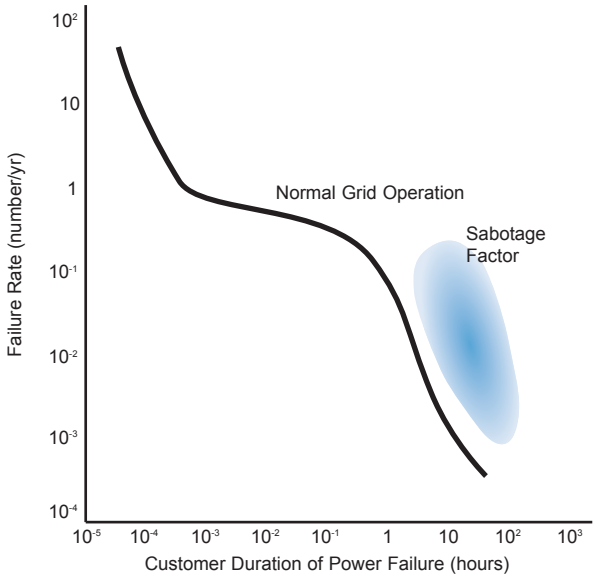
Mary Catherine Martin
Heidi Beauregard

Digital Power Group
www.digitalpowergroup.com
1615 M Street NW, Suite 400
Washington, DC 20036
mmills@digitalpowergroup.com
phuber@digitalpowergroup.com

Sponsors & Supporters
Sponsorship of this White Paper was provided by EYP Mission Critical Facilities (Chair, Technical Advisory Committee), Cummins Power Generation, Danaher Power Solutions, EnerSys Reserve Power, Powerware, and Schneider Electric Square D.

We would also like to thank, for their ongoing assistance and support in our pursuit of this and related subjects, both Gilder Publishing and Forbes Publishing who (sequentially) published our investment newsletter, The Digital Power Report.

Electric Failures: Customer Perspective



Derived from: "Powering the Internet-Datacom Equipment in Telecom Facilities," Advisory Committee of the IEEE International Telecommunications Energy Conference (1998).

Opportunities for deploying new generation at this level of the grid — either permanently or when emergencies arise — are expanding, although still greatly under deployed. Utility-scale mobile "generators on wheels" — either diesels or turbines – offer an important additional option. Some substations already play host to small parking lots worth of tractor-trailers, each carrying 1 to 5 MW of generators. In the longer term, other sources of substation-level generation and storage may include fuel cells, and massive arrays of advanced batteries.

For the most critical loads, however, none of these options is an adequate substitute for on-site backup power. On-site power begins with on-site supplies of stored electrical, mechanical, or chemical energy – typically mediated and controlled by the high-power electronics and controls of a UPS. Rechargeable batteries remain the overwhelmingly dominant second-source of power. But batteries store far less energy per unit of volume or weight than do liquid hydrocarbon fuels.

Thus, to cover the threat of longer grid outages, the backup system of choice is the stand-by diesel generator. Sized from 10s to 1000s of kilowatts, diesel gensets can provide days (or more) of backup run time – the limits are determined only by how much fuel is stored on-site, and whether supplies can be replenished. Diesel generators are strongly favored over other options because they strike the most attractive balance between cost, size, safety, emissions, and overall reliability. And the far-flung, highly distributed infrastructure of fuel oil storage tanks is effectively invulnerable to the kinds of catastrophic failures that could incapacitate power lines or gas pipelines across an entire region.

To complement the hardware, monitoring and maintenance play a key role in maintaining power reliability, from the gigawatt-scale tiers at the top of the grid, down to the UPS and individual loads at the bottom. Real-time control plays an essential role in the stabilization of still-functioning resources, and the rapid restoration of power to critical loads after a major failure in any part of the grid. At the grid level, supervisory control and data acquisition systems (SCADA) are used by utilities and transmission authorities to monitor and manage distribution. At the user level, all the power hardware likewise depends increasingly on embedded sensors and software to monitor and coordinate – a non-trivial challenge as problems happen at the speed of electricity.

Reliability-centered maintenance – familiar in the aviation industry but still a relatively new concept for power – is becoming more important with the rising complexity of systems. Some of the most useful critical-power investments thus center on routine upgrades that replace older equipment with state-of-the-art hardware, which has built-in digital intelligence and monitoring capabilities. Changes as seemingly simple as speeding up the performance and automating of circuit breakers can greatly lower the likelihood of serious continuity interruptions precipitated by the power-protection hardware itself. And sensor- and software-driven predictive failure analysis is now emerging, and will certainly become an essential component of next-generation reliability-centered maintenance.

Resilient Design

One of the most important – and least appreciated — challenges in the critical-power arena is to determine just how robust and resilient supplies of power actually are. It is easy to declare a power network "reliable," but difficult to ascertain the actual availability metrics. The aviation and nuclear industries have spent many decades developing systematic, quantitative tools for analyzing the overall resilience of alternative architectures, and continuously improving the best ones.

But the tools of probabilistic risk analysis–essential for any rigorous assessment of reliability and availability — are still widely underused in critical-power planning. Employed systematically, they require power engineers, statisticians, and auditors to physically inspect premises, analyze multiple failure scenarios, draw on hardware failure-rate databases, and incorporate both human factors and external hazards. Proper critical design takes into account the key (though frequently overlooked) distinction between power reliability, and the actual *availability* of the system thus powered. The analytical tools and the technologies required to engineer remarkably resilient, cost-effective power networks are now available. The challenge is to promote their intelligent use when and where they are needed.

Private Investment And The Public Interest

Significant niches of the private sector were making substantial investments in backup power long before 9/11, because electricity is essential for operating most everything else in the digital age, and because the grid cannot provide power that is sufficiently reliable for many very important operations. Backing up a building's power supplies can be far more expensive than screening its entrances, but improving power improves the bottom line, by keeping computers lit and the assembly lines running. Likewise, in the public sector: Secure power means better service.

Though undertaken for private or local purposes, such investments directly increase the reliability and resilience of the public grid as a whole. In the event of a major assault, the process of restoring power to all will be speeded up and facilitated by the fact that some of the largest and most critical loads will be able to take care of themselves for hours, days, or even weeks.

Even more important, the process of restoring power system-wide has to begin with secure supplies of power at the critical nodes. Coordinating the response to a major power outage requires functioning telephone switches, E911 centers, and police communications, and the grid itself can't be re-lit unless its supervisory control networks remain fully powered. The most essential step in restoring power is not to lose it – or at worst, to restore it almost immediately – at key nodes and subsidiary grids from which the step-by-step restoration of the larger whole can proceed.

Finally, in times of crisis, private generators can not only reduce demand for grid power, they can — with suitable engineering of the public-private interfaces — feed power back into limited parts of the public grid. Options for re-energizing the grid from the bottom-up are increasing as the high-power switches and control systems improve.

In sum, the most effective way for government to secure the nation's critical power infrastructure is to encourage private sector investment in critical power facilities – not just by the relatively small numbers of quasi-public utilities and large federal agencies, but by private entities and state and local government agencies. Dispersed planning and investment is the key to building a highly resilient infrastructure of power.

Accordingly, as discussed in more detail at the end of this report, we identify eight major areas for coordinated action by policy makers, industry associations, and end users in the public and private sectors.

1. Assess Vulnerabilities

Policy makers should be leading and coordinating the efforts of user groups, critical power providers, and utilities to conduct systematic assessments of critical-power vulnerabilities, for specific industries, utility grids, and configurations of backup systems.

2. Establish Critical-Power Standards for Facilities Used to Support Key Government Functions

Federal and local organizations should work with the private sector to establish guidelines, procedures, and (in some cases) mandatory requirements for power continuity at private facilities critical to government functions.

3. Share Safety- and Performance-Related Information, Best Practices, and Standards

Utilities, private suppliers, and operators of backup power systems should develop procedures for the systematic sharing of safety- and performance-related information, best practices, and standards. Policy makers should take steps to facilitate and accelerate such initiatives.

4. Interconnect Public and Private Supervisory Control and Data Acquisition Networks

The supervisory control and data acquisition networks operated by utilities and the operators of backup power systems should be engineered for the secure exchange of information, in order to facilitate coordinated operation of public and private generators and grids. Policy makers should take steps to facilitate and accelerate that development.

5. Secure Automated Control Systems

The necessary integration of supervisory control and data acquisition networks operated by utilities and the owners of backup power systems requires high assurance of cyber-security of the networks in both tiers. Policy makers should take steps to advance and coordinate the development of complementary security protocols in the public and private tiers of the electric grid.

6. Share Assets

Policy makers and the private sector should take steps to promote sharing of "critical spares" for on-site generation and power-conditioning equipment, and to advance and coordinate the establishment of distributed reserves and priority distribution systems for the fuel required to operate backup generators.

7. Enhance Interfaces Between On-Site Generating Capacity and The Public Grid

Improved technical and economic integration of on-site generating capacity and the public grid can backup critical loads, lower costs, and improve the overall resilience of the grid as a whole, and should therefore rank as a top priority for policy makers and the private sector.

8. Remove Obstacles

Private investment in critical-power facilities creates public benefits, and policy makers should explore alternative means to remove obstacles that impede private investment in these facilities.

Critical Power
Contents

INTRODUCTION

Plans for the long-term protection and hardening of U.S. infrastructures are now underway, under the auspices of the Department of Homeland Security (DHS). Two of the leading public/private partnerships developing standards and plans for action include The Infrastructure Security Partnership (TISP) and the Partnership for Critical Infrastructure Security (PCIS). Through these and a web of other similar initiatives, a vigorous and broad effort is under way to identify, coordinate, and direct the reinforcement, protection, and security of key infrastructure components in both the public and the private sectors. Electric power is one of the six network-centered sectors that have been identified as key, along with information and communications, banking and finance, oil and gas, rail and air transport, and water. Four critical service sectors have also been identified: Government, law enforcement, emergency services, and health services.

All of these critical sectors are interdependent in varying degrees. But electricity occupies a uniquely important role. The loss of power shuts down telephone switches, wireless cell towers, bank computers, E911 operator centers, police communication networks, hospital emergency rooms, air traffic control, street lights, and the electrically actuated valves and pumps that move water, oil, and gas, along with the dedicated, highly-specialized communications networks that control those physical networks.

The loss of power also takes out virtually all of the new systems and technologies being deployed for 24/7 security in both private and public facilities, not just communications and computing but everything from iris scanning to baggage x-raying, from security cameras (visual and infrared) to perimeter intrusion systems, from air quality monitors to air-scrubbers.

More broadly, the loss of power shuts down any factory, plant, office, or building that depends on computers, communications systems, pumps, motors, cooling systems, or any other electrically operated system. As the President of PCIS recently testified in Congress:

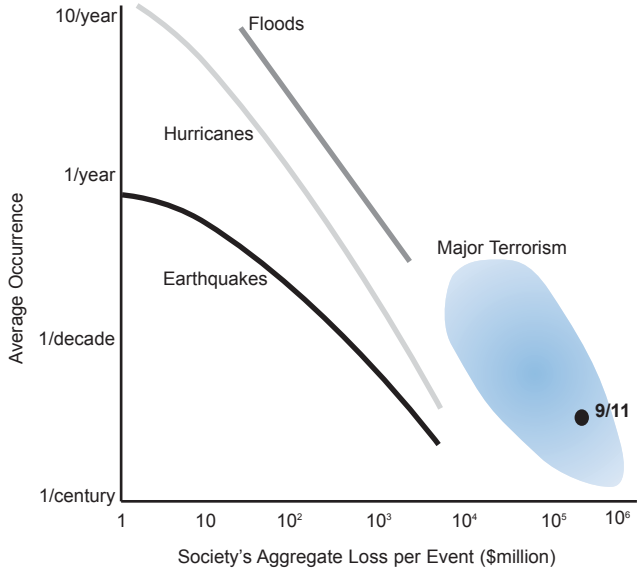
> *(T)he line between physical and cyber assets is becoming even more blurred by the widespread use of digital control systems – electronically controlled devices that report on kilowatt hours transmitted, gallons per hour of oil and water, cubic feet of natural gas, traffic on "smart roadways," and can actually control physical assets like flood gates; oil, gas, and water valves and flow controllers; ATM machines; and the list keeps growing.*[1]

The infrastructure of "critical power" is thus highly distributed. It is also multi-tiered – there are many different levels of "criticality" to address. Power is critical wherever it fuels a critical node, however large or small. Some nodes are as large as a military base, a bank, or a chip fab; some are as small as a single cell tower, a valve in a pipeline, or a crucial switch on the grid. At some critical nodes, the power only needs to be secure enough to permit an orderly shut down; others have to be robust enough to run autonomously for hours, days, weeks, or even longer. And the number of critical nodes continues to increase rapidly, as the entire nation grows increasingly electrical, increasingly digital, and increasingly automated.

The hardening of our electric power infrastructure thus requires actions that extend much deeper and more ubiquitously than is commonly recognized. The handful of gigawatt-scale power plants, along with the public grid, certainly must be protected. But there are hundreds of thousands of smaller nodes and private grids – ranging from tens of kilowatts to tens of megawatts in size – that must be protected. Reliability levels must be structured, tiered, and nested. However much is done to strengthen it, the three-million-mile grid will inevitably remain the least reliable (though also the most affordable) source of power, just as it is today; far higher levels of electrical hardening will be required in much smaller islands of reliability – in the nodes that provide communications, computing, key security and health services, and so forth. So, while the public grid itself must be hardened and protected, it is neither feasible nor economical to sufficiently harden the entire grid as much as it is possible and necessary to harden much larger numbers of discrete, private grids and nodes.

Securing the infrastructure of critical power will require, in other words, an approach similar to the one taken in addressing the Y2K bug in computer software and firmware several years ago. No top-down solution was possible; the points of vulnerability had to be identified, and the fixes implemented on a distributed, granular basis, with the private sector ultimately taking most of the initiative. The need to

Figure 1.
Wide-Impact Disasters



Derived from: Amin, Massoud, "Financial Impact of World Trade Center Attack," EPRI, DRI-WEFA (January 2002).

Society-Wide Impacts From Major Disasters
Businesses, emergency planners, insurance companies, and government now face the challenge of a new 'zone' of risk and consequence.

adopt that same approach for securing data and telecom facilities was reaffirmed in an Executive Order issued barely a month after the 9/11 attacks.

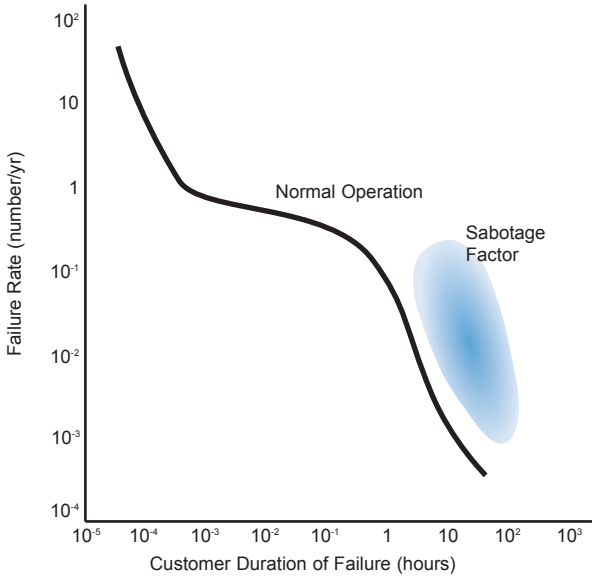
> *The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and* ***the physical assets that support such systems****. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.*[2] [emphasis added]

Electric power is certainly the most important of the "physical assets that support such systems." And most of the responsibility for securing the key nodes of the power infrastructure and guaranteeing supplies of critical power will ultimately fall not on utilities or the federal government, but on the private sector, and on the lower tiers – the counties, municipalities, and towns – of the public sector. Most of the critical nodes are owned and operated in these lower levels. Securing critical power must inevitably focus on numerous, smaller nodes and islands of power vulnerability.

The grid has always been vulnerable, and major segments of both the public and private sectors have long recognized the need for taking a distributed approach to securing their own particularized critical power requirements. The military certainly grasps the critical importance of power in all its systems, and deploys backup power in depth. So do federal, state, and local government agencies, hospitals, phone companies, wireless carriers, broadcasters, banks, insurance, financial trading companies, major providers of online and Web-hosting services, package distribution companies like UPS and Federal Express, major manufacturers, and pharmaceutical and biotech companies. Utilities themselves widely deploy backup-power systems to keep control centers, valves, switches, and other essential hardware running in power plants, when the power plant itself is unable to supply the grid that powers the plant's own, internal infrastructure.

But with that said, much of yesterday's planning for emergencies must now be reevaluated. In the past, many enterprises simply did not need to deploy backup power at all, because the risk-cost profile of

Figure 2.
Electric Grid Failures: Customer Perspective



Derived from: "Powering the Internet-Datacom Equipment in Telecom Facilities," Advisory Committee of the IEEE International Telecommunications Energy Conference (1998).

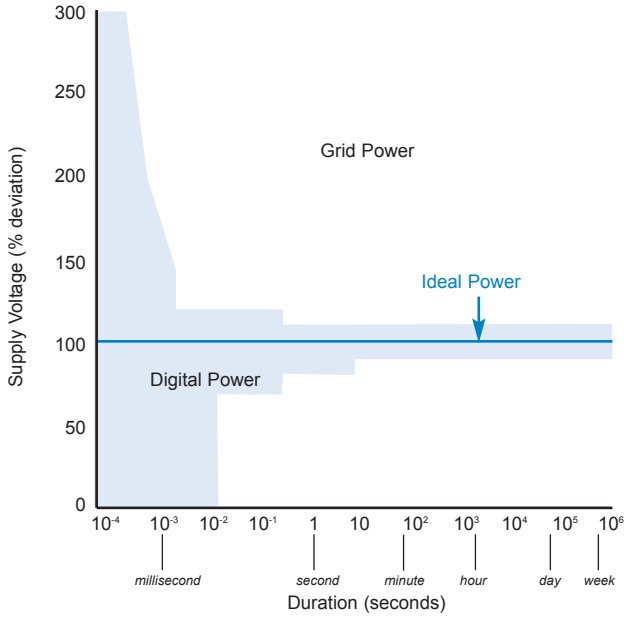
Customer Power Outages: Frequency & Duration
The potential for sabotage creates an entirely new regime for customer outages, adding yet another dimension to protecting critical operations from the inherently unreliable grid.

expected power failures made it economically rational to simply do nothing, and simply shoulder the costs of the infrequent, and typically short, outages when they occurred. Natural disasters – mainly weather related – presented the most significant threat of longer outages, and these risks too were reasonably well understood and bounded. *(Figure 1)*

Much of the rest of the power-related analytic and engineering effort has been directed at power *quality* – smoothing out spikes and dips that last for only fractions of a second – or short-duration issues of power *reliability* – dealing with outages of minutes to an hour or so. *(Figures 2 and 3)* Today's planning, by contrast, must address the threat of grid outages measured in many hours or days. This requires a different level of hardening of local power infrastructure, to assure *continuity* of operations. Heretofore, *that* challenge has been undertaken only by the likes of military bases and Federal Reserve banks.

The failure profiles of the past reflected the relatively benign and familiar threats of the past. Investments in power assurance were planned accordingly. The new environment requires a fundamental reassessment of where power requirements are critical, and how supplies of critical power can be assured.

Figure 3.
Digital Demands and Grid Power



Source: Recommended Power Quality Envelope, IEEE 445-1987.

DEMAND

Congress has broadly defined the starting point to assess the scope and character of demand for critical power. The USA Patriot Act defines critical infrastructures as:

> *[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

From this high-level starting point, most discussions of critical infrastructure jump quickly to lists of networked facilities and services, with electric power ranked somewhere down the list. If any attempt is made to rank levels of criticality, information and communications often come first, alongside government, law enforcement, emergency services, and health services. Banking and finance, electricity, oil, gas, water, and transportation are typically viewed as defining the second tier.

This gets things backward. However familiar and pedestrian electric power may seem, it is the first domino of critical infrastructure.

Powering Public Networks

It does not require a great deal of fine analysis to rank as "critical infrastructure" the principal information and material-moving networks of the modern economy – the telecom and financial networks that move bits, and the electricity, oil, gas, and water networks that move material and energy. Defining something as critical is, ultimately, a statement that many people depend in important ways on a system or service, the failure of which will set off a cascade of harmful consequences. Large networks are critical simply because so many people depend on them so much.

The security of all of these networks is the subject of urgent, on-going assessment. Much of the analysis has been focused on physical and cyber security – protecting the physical structures themselves, or the computers that are used to control them. But their greatest vulnerability is the power on

Table 1. Telecommunications Networks

Category	Number
Broadcast TV [5]	1,500
Broadcast radio [6]	10,000
Telephone (central offices)[7]	25,000
Cable (headends, etc.)[8]	10,000
Wireless Infrastructure Mobile Telephone Switching Offices [9]	2,800
Base stations[10]	140,000
Base station controllers[11]	1,900
Private satellite links[12]	700 (e)
Major internet data centers [13]	400
Internet Network Access Points (NAPs) [14]	11
ISPs [15]	7,000 (e)
ISP backbone connections[16]	12,000
Internet points of presence [17]	16,000
Commercial buildings with significant data centers and/or info networks [18]	>9,000
Critical financial networks (e.g., major banks)[19]	19,000

which every aspect of their control and operation ultimately depends. While the multiple layers of the nation's critical infrastructure are highly interdependent, *electric power* is, far more often than not, the prime mover – the key enabler of all the others.

The information and communications sectors are certainly all-electric – bits are electrons, tiny packages of energy moving through long wires, or oscillating in antennas to project radio waves, or exciting lasers to project information through fiber-optic glass. Much of the movement of water, gas, and oil depends on electric pumps and electrically controlled valves. Rail and air transportation are completely dependent on electronic communication and traffic controls; much of short-haul rail is also electrically powered. The agencies and enterprises that provide government, law enforcement, emergency services, and financial services are equally dependent on their communications and computers. And modern hospitals depend completely on all-electric technology.

Simulations of terrorist attacks on the public grid have thus demonstrated a process in which a very small number of well directed attacks precipitate multi-state power outages, which in turn disrupt telecommunications and natural gas distribution systems, and – soon thereafter – transportation, emergency services, and law enforcement. This was in fact how the disaster played out in the New York City area on 9/11. The collapse of the Twin Towers destroyed two Consolidated Edison substations that relayed electricity to a large area of Lower Manhattan. Successive layers of critical infrastructure then collapsed as a result. Power outages degraded landline telephone service and subway service. Communications failures then undermined or paralyzed evacuation and emergency response services. The Department of Homeland Security's Critical Infrastructure Assurance Office (CIAO – formerly in the Commerce Department) has analyzed "[t]he cascading fallout" from the 9/11 attack, much of it traceable directly to the loss of electricity for telecommunications. That same dynamic is analyzed in Critical Infrastructure Interdependencies, a study published by the U.S. Department of Energy (DOE) soon after the attack.[3]

Analyses of the vulnerabilities of other critical-infrastructure sectors have reached similar conclusions: The loss of electric power quickly brings down communications and financial networks, cripples the movement of oil, gas, water, and traffic, and it paralyzes emergency response services.

Telecommunications Networks (Table 1)

Broadcast, telephone, cable, data, and networks, other business networks are now completely dependent on electric power. A May 2002 report, prepared by major wireless and wireline telecom trade associations, of course emphasized the importance of communications as a critical infrastructure service in its own right, but also stressed that sector's dependence on electricity.[4] After the 9/11 attack, the report notes, "many customers in New York found that their communications problems stemmed not from destroyed telecommunications hardware but from power failures and stalled diesel generators." To address the problem, however, the report mainly urged utilities to modify their "electric service priority systems" by "adding a limited number of specific telecommunications critical facilities that service National Security and Emergency Preparedness requirements." Little emphasis was placed on the industry's own ability and responsibility to plan for more prolonged grid outages, and take steps to secure its own power supplies.

Financial Services Networks (Table 2)

Government agencies and trade associations that regulate and represent this sector have devoted considerable effort to assuring "continuity" of operations in the event of another major attack. A January 2003 report by the General Accounting Office (GAO) on this sector's vulnerabilities notes that financial services are "highly dependent on other critical infrastructures," particularly the "telecommunications and power sectors."[20] This then leads to a discussion of the widespread power disruptions that could result from cyber attacks on the "supervisory control and data acquisition" (SCADA) systems used to control power and other energy distribution networks. A second GAO report issued in February 2003 concluded that while progress had been made, financial organizations remained directly or indirectly vulnerable to disruptions of their underlying supplies of power.[21] This GAO report recounts how a provider of telecom services to Wall Street had to shut down a key telecom switch in the late evening of September 11, 2001, because "commercial power to that switch was lost, and backup power supplies (generator, then batteries) were eventually exhausted before… technicians could gain access to their facilities in order to restore power." The resumption of financial market services had to await the resumption of telecom services, which had to await the arrival of backup generators and the fuel to run them.

An April 2003 paper, by the Federal Reserve, likewise emphasized the financial sector's vulnerability to wide-scale disruptions of "transportation, telecommunications, power, and other critical infrastructure components across a metropolitan or other geographic area." The report also emphasized that backup sites "should not rely on the same infrastructure components" as those used by the primary site.[23]

Table 2. Financial Services Networks [22]

Institution Type	Total	Large		Small & Medium	
		Number	Assets ($billions)	Number	Assets ($billions)
Federal Reserve	970	25	1,400	950	300
State banks	5,000	10	300	5,000	940
National banks	2,000	40	3,000	2,100	700
Federal and state thrifts	900	20	600	870	400
Federal credit unions	10,000	1	15	10,000	500
Total*	19,000	100	5,200	19,000	2,800

* Totals don't match due to rounding

Table 3. Law Enforcement, Public Safety, and Emergency Services Networks

Category	Number
Hospitals [24]	5,800
Local health clinics [25]	23,000
Nursing homes [26]	17,000
E911 call centers [27]	6,000
Fire & rescue services [28]	45,000
Critical municipal buildings (incl. police)[29]	14,000

Networks of Law Enforcement, Public Safety, and Emergency Services (Table 3)

A report by the U.S. Fire Administration (USFA) – part of the Federal Emergency Management Administration (FEMA), which is now part of DHS – lists as critical nodes E911 and other public safety communications centers and dispatch networks, fire, rescue and emergency medical service stations, pumping stations and water reservoirs for major urban areas, along with bridges, tunnels, and major roadways serving large population centers. Electric power is critical at all of these nodes. Government, police, and other emergency services all depend heavily on communications; hospitals and critical care facilities are also completely dependent on electricity to power the sensors, imaging systems, pumps, and other equipment used to form images and move materials through the modern hospital and its patients.

After ice storms crippled much of the Northeast coast in 1998, FEMA issued a number of power-related findings and recommendations.[30] Numerous government agencies involved in disaster response had lost their communications capabilities, the agency reported, because of a loss of electric power. Many broadcast stations likewise stopped transmitting news updates and emergency messages because of insufficient backup generator capacity. Power interruptions had caused the loss of food supplies at 75 percent of Disaster Recovery Centers. FEMA specifically recommended the deployment of on-site auxiliary power capacity sufficient to keep key equipment operational "for the duration of a utility outage" at critical-care facilities in hospitals, nursing homes, broadcast

stations, and at all National Weather Service (NWS) radio transmitters. Nevertheless, a comprehensive survey by the USFA in 2002 found that 57 percent of firehouses still had no backup power systems.[31]

Physical Networks: Electricity, Oil, Gas, Water, and Transportation (Table 4)

The largest and most important physical networks – the electric grid itself, water, oil, and gas pipelines, and transportation networks – are all highly dependent on electric power to drive pumps and activate valves and switches. A report from the USFA recounts how one major metropolitan area introduced "rolling brownouts" to curtail electrical power consumption, recognizing that this would interrupt domestic water consumption – but initially overlooking the fact that the intermittent shutdown of water pumps would interfere with firefighting as well.

The grid requires its own backup power to actuate valves and switches, to run pumps and lights in electric power plants when primary sources of power fail, and to assure the delivery of power to the communications and control networks that activate switches and breakers to stabilize the grid when transformers fail, lines go down, and large loads short out.

Supervisory Control and Data Acquisition (SCADA) for Physical Networks

The physical networks that move material, energy, and vehicles are all critically dependent on their control systems. The electric grid, oil and gas pipelines, and many industrial systems (and especially those managing hazardous chemicals), are monitored and controlled by means of complex, computer controlled, SCADA networks that collect and convey information about the state of the network and dispatch commands to actuate switches, circuit breakers, pumps, and valves. A critical-infrastructure report issued by the American Petroleum Institute in March 2002, for example, focuses primarily on physical and personnel issues relating to security, but notes the importance of networked computer systems that run refineries and pipelines, and the "electrical power lines (including backup power systems)" on which their operations depend.[55]

SCADA networks, which generate over $3 billion per year in global revenues from hardware and software sales, control annual flows of many hundreds of billions of dollars of energy, and also monitor and control all major transportation of water and wastewater. Utility operations, for example, typically center on SCADA master stations located in one, or

Table 4. Physical Networks: Electricity, Oil, Gas, Water, and Transportation

Category	Number/Size
Electricity	
Transmission SCADA control points	
FERC grid monitor/control [32]	12
Network Reliability CoordinatingCenters [33]	20
Regional Transmission Control Area Centers [34]	130
Utility control centers [35]	>300
Power plants [36]	10,500 (e)
Large (>500 MW)	500 (e)
Small (<500 MW)	10,000 (e)
Transmission Lines	680,000 miles
Transmission substations	7,000
Local distribution lines	2.5 million miles
Local distribution substations	100,000
Oil & Gas	
Oil & Gas SCADA systems	>300
Oil pumping stations [37]	3,000
Gas compressor/pumping stations [38]	4,000
Oil pipelines [39]	177,000 miles
Gas pipelines [40]	1.4 million miles
Oil wells [41]	520,000
Gas wells [42]	360,000
Off-shore wells [43]	4,000
Natural gas processing [44]	600
Oil refineries [45]	150
Oil product terminals [46]	1,400
Oil "bulk stations" [47]	7,500
Oil storage terminals	2,000 (e)
Gas storage facilities [48]	460
Gasoline service stations	180,000
Water & Wastewater	
Treatment facilities (1990)[49]	40,000
Community water systems [50]	56,000
Transportation	
FAA critical centers [51]	56
Airport control towers [52]	560
Rail control centers (99,000 miles)[53]	100
Major municipal traffic control centers [54]	>100

sometimes two, key locations; in a few SCADA networks, regional control centers can take over local operations in the event of a major calamity that takes out the master stations. These master stations may monitor data from 30,000 or more collection points, as often as every two seconds. Much of the communication with the field equipment sensors occurs via analog and digital microwave technology; fiber-optic lines, satellite links, spread-spectrum radio, two-way radio, and other technologies, particularly in the backbones of these private communications networks.

And the importance of power to the continued operation of the networks that distribute materials and energy is growing. The recent push to make electric power markets more competitive is creating more points of interconnection and power hand-off, requiring more data transparency, and much closer and more precise coordination of power flows. Gas and oil pipelines are becoming more dependent on electrically actuated and telecom-controlled switches. A significant number of natural gas pipeline shutoff valves, for example, are manually operated handwheels, that may, in emergency situations, take hours to locate and shut down. Remotely actuated valves allow rapid pipeline shutdown – but require secure power for the SCADA control network and the valves themselves.

In the past, these systems were generally designed and installed with minimal attention to security. Experts now view them as highly vulnerable to cyber attack.[56] Electronic intrusions could precipitate widespread power outages at regional and even national levels. SCADA systems simply *must* be kept running to prevent minor disruptions from turning into major ones. When major disruptions occur, the SCADA systems will be integral to the recovery process, because they provide the essential information and control capabilities to coordinate emergency responses. When SCADA networks go down, the networks they control go down too, and they can't be practically restarted until the SCADA networks themselves become operational once again.

Command and Control Systems for Transportation Networks

Much of the transportation system likewise depends on communications and data networks for coordination and control. And while very little of the transportation system itself is electrically powered, all of the control systems are. However much kerosene or diesel fuel they may have at hand to fuel their engines, planes don't fly without electrically powered air traffic control, railroads don't run without the communications and control networks that manage traffic flow and the configuration of the tracks, and ships and trucks don't move without the similar control/scheduling systems that synchronize movement through harbors and control the traffic lights.

In many respects, the four major families of networks – telecom, finance, government and public safety, and the physical (material, power, transportation) – all depend on each other. Electric power plants depend on railroads and pipelines for their raw fuel; railways and gas pipelines need electricity for supervision and control, and all of the networks depend on police, fire, and emergency services to maintain safety and public order. But electric power is, nevertheless, uniquely important. After major catastrophes, the process of restarting normal life begins with limited supplies of raw fuel – most often diesel fuel – that are used to fire up backup generators, that are used to restart everything else – the communications networks, computers, pumps, and valves that move information and financial data, and reactivate the government services and the material and energy-moving networks, which bring in still more fuel, and then still more power.

The Vulnerable Public Grid

An important 1997 report Critical Foundations by the President's Commission on Critical Infrastructure Protection provides a top-down analysis of the vulnerabilities of the public grid.[57] The report emphasizes how much other infrastructure networks (most notably telecommunications, finance, and transportation) have come to depend on electric power for their continued operation, and notes the "significant physical vulnerabilities" of "substations, generation facilities, and transmission lines." The report contains many useful recommendations for making the public grid more secure. Yet in the end, it simply fails to address the plain – and widely recognized – fact that the grid itself can never be made secure enough to guarantee power continuity at the most critical nodes.

In similar fashion, utilities themselves certainly recognize how much other sectors depend on power.

All major utilities have established "electric service priority" (ESP) protocols to prioritize efforts made to restore power after a major outage. High on the list, of course, are life support, medical facilities, and police and fire stations. But what most utilities emphasize, understandably enough, is what they themselves can do to help restore grid power quickly to the customers that need it the most.

Thus, utilities consult with other sectors in setting these priorities, and in the post-9/11 environment there is, inevitably, a certain amount of lobbying under way to persuade utilities to reorder their power-restoration priorities. The telecommunications industry, for example, launched a "Telecommunications Electric Service Priority" (TESP) initiative to urge utilities to "modify their existing ESP systems by adding a limited number of specific telecommunications critical facilities that service National Security and Emergency Preparedness requirements."[58] The proposed list of such facilities is a long one: It includes all facilities engaged in "national security leadership, maintenance of law and order, maintenance of the national economy, and public health, safety, and welfare." TESP defines "critical facilities" as "those that perform functions critical to the monitoring, control, support, signaling, and switching of the voice telecommunications infrastructure."

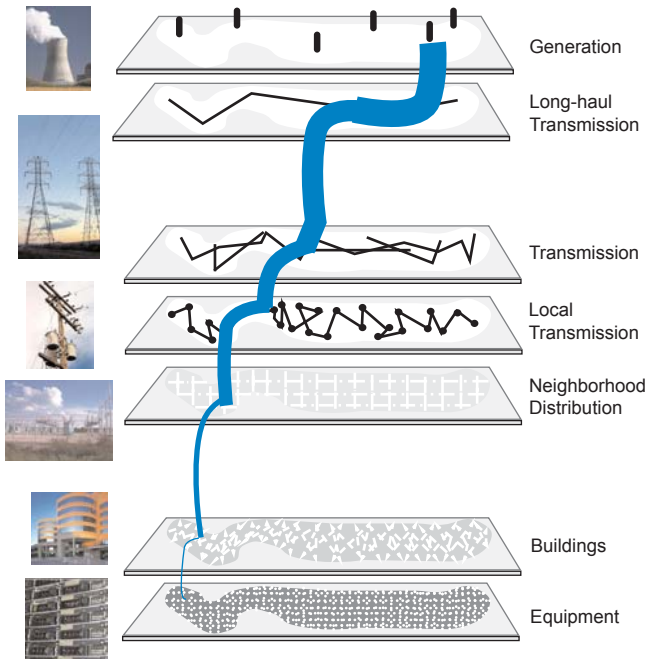
Understandable and even necessary though it is, the lobbying for priority in the utility's power-restoration hierarchy is, ultimately, an acknowledgement that a power-dependent facility isn't "critical" enough to need power better than the grid can supply – or else it is an abdication of the responsibility to secure alternative, off-grid power supplies.

Utilities can and do establish service resumption priorities. They also continuously improve the robustness of the grid as a whole. Enormous amounts of investment have been made to improve the reliability of the public grid since a single faulty relay at the Sir Adam Beck Station no. 2 in Ontario, Canada, caused a key transmission line to disconnect ("open") on November 9, 1965, plunging the entire northeastern area of the United States and large parts of Canada into an eighteen-hour blackout. That seminal event led to the creation of the North American Electric Reliability Council (NERC) and a substantially more resilient grid. But the grid still has many points of vulnerability, and its inherent fragility will never be eliminated. While continuing to rely heavily on the grid in their normal operations, the operators of all truly "critical" nodes and networks also take steps to create their own, independent islands of secure power, to ensure continuity of operation in the case of a major grid outage.

What makes the grid essential is also what makes it vulnerable – it is a vast, sprawling, multi-tiered structure that reaches everywhere, and is used by everyone. Indeed, measured by route miles and physical footprint, the North American grid is by far the largest network on the planet. *(Figure 4)*

The top tier of the grid is fueled (most typically) by coal, uranium or gas; each lower tier is typically "fueled," initially at least, by the electric power delivered from the tier above. "Generating stations" in the top tier dispatch electrical power through some 680,000 miles of high-voltage, long-haul transmission lines, which feed power into 100,000 "substations." The substations dispatch power, in turn, through 2.5 million miles of local distribution wires. The wires are extended and exposed, while the grid's power plants are huge (because big plants burn fuel more efficiently) and thus comparatively few and far between. Nearly all the high-voltage lines run above ground and traverse the open country, and a handful of high-voltage lines serve entire metropolitan regions. At the same time, a couple of large power

Figure 4.
The Multi-Tiered Grid



Derived from "Distributed Energy Resources Interconnection Systems," U.S. DOE NREL (September 2002).

Table 5. Critical Municipal Facilities[59]	
Type	**Examples**
Emergency Services	Police stations, fire stations, paramedic stations, emergency communication transmitters
Water System	Water supply pumping stations, wastewater pumping stations and treatment plants
Transportation	Traffic intersections, aviation terminals and air traffic control, railroad crossings, electric rail systems
Medical	Hospitals, nursing homes, mental health treatment facilities, specialized treatment center (e.g., outpatient surgery, dialysis, cancer therapy), rehabilitation centers, blood donation centers
Schools	Nursery schools, kindergarten, elementary schools, high schools, colleges, business and trade schools
Day Care	Registered facilities, sitter services, after-school centers
Senior	Senior citizen centers, retirement communities
Social Service	Homeless/transient shelters, missions and soup kitchens, youth, family, and battered person shelters, heating/cooling shelters
Detention Centers	Jails, youth detention centers
Community Centers	Libraries, civic centers, recreational facilities
Public Assembly	Stadiums, auditoriums, theaters, cinemas, religious facilities, malls, conference centers, museums
Hotels	Hotels, motels, boarding houses
High-rise Buildings	Apartments, condos, commercial
Food Services	Restaurants, supermarkets, food processing facilities
Industry	Hazardous material handling

plants can provide all the power required by a city of a half-million. Many communities are served by just a handful of smaller power plants, or fractional shares of a few bigger power plants.

Taken together, these attributes make the public grid inherently vulnerable to major disruptions. Demand overloads simultaneously stress all of the main power cables – typically three to five – serving a large city, and one failure can trigger others. On August 10, 1996, three lost transmission lines and some malfunctioning equipment triggered a series of cascading blackouts that paralyzed the West Coast, affecting 7.5 million customers in 11 states and two Canadian provinces. Sometimes purely physical stresses affect the length of the conduits that house power lines. In April 1992, for example, construction workers installing support pillars in the Chicago River punctured the roof of a freight tunnel beneath the river bottom; the ensuing flood shut down utility power for weeks in the heart of Chicago. In response to that and similar events, the City of Chicago with the DOE undertook a uniquely comprehensive and prescient study of the consequences of power outages, which catalogues and categorizes critical-power customers. *(Table 5)*

Serious problems tend to propagate through the grid, as fast as the power itself. Even a severe electrical failure on a single (large) customer's premises can travel upward through the grid to cause much more widespread disruptions. Failures at key points higher in the grid can black out far larger areas. The November 1965 Northeast blackout mentioned earlier was caused by the failure of one small relay in Ontario, which caused a key transmission line to disconnect; that triggered a sequence of escalating line overloads that cascaded instantaneously down the main trunk lines of the grid. Additional lines failed, separating additional plants from cities and towns that used their power. Generating plants in the New York City area then shut down automatically to prevent overloads to their turbines. While much has been improved since the 1960s, recent simulations confirm that deliberate attacks on a very limited number of key points on the public grid could still cause very widespread outages that would take, at the very least, many days to correct.

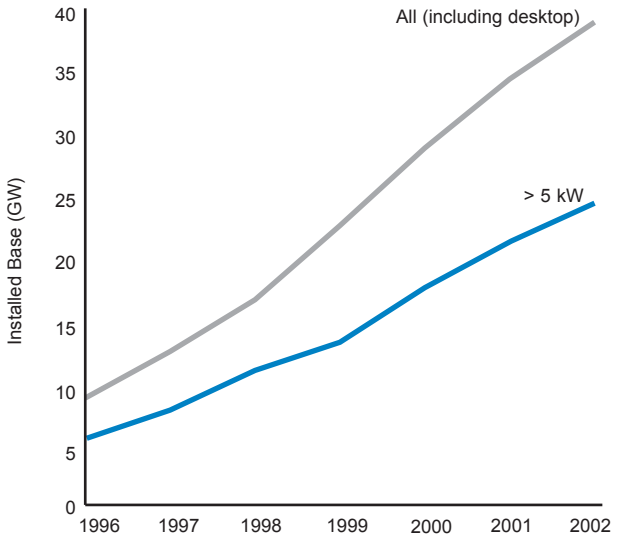
Precisely because it is so critical, a late-2002 White House briefing involving the President's Critical Infrastructure Protection Board specifically noted that the electric power grid now stands "in the cross hairs of knowledgeable enemies who understand that all other critical-infrastructure components depend on energy for their day-to-day operations."[60]

A New Profile for Grid-Outage Risks

Installations of backup generators, uninterruptible power supplies (UPS), and stand-by batteries provide an initial – though backward-looking – measure of total demand for critical power as already determined by end-users themselves.

In many ways the presence of a UPS provides the most telegraphic and useful indicator of a critical electrical load on the premises. A UPS isn't cheap, it isn't deployed lightly, and – as its name reveals – its whole purpose is to assure the continuous provision of power, most often to digital loads. Thus, an array of power electronics, sensors, software and batteries takes power from whatever source can supply it – the

Figure 5.
Uninterruptible Power Supplies



Derived from: Powerware and Frost & Sullivan World UPS Market 2002.

Total Installed Uninterruptible Power Supplies (UPS)
The presence of a UPS provides the most telegraphic and useful indicator of what customers consider "critical" electrical loads.

grid, the stand-by batteries, or a backup generator or fuel cell – and delivers power devoid of sags, spikes, and harmonics. Typically, the on-board battery back-up is just sufficient to permit switching to a secondary source after the grid fails – a backup generator, or a larger bank of batteries. The smallest UPS units sit on desktops; the largest serve entire offices or small buildings. The UPS functions very much as a kind of silicon power plant – taking in "low grade" fuel (in this case, dirty and unreliable kilowatt-hours) to convert into a higher-grade fuel (sag- and spike-free, always-on kilowatt-hours).

Most of the large-unit capacity is in commercial buildings, with some significant share used in industrial environments to maintain critical non-computing digital loads. Fully half of non-desktop UPS capacity is supplied by 75-kilowatt (kW) or larger UPS units. One-third of that capacity is supplied by units larger than 200 kW.

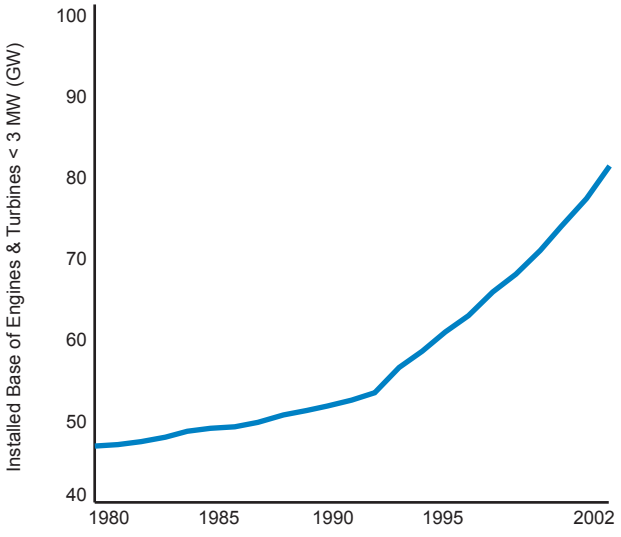
Based on annual UPS shipments and the typical operating lifetimes of these units, we estimate that approximately 25 gigawatts (GW) of large UPS capacity is currently installed and running in businesses and government buildings in the United States, with another 10 to 15 GW of capacity in smaller desktop-sized units in both businesses and residences. *(Figure 5)*

These remarkable figures provide a direct, quantitative estimate of how much U.S. power consumption is viewed as (in some sense) "critical" by end-users themselves. To put them in perspective, the public U.S. grid as a whole is powered by roughly 790 GW of large coal, nuclear, gas-fired, and hydroelectric plants – thus, about 3 to 5 percent of the *grid's* capacity is complemented and conditioned by UPS capacity in buildings and factories.[61]

Deployments of backup generators – the vast majority of them reciprocating engines that burn either diesel fuel or natural gas – provide a second rough indicator of end-users' assessments of their own "critical power" requirements. The indicator is imprecise, because generators are also widely used to supply power in off-grid locations. Nevertheless, trade estimates indicate that there is now 80 GW of backup generation capacity deployed in the United States – in the aggregate, about 10 percent of the grid's capacity. Over the past several years, no less than 1 megawatt (MW) of such distributed (grid-independent) capacity is now being purchased for every 6-10 MW of central-power-plant capacity brought on line.[62] *(Figure 6)*

One finds, for example, thirteen two-megawatt diesel generators installed outside AOL's two major

Figure 6.
Off-Grid Backup Power



Derived from: Diesel & Gas Engine Worldwide Engine Order Survey.

Sales of Backup Power Generation
Total purchases of "small," distributed generators for backup power (rarely connected to the grid) are a significant share of the 40 MW/yr of utility central station capacity added annually in the past two years.

centers in Prince William County and Herndon, Virginia. Real estate companies and data hotels like Equinix, Level3, and Qwest have likewise become major owner-operators of distributed generation (DG) power systems. And all the major engine makers assemble and lease power-plants-on-wheels – tractor-trailers with hundreds of kilowatts to several megawatts of generating capability. These units are positioned around the country for emergencies, parked in substations (to meet peak demand, or replace power from lost transmission feeds), or in parking lots near critical loads.

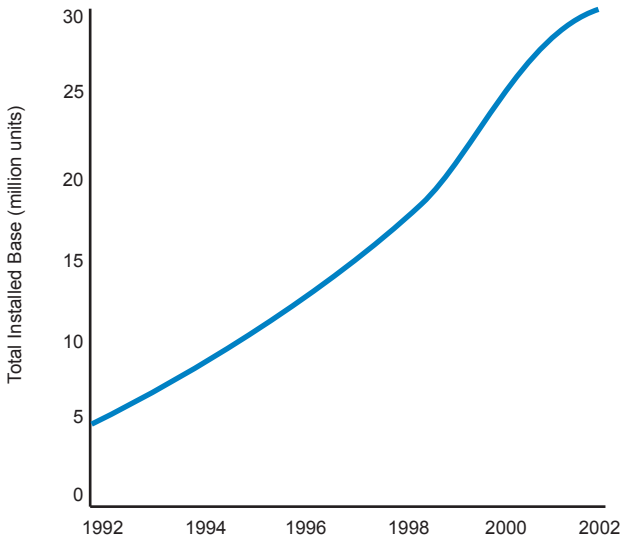
The installed base of stand-by batteries provides a third – again retrospective – measure of what end-users perceive to be their "critical power" needs. The sale of long-life, high-performance backup lead-acid batteries soared through the year 2000 – doubling over a few years to the point of creating delivery shortages. Even though the market is still working off that inventory, sales of new batteries remain 20 percent higher than five years ago – and the advent of data centers and wireless telecom has permanently moved such heavy-duty "industrial" batteries to the lead position in a business formerly dominated by batteries used in more traditional industrial motive power applications (e.g., lift trucks).[63] There is thus a collective total of about 40 million kilowatt-hours stored at any time in about 30 million lead-acid batteries distributed across the landscape (enough electricity to run one million homes for 24 hours). *(Figure 7)*

For every 500 kW of UPS, there are typically five tons of batteries nearby. Telephone company central offices and data centers, for example, still typically contain entire floors filled with lead-acid batteries. The floor space set aside for large UPSs – 100 to 1,000 kW AC and DC silicon power plants – is likewise dominated by lead and acid. There are batteries in every wireless base station and in every optical headend. Some 249 batteries on steel racks stand behind the planet's most precise atomic clock in Boulder, Colorado.

It would be a serious mistake, however, to infer from existing deployments of UPS systems, batteries and generators that the full extent of the need for such facilities has already been recognized and addressed. To begin with, many enterprises simply fail to plan for rare-but-catastrophic events until after the first one hits. Thus, for example, the four large, broad-scale power outages of the last 10 years – Hurricane Andrew in Florida in 1992, Hurricane Fran in Virginia in 1996, and ice storms hitting the East Coast during the winters of 1998 and 2002 – precipitated a cascade of new orders for on-premises power supplies, and these orders continued to be placed for weeks after grid power had been restored.[64] Planning rationally for infrequent but grave contingencies is inherently difficult, and even risk-averse planners have a strong tendency to discount to zero hazards that are thought to be just "too unlikely" to worry about. Many essential services and businesses have critical power needs that have not been addressed only because they have never been systematically assessed.

It is impossible to estimate with any precision how many sites have critical power needs that simply remain unrecognized because they haven't yet been hit by disaster. We do know that there are hundreds of thousands of 10 to 100 kW sites nationwide – the electrical loads now created by tens of thousands of high-end wireless base stations, fiber repeater shacks, and digital offices that – unlike the phone company's central offices – have limited (and sometimes, no) backup. The national banks and financial exchanges have already deployed their backup power systems (although, as earlier noted in a recent GAO report, many are not adequate for the new challenges), but many smaller commercial, investment, regional banking, credit, and trading companies may not yet have done so. The federal government's buildings

Figure 7.
Heavy Duty Backup Batteries



Derived from: Enersys, Battery Council International

Table 6. Cost of Power Interruptions for Industrial Plants[65]		
Interruption Length	Cost/kW Load Interrupted	
	Minimum	Maximum
1 minute	$1	$17
1 hour	7	43
3 hours	14	130

Table 7. Cost of Power Interruptions for Office Buildings with Computers[66]		
Interruption Length	Cost/Peak kWh not delivered	
	Minimum	Maximum
15 minutes	$5.68	$67.10
1 hour	5.68	75.29
> 1 hour	0.48	204.33

already have their backup power, but state and particularly local governments lag far behind them. The general unwillingness to confront hazards that are both very grave and very remote has always been a problem. But it is an especially serious one when risk profiles change – as they surely have in the post-9/11 era. Countless enterprises that were inadequately prepared for hurricanes and ice storms are at even greater risk now that sabotage and terrorism have changed the profile of credible threats.

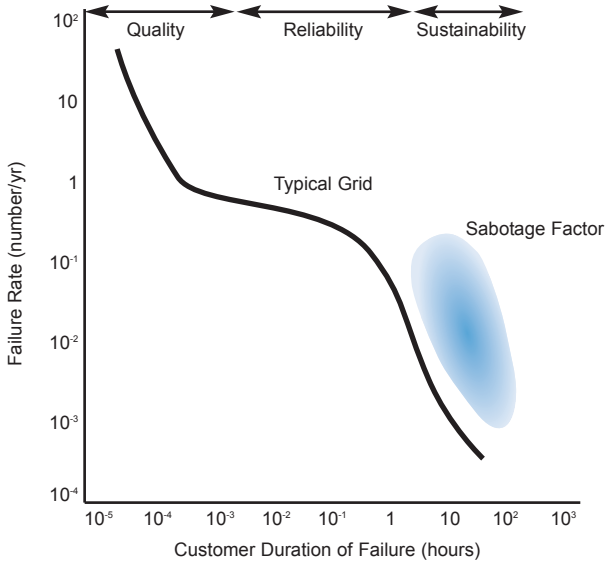
Even enterprises that have prepared properly for yesterday's risk profiles may well be unprepared for tomorrow's. Many surveys, for example, have attempted to document the costs of outages for various industrial and commercial enterprises. *(Tables 6 and 7)* These surveys typically address costs of equipment damage, loss of in-production materials and products, and lost employee productivity, among other factors, from outages that last *minutes* to (typically) *one hour*. But the choice of a one-hour outage, rather than, say, a three-day outage, reflects the survey's assumptions about what kinds of outages are reasonably likely.

The risk-of-failure profiles of the past reflect the relatively benign threats of the past – routine equipment failures, lightning strikes on power lines, and such small-scale hazards as squirrels chewing through insulators or cars colliding with utility poles. Most accidental grid interruptions last barely a second or two, and many "power quality" issues involve problems that persist for only tens of milliseconds (one or two cycles). In most areas of the country, grid outages of an hour or two occur, on average, no more than once or twice a year, and longer outages are much rarer than that. Accidental outages tend to be geographically confined as well; the most common ones involve blown circuits in a single building (and, most typically, caused by human error – ironically enough, much of it "maintenance" related), or interruptions confined to the area served by a single utility substation.

The possibility of deliberate attack on the grid, however, changes the risk profile fundamentally – that possibility sharply raises the risk of outages that last a long time and that extend over wide areas. The planning challenge now shifts from issues of power *quality* or *reliability* to issues of business *sustainability. (Figure 8)* Planning must now take into account outages that last not for seconds, or for a single hour, but for days.

There is normally very little risk that several high-voltage lines feeding a metropolitan area from several different points on the compass will fail simultaneously, and when just one such line fails, all the resources at hand can be mobilized to repair it. Deliberate assaults, by contrast, are much more likely to disable multiple points on the network simultaneously. A National Academy of Sciences 2002 report drove this reality home with its stark observation: "[A] coordinated attack on a selected set of key

Figure 8.
Electric Grid Failures: Customer Perspective



Derived from: "Powering the Internet-Datacom Equipment in Telecom Facilities," Advisory Committee of the IEEE International Telecommunications Energy Conference (1998).

The Power Sustainability Challenge
*The power engineering challenge now expands beyond the quality or reliability of electricity, to include **sustainability**—the ability to continue to operate in the event of outages that last not for seconds, minutes or an hour, but days.*

points in the [electrical] system could result in a long-term, multistate blackout. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years."[67] Users, who have perceived no need to plan systematically, even for those outages that fit the traditional statistical profiles, may now require systems to address the new risks. Enterprises that can afford simply to shut down and wait out short black-outs may not be able to take that approach in response to the mounting threats of longer outages.

Powering Critical Nodes

Roughly one-half of U.S. electric power is consumed by mass-market users – residences and small businesses with peak power requirements under about 20 kW. Overwhelmingly, these consumers currently rely on grid power – power that's (roughly) 99.9 percent reliable, that retails for about 10¢/kWh, and that is generated at large, centralized power plants for about 3¢/kWh wholesale. The average residential customer experiences 90 minutes of power interruptions per year – with 70 to 80 minutes of that down time attributable to distribution system problems – but finds this quality of service acceptable, because the power is used mainly for non-critical purposes that operate on flexible schedules. The washing of clothes and dishes can be postponed; refrigerators and homes remain acceptably cool (or warm) even when the power goes out for several hours; for longer outages, people can temporarily relocate, if they must, to places such as shelters and other centralized facilities where power remains available. If these customers want greater reliability, they generally obtain it by buying power "appliances" – most typically desktop-UPS units for computers or small gasoline or diesel backup generators for other purposes.

At the other pole, aluminum smelters and large auto assembly lines, and enormous commercial complexes, among others, may deploy backup power facilities for certain nodes and control points within their facilities, but cannot backup their entire operations. These monster-load customers, with peak loads above about 10 MW, account for about 20 percent of U.S. electric consumption. Like it or not, they typically have no choice but to depend on the public grid. To make their power more reliable, they work directly with the utility; the most common approach is to engineer two independent links to the public grid, that connect, if possible, with independent high-voltage lines that are powered in turn by different power plants. Any other approach would be prohibitively expensive, because it would leave huge amounts of generating capacity standing idle most of the time. *(Tables 8 and 9)*

(Even in this high-power arena there are, nonetheless, a relatively small subset of digital loads that easily exceed 1 MW of demand – large data and telecom centers – and that simply have no choice but to deploy adequate grid-free backup. The central new challenge for this class of customer is how to deal with the addition of the continuity metric.)

That leaves the middle tier of loads, from roughly 20 kW on up to a megawatt or so. This segment of demand accounts for about 30 percent of U.S. power consumption. A disproportionate share of private production and public services fall within this tier, however – air traffic control centers, supermarkets, city halls, factories, broadcast stations, frozen-food warehouses, office buildings, most data centers, and telephone exchanges, among countless others. These middle-tier nodes are also uniquely important in the process of recovering from major outages. Most users in the top and bottom tiers can ride out power outages for days, or even weeks, so long as power is restored reasonably quickly to tens of thousands of discrete nodes in this middle tier. Thus, in times of disaster, recovery always begins locally, in islands of self-help and resilience.

Large numbers of hospitals, government agencies, phone companies, and private enterprises have already taken steps to secure their power supplies

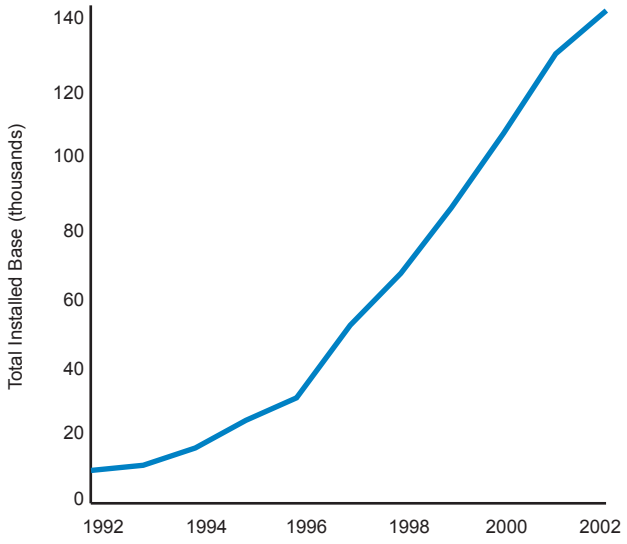
Table 8. Electric Demand: Commercial Buildings[68]

	Small	Midsize	Large
Average kW/Building	10	65	740
Size (x1000 sq ft)	1 – 10	10 – 100	>100
Number of Buildings (thousands)	3,000	1,000	100
Percent of Total Commercial Electricity	23	40	38

Table 9. Electric Demand: Manufacturing Establishments[69]

	Small	Midsize	Large
Average kW/Establishment	100	2,500	19,300
Size (employment)	1 – 99	100 – 499	500+
Number of Establishments	328,000	30,000	4,800
Percent of Manufacturing Electricity	15	38	47

Figure 9.
Cellular Base Stations



Source: Cellular Telecommunications & Internet Association Semi-Annual Wireless Survey.

Cellular Base Stations
Cellular telephony is now a central part of emergency response for citizens, businesses, and emergency professionals, making the sustainability of these networks no longer solely an issue of customer satisfaction.

from the bottom up. They do not count on the public grid alone to meet their critical power requirements – they identify critical-power loads, and then add stand-by generators and switching systems to boost overall reliability. They define critical power in terms of specific loads and nodes, not the network as a whole. This bottom-up approach to securing critical power is an essential complement to top-down efforts to secure the grid. The Institute of Electrical and Electronics Engineers (IEEE) begins from that same premise in its comprehensive analysis and standards document on Emergency and Standby Power Systems.[70] First issued in 1987, and last updated in 1995, this document is still perhaps the most comprehensive analysis of the end-user initiatives that are required to ensure power continuity at critical nodes. A more recent IEEE publication in 2001 expands their standards and evaluations on power from the perspective of different classes of end users, focusing more generally on various non-emergency aspects of distributed generation for industrial and commercial markets.[71]

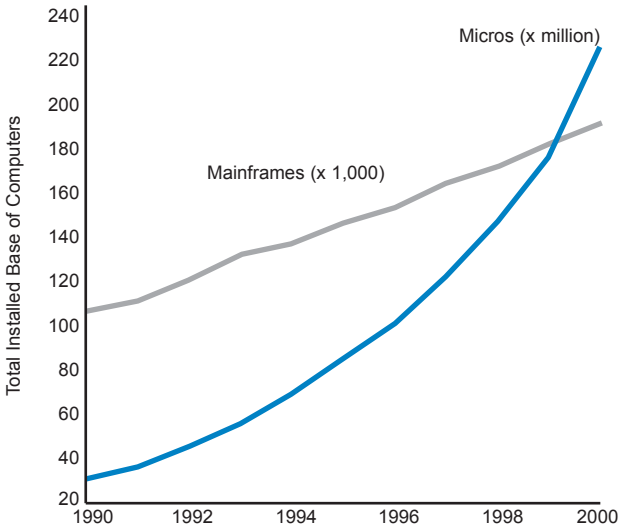
Like the critical public infrastructure that they mirror, most critical-power nodes are defined by the private networks they serve – the hubs that switch and route information, or that control the movement and flow of key materials through physical networks, or that power essential safety systems and services.

Whether it serves a corporation or a city hall, a node that switches or dispatches more than a gigabyte per second of data for much of the working day, or a megabyte per second on a 24/7 basis, or more than 10 kW of analog or digital signal through the airwaves – likely plays a very important role in the day-to-day lives of many people. A typical telephone exchange requires about 100 kW to power it; a television station, about 100 to 250 kW; a radio station, 20 to 100 kW; a cell tower 10 to 20 kW. In some of these sectors – broadcasting, for example *(See Table 1)* – the number of critical nodes has not changed much in the past several years. In others – data centers and wireless telephone transceivers, for example – the number of critical nodes has been rising rapidly. *(Figure 9)*

Powering the wireless communication infrastructure is particularly important because it is in many respects much less vulnerable than the wireline network. Emergency planners have long recognized that the broadcast networks are essential for mass announcements in times of crisis, as are the radio networks used to coordinate responses by police, fire, and emergency services. Assuring the power requirements of wireless telecommunications networks has emerged as a uniquely important priority in critical power planning, because wireless nodes can be replicated more cheaply, and secured much more effectively, than wired networks. Wireless networks also support mobility, which is often essential to providing critical services and when recovering from major disasters.

The public broadcast and wireless networks already rank as part of the "critical" infrastructure. What is still often overlooked, however, is that there are now tens of thousands of private nodes that route and dispatch comparable (or larger) volumes of data. However private or local it may appear, an information node that requires 10 to 50 kW or more of continuous power is likely to be one on which thousands of people depend in some very direct way. To put this number in perspective, a typical U.S. household is a 1.5 kW load (24/7 average), with 10 to 20 percent of that power (150 to 300 continuous Watts) consumed by televisions, telephones, computers, and related peripherals. Comparable computing and communications nodes in commercial and municipal centers define a new, critical class that have received far too little notice in planning to secure critical

Figure 10.
Computers in Businesses*



*Excludes PCs in residences.

Derived from: "Information Technology Data Book 2000," "Home Computers and Internet Use in the United States: August 2000," and U.S. Census "Access Denied: Changes in Computer Ownership and Use: 1984-1997," U.S. Census.

Total Installed Base of Business Computing

The commercial inventory (which excludes 58 million PCs in homes and excludes notebook PCs) provides an indication of the number of computers in data centers, or data rooms. The total commercial employment of fewer than 90 million people (i.e., well under 90 million "desktops") suggests substantially more than 120 million microcomputers clustered in critical nodes of varying sizes.

infrastructure.

Because these nodes are privately owned and operated, and so widely dispersed, it is extremely difficult to quantify their numbers or pin down with any precision the roles they play in maintaining communication, control and the continuity of critical operations. There are, however, some relevant high-level statistics. The total inventory of computing systems installed in all commercial buildings continues to rise rapidly. *(Figure 10)*

Most of the 220 million microcomputers used by American business are located in approximately one million buildings in the mid-tier of the three-tiered hierarchy of power loads. *(See Table 8)* Further analysis of commercial building data suggests a profile of how the critical loads are distributed. *(Table 10)*

It is even more difficult to define and catalogue critical-to-power *physical* networks in the private sector. A recent paper by the Electric Power Research Institute (EPRI) emphasizes the power vulnerability of enterprises engaged in continuous process manufacturing of such things as paper, chemicals, petroleum products, rubber and plastic, stone, clay, glass, and primary metals – all companies with manufacturing facilities that continuously feed raw materials, often at high temperatures, through an industrial process.[74] Many other large factories and corporations have their own internal water, water-treatment, and on-premises pipeline services.

The total power requirements of industrial facilities are defined by individual industrial processes, and vary widely. *(Table 11)* But digital technologies are rapidly taking control of almost *all* industrial processes, even the most familiar and mundane; as a result, there are now very few industries that can continue to function at any level without sufficient electricity to power their key command-and-control networks. *(Table 12)* At the same time, there is steady growth in the number of processes that depend on electricity as their primary fuel – as, for example, when electrically-powered infrared ovens and lasers displace conventional ovens and torches for drying paint and welding metals. Not all of these applications are "critical," but some significant fraction of them is, because they manufacture or service materials or components required for the continued operation of networks on the front lines.

In the end, "critical power" requirements must be defined application-by-application, and site-by-site. They depend on tolerance for interruptions and out-

Table 10. Electric Demand: Commercial Buildings[72]

Principal Building Activity*	Buildings (thousands)	kW/Building (avg)[73]
Critical Category #1		
Health Care	130	100
Public Order & Safety	60	40
Critical Category #2		
Office	750	60
Mercantile	670	40
Food (Sales + Service)	520	40
Service	470	20
Critical Category #3		
Lodging	150	70
Education	330	40
Public Assembly	300	40
Warehouse & Storage	500	25
Religious Worship	300	10

*There is of course not a one-to-one correlation in such data as many of the critical loads, for example in hospitals, are digital in nature, but would not be counted as "microcomputers" in the statistical sources used.

Table 11. Electric Demand: Manufacturing Sector[75]		
Industry	Establishments (thousands)	kW/Establishment (avg)
Primary Metals	4	8,500
Petroleum & Coal Products	2	5,950
Paper	5	5,100
Chemicals	9	4,650
Textile Mills	3	1,960
Transportation Equipment	8	1,350
Beverage & Tobacco Products	2	1,030
Plastics & Rubber Products	12	870
Food	17	785
Computer & Electronic Products	10	780
Electrical Equipment, Appliances, Components	5	690
Nonmetallic Mineral Products	11	680
Wood Products	12	370
Machinery	20	280
Fabricated Metal Products	41	250
Textile Product Mills	4	240
Furniture & Allied Products	11	150
Leather & AlliedProducts	1	150
Printing & Related Support	26	110
Apparel	13	80
Miscellaneous	14	170

ages, however short or long, which depend in turn on how much outages cost the enterprise or agency itself, and those who depend on its goods or services. Secondary losses outside the enterprise may be far larger than those within it. A power failure at a credit-card-verification center, for example, will entail relatively modest internal losses, but may obstruct ordinary commerce for merchants and customers worldwide.

The costs are often very sensitive to the duration of the outage. Even the briefest interruptions can be enormously expensive when they take down the computers that run an airline's entire reservations system, or a financial institution's trading desk, or some manufacturing processes with long "reboot" procedures. Even a momentary loss of the power needed by an air traffic control center, or a process control system in a high-speed automated manufacturing plant, may cause catastrophic losses of life or capital. Refrigerated warehouses, by contrast, may be able to ride through outages lasting many hours without significant loss – but then at some point refrigerated foods begin to spoil, and losses become severe.

That critical power requirements are so highly variable and distributed presents both a problem and an opportunity in the formulation of public policy.

On the one hand, it is not possible to secure requirements for critical power by focusing on the grid alone. The grid is a shared resource; the whole thing simply cannot be hardened enough to meet the needs of the tens of thousands of truly critical nodes scattered throughout the country in both public and private sectors.

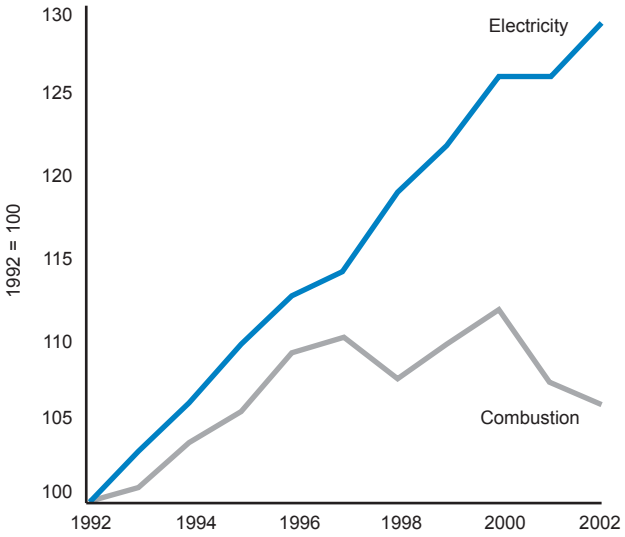
On the other hand, the efforts undertaken to harden these many individual nodes will have a direct, positive impact on the reliability of the public grid as a whole. As noted, large-area power outages are often the result of cascading failures. Aggressive load shedding is the one way to cut off chain reactions like these. The development of a broadly distributed base of secure capacity and well-engineered local grids on private premises will add a great deal of resilience to the public grid, simply by making a significant part of its normal load less dependent on it. Islands of especially robust and reliable power serve as the centers for relieving stresses on the network and for restoring power more broadly. In the aggregate, private initiatives to secure private power will have a very large beneficial impact on the stability and reliability of the public grid as well.

Fueling the Digital Economy

It is increasingly difficult to define just where the *digital economy* ends, and thus by extension, the needs for critical power. Microprocessors are now embedded everywhere, and are often in final control of such mundane activities as opening and closing cash registers and doors. EPRI defines the digital economy to encompass telecommunications, data storage and retrieval services, biotechnology, electronics manufacturing, the financial industry, and

Table 12. Digital Penetration in Manufacturing[76]	
Digital Technology	Share of Manufacturers (%)
Computer-Aided Design	85
Local Area Networks	70
Just-in-Time Systems	60
Computer-Aided Manufacturing	60
Robots	20

Figure 11.
Growth in End-Use Demand*



* Commercial and industrial sector primary energy consumption.

Source: EIA Monthly Energy Review (March 2003).

Growth in Commercial & Industrial Energy Demand
The technologies driving growth in the commercial and industrial sectors of the economy have been mainly fueled by electricity, thereby continually increasing the number and magnitude of critical uses of power.

countless other activities that rely heavily on data storage and retrieval, data processing, or research and development operations. What is clear, in any event, is that all digital hardware is electrically powered; when the electrons stop moving, so do the bits.

However defined, the digital economy is by far the fastest growing segment of the overall economy. Largely as a result, more than 90 percent of the growth in U.S. energy demand since 1980 has been met by electricity. *(Figure 11)*

Even during the most recent years of sluggish economic growth, demand for electricity has continued to rise by 2 to 3 percent annually – and by about 4 percent in 2002 – growth rates that may appear modest but are quite substantial in absolute power (and hardware) terms considering the magnitude of annual U.S. electric use (3.6 trillion kilowatt-hours).

The nearly uninterrupted century-long growth in electric demand (driven, a priori by the preferential growth in technologies that use electricity over combustible fuels) has continued to increase the economy's dependence on kilowatt-hours. The nation is now at a point where electricity accounts for over 60 percent of all fuel used by the GDP-producing parts of the economy (industry, commerce, services) – in 1950, the figure was only 25 percent. *(Figure 12)*

That the trend illustrated in *Figure 11* will continue is strongly suggested by the nature of capital spending which is skewed heavily towards electricity-consuming hardware. Some 60 percent of all new capital spending is on information-technology equipment, all of it powered by electricity, and the most recent data show that percentage rising. *(Figure 13)* All the fastest growth sectors of the economy – information technology and telecom most notably – depend entirely on electricity.

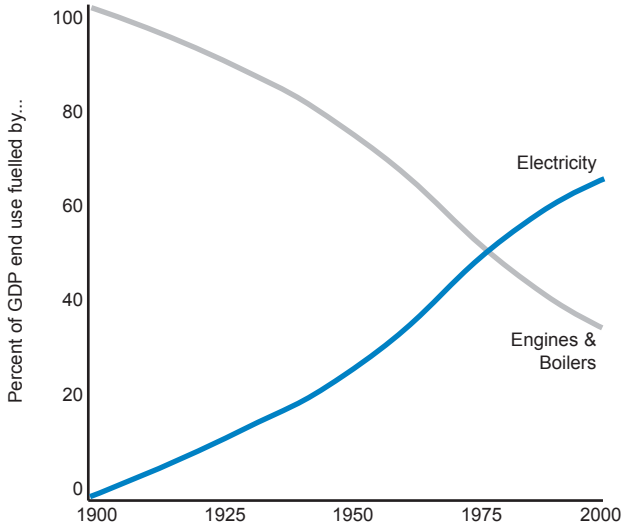
Table 13. Digital Demand (EPRI)[79]

Sector	TWh/year	Percent Share of Sector
Residential	150	13
Commercial	148	13
Industrial	93	9
Total U.S.	391	12

According to surveys conducted by the University of Delaware's Disaster Research Center, large and small businesses in five major business sectors see electricity as "the most critical lifeline service for business operations."[77]

EPRI estimates that approximately 9 percent of electricity used in the industrial sector is now used to power digital hardware, most of it in manufacturing electronic components and in automated process control. *(Table 13)* And EPRI attributes 12 percent of

Figure 12.
End-Use Dependence on Fuel*



* Excludes residential energy: counts only fuels used by GDP-producing sectors; transportation, industry (incl. mining, agriculture) and services.

Source: EIA Annual Energy Review 2000, Bureau of Economic Analysis, and U.S. Census Bureau Historical Statistics of the United States Colonial Times to 1970.

Fueling the GDP
The businesses, activities and technologies that comprise the GDP have grown continually more dependent on electricity.

all U.S. power consumption in 2001 to the operation and manufacture of digital devices (microprocessors, chips, and related systems), digital applications (e.g. home entertainment, digital office equipment, networks, data processing, and digital controls), and digitally-enabled enterprises (businesses that are exceptionally dependent on digital technologies, including security, banking/finance, e-commerce, and data warehousing and management). Our own analysis of the same constellation of digital demands, from desktop to data center, and from factory to chip fab, led us to much the same conclusion as EPRI's, a couple of years earlier.[78] *(Table 14)*

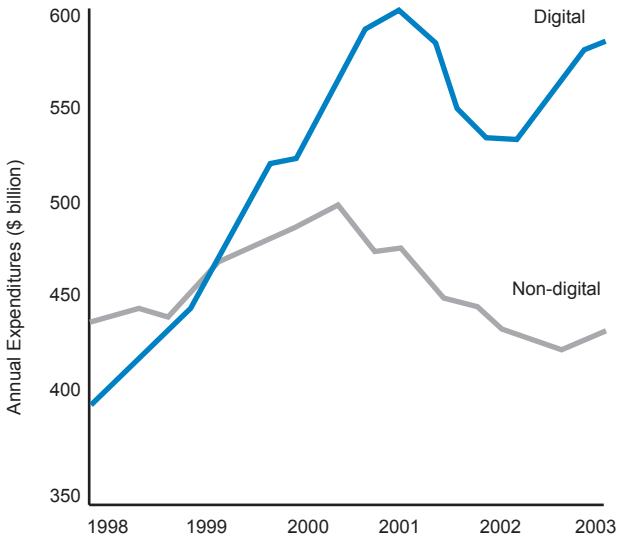
Focusing only on the narrower universe of the digital desktop, the DOE's Energy Information Administration (EIA) periodically estimates that about 1.4 percent of national electric demand comes from PCs and ancillary hardware (e.g. printers, monitors) sitting on desks in homes, and 2.6 percent from machines in offices. (These approximations depend heavily on estimates about usage patterns – how many hours a day our computers, monitors, printers, and other desktop hardware are left running.) In its breakdown of residential consumption of electricity, the EIA also notes cryptically that the other "(e)lectronics, which include audio/video devices and PC add-ons such as scanners and printers, are estimated to account for 10 percent of all residential electricity use," or about 3 percent of total *national* electric use.

Cooling and backup power requirements add another, generally ignored, yet significant component to these totals. They add not only to the absolute magnitude of demand associated with digital loads,

Table 14. Digital Electricity Demand [80]

Source	Percent of U.S. Electricity
Networks	**~1 - 2**
Wired	~0.2 - 0.5
Wireless	~0.2 - 0.6
Data centers	~0.2 - 0.4
Factories	**~2 - 6**
Chip fabs	~0.5
All other digital manufacturing	~2 - 6
Desktops	**~6**
In offices	~2.6
UPS systems	>0.5
In homes	~1.4
Cooling all of the above	~1.5
TOTAL	**9 - 14**

Figure 13.
Capital Spending on Hardware



Source: Commerce Department and Business Week.

Growth in End-Use Demand
Spending on new hardware is heavily biased towards electricity-consuming and in particular highly power-sensitive and often "critical" digital equipment.

but frequently in the former case to yet another critical node. Indeed, a number of computing facilities within factories or offices have been forced to shut down during power failures despite the successful operation of a facility's UPS and backup generators – because the UPS and backup system was not installed to operate the air conditioning system that cooled the computing room. Rapid over-heating lead to the need for manual shut-down of the computing.

Several years ago, a British study was the first to note the related anomaly in the commercial sector – efficiency of conventional electric demand was rising rapidly (lighting, standard equipment, air conditioning) – but overall commercial building electric (and cooling) demand just didn't fall (it rose).[81] The study authors attributed it to the rising direct demand from digital equipment, including rising cooling demand. Recent data for Manhattan suggests a similar trend. Compared to the booming '90s, despite the cooler economy and much higher office vacancies (15 percent v. 5 percent), ConEd reports electric growth now running 25 percent higher in the past year or two – attributing demand to greater use of digital hardware, and to the greater use of air conditioning.[82]

Wireline and wireless communications infrastructures, together with large data centers, account

for another 1–2 percent of total demand. The fastest-growth sector of demand in the EIA commercial building statistics, for example, is a miscellaneous grab-bag category called "other" loads that "(i)ncludes miscellaneous uses, such as service station pumps, automated teller machines, telecommunications equipment, and medical equipment" – this category now accounts for a remarkable 36 percent of all commercial building electric use (12 percent of national demand). The EIA doesn't parse these numbers further, but given the extensive list of equipment that is explicitly counted outside of "other," it seems likely that "telecommunications equipment" is a very important component here.

Finally, the manufacturing of digital equipment accounts for another 2 to 6 percent of total electric demand. In 1998, the U.S. Environmental Protection Agency (EPA) had estimated the nation's fabs (microprocessor fabrication factories) accounted for almost 0.5 percent of national electricity consumption. That number has surely grown since then. The 100 big semiconductor fabs in the United States operate at typical 10 to 20 MW loads per fab, with $1 million/month electric bills. And the manufacturing of information technology extends far beyond the fabs – in fact the fabs almost certainly rank last and least in the digital manufacturing sector's demand for power.

The macroeconomic statistics lend support to these estimates. The U.S. Department of Commerce estimates that the information portion of the economy accounts for at least 8 percent of the GDP.[83] The Federal Reserve estimates that information technology accounts for 20 to 60 percent of GDP growth.[84] And as a general rule, every 1 percent point of GDP growth drives a 0.7 to 1 percent point of kWh growth according to the EIA.[85] Thus, at the macroeconomic level, information technology – if it uses its proportionate share of energy – would appear to account for at least 8 percent of all *energy* use, and a disproportionately higher share of *electric* use.

It is impossible to estimate with any precision how much economic leverage to attribute to these all-digital loads. What is intuitively clear, however, is that securing power supplies to digital loads generally is a high priority, because so much else cannot continue to function when the microprocessors and digital communications systems shut down.

Hard Power

The public grid's inherent vulnerabilities have been noted before. Its architecture – one of relatively small numbers of huge power plants linked to millions of locations by hundreds of thousands of miles of exposed wires – has been frequently criticized, though generally by those who do not understand either the technology or the economics of power production. What is equally clear, however, is that the public grid's architecture is exceptionally efficient. Power plants are thermal machines, and in the thermal world, bigger is almost always much more efficient than smaller. Today's 180 MW frame turbines now attain almost 60 percent thermal efficiency; a 30 kW microturbine attains 26 percent. Utilities running huge turbines produce 3¢/kWh electrons; in the best of circumstances, microturbines can perhaps generate 15¢/kWh power. Even as oil prices have gyrated, the average retail price of utility-generated power has fallen 10 percent since 1990, and wholesale prices are in virtual free-fall. This means that most of the demand will inevitably continue to be satisfied by grid power.

But even before 9/11, it had become clear that the digital economy requires much more than the grid alone can deliver. Utilities have traditionally defined an "outage" to be an interruption of 5 minutes or more. But the Information Technology Industry Council (ITIC) in the guideline known as the "ITIC curve" defines a power "failure" as any voltage that falls below 70 percent of nominal for more than 0.02 seconds, or below 80 percent of nominal for more than 0.5 seconds. Additional parameters address voltages below 90 percent of nominal for more than 10 seconds, and over-voltage conditions that can (all too easily) fry sensitive electronics. The "brownout" – a grid-wide reduction in voltage – is the utility's first response to generating capacity shortages. But a brownout that merely dims bulbs can shut down digital equipment.

The challenge and the opportunity for both public and private planners are to address the new critical-power challenges in ways that solve both problems. Mounting threats from the outside give increasing reason to question the grid's reliability in any event. At the same time, every significant node in the digital economy defines a point of rising demand for power that is exceptionally clean, reliable, and sustainable – far more so than the grid can

ever deliver, even in the absence of any threat of deliberate attack. In a recent survey, security directors at leading U.S. businesses ranked the threat of terrorism among their top five concerns, but few expected to see any increase in their budgets in the next few years.[86] The typical view is that security issues "won't generate revenue, they'll consume capital." The pressure to reduce costs exceeds the pressure to improve security.

With power, however, these two objectives can often be complementary. For many in the digital economy, grid power is inadequate in any event; this is why there has been so much investment already in backup generators, uninterruptible power supplies, and backup batteries. The challenge going forward is to extend investment in power *quality* and *reliability* – which many businesses need and are undertaking in any event – to assure *continuity* of operation in the event of larger and longer interruptions in grid-supplied power.

RESILIENT POWER

Airports have their individual towers, but the flow of commercial aircraft at altitude is controlled by "National Airspace System" (NAS) facilities – about two dozen regional control centers, together with another 19 air-traffic-control hubs co-located in airport control towers at the nation's busiest airports. For obvious reasons, all are deemed "critical." And a typical control tower requires about 200 kW of power to stay lit; the major centers need about 500 kW.

The Federal Aviation Administration (FAA) has long recognized that it "cannot rely solely on commercial power sources to support NAS facilities. In recent years, the number and duration of commercial power outages have increased steadily, and the trend is expected to continue into the future."[87] The FAA has thus deployed extensive critical-power backup facilities – in the aggregate, some 9,000 batteries, 3,000 generators, and 600 UPS systems. The Agency has deployed some 2,000 kW of diesel generators, for example, in double-redundant architectures.

In a year-2000 report,[88] the Agency nevertheless recognized that the extensive backup facilities it does have are seriously insufficient and out of date; a major upgrade is now underway. All of its principal power systems are being equipped with high-resolution sensors, linked via Ethernet networks. A follow-up report in February 2003 reviews the capital investments still required, and stresses that further up-grades are urgently needed.[89] The Agency estimates that it would require approximately $100 million annually to replenish the entire inventory of its backup power systems every 15-20 years.

Tiers of Power

As noted above, the electrical grid is a multi-tiered structure. *(See Figure 4)* Architecturally similar arrays of generators, wires, switches, and transformers appear within each of the grid's principal tiers. The generation and transmission tiers at the top have stadium-sized, gigawatt-scale power plants and commensurately high-voltage wires, building-sized transformers, truck-sized capacitors, and arrays of mechanical and electromechanical relays and switches. *(Figure 14)* The distribution tiers in the middle have tennis-court-sized, megawatt-scale substations, van-sized transformers, and barrel-sized transformers mounted ubiquitously on poles and in underground vaults. *(Figure 15)* The bottom tiers transform, condition, and distribute power within factories, commercial buildings, and homes, via power-distribution units, lower-voltage on-premise grids, and dispersed switches, batteries, and backup systems further downstream. *(Figure 16)*

In the most primitive architecture, the grid is just power plant and wires, no more. Power is generated at the top tier, consumed at the bottom, and transported from end to end by a passive, unswitched, trunk-and-branch network. This was the structure of the very first grid, from Edison's Pearl Street station in New York, in 1882. The higher up things fail, the more widely the failure is felt.

The modern grid is, of course, much more robust. Many different power plants operate in tandem to maintain power flows over regions spanning thousands of miles. In principal, segments of the grid can be cut off when transformers fail or lines go down, so that failures can be isolated before they propagate to disrupt power supplies over much larger regions. (The effectiveness depends on the level of spending on the public grid, which has been in decline for years.) Identical strategies of isolation

Figure 14.

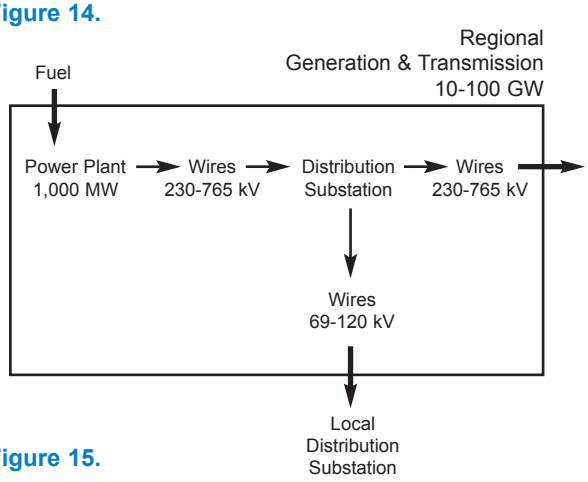


Figure 15.

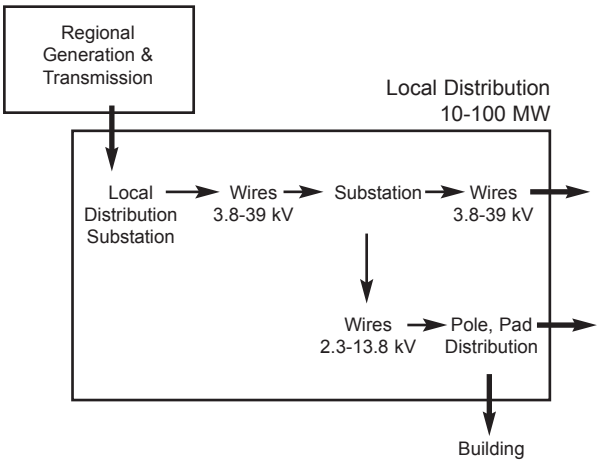
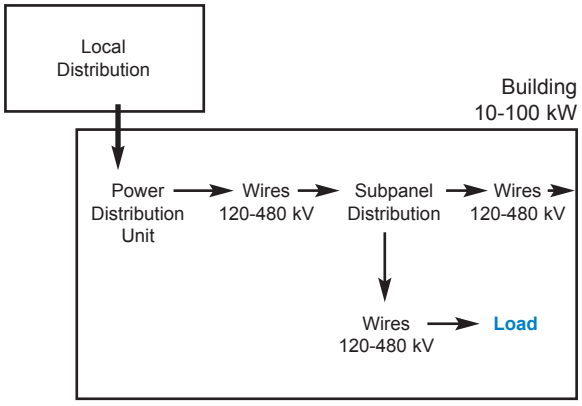


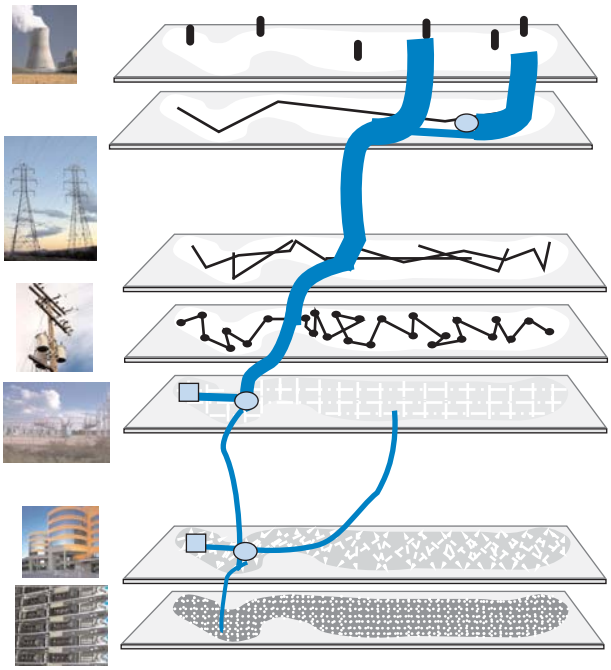
Figure 16.



and redundancy are used on private premises, to make the supplies of power to critical loads much more reliable than the grid alone can be counted on to deliver.

Switches control the flow of power throughout the grid, from power plant down to the final load. "Interties" between high-voltage transmission lines in the top tiers allow even the very largest plants to supplement and backup each other. Distributed generation facilities located in the middle tiers can power smaller segments of the grid, and keep them lit even when power is interrupted in the highest tiers. When power stops flowing through the bottom tiers of the public grid, critical-power circuits on private premises are isolated and private, on-premises generators kick in. *(Figure 17)*

Figure 17.
Adding "Interties," Switches and Local Generation



The first essential step in restoring power after a major outage is to isolate faults and carve up the grid into smaller, autonomous islands. From the perspective of the most critical loads, the restoration of power begins at the bottom, with on-site power instantly cutting in to maintain the functionality of command and control systems that are essential in coordinating the step-by-step restoration of the larger whole.

Adding Logic to the Grid: The Static Transfer Switch

The switches that perform these functions must operate very fast. As discussed earlier, a "blackout" for digital equipment is any power interruption that lasts more than a few tens of milliseconds. Such speeds are beyond the capabilities of an electromechanical switch, however. *(Figure 18)* The most critical switching function must therefore be performed by a high-speed, solid-state device – a "digi-

tal" switch that can open and close circuits fast enough to maintain the flow of smooth, seamless power to digital loads. This device – the "static transfer switch" (STS) thus plays an essential role in mediating between alternative sources of power. It opens and closes power circuits faster than sensitive loads can discern, and faster than destructive harmonics can propagate, providing local isolation, selectively, and on command.

An STS is typically built around a silicon controlled rectifier (SCR) – a fat, six-inch, 1,500-micron-thick silicon wafer, that does for power what a Pentium does for logic; the device is called "static," ironically, because it has no moving mechanical parts, and can thus open and close extremely fast. High-power silicon-based transfer switches were introduced in 1971, but the first such device with fully integrated microprocessor controls did not become available until 1994. *(Figure 19)*

Figure 19.
Static Transfer Switch

Source: Danaher Power Solutions

An STS monitors the availability and quality of power from two (or more) independent sources of power, and instantly flips to a secondary feed upon detecting a sag or similar problem in the primary. The STS thus contains high-speed sensing and logic that allows switching behavior to be tailored, in real-time, to meet the different optimum opening and closing of a circuit (a major factor in preventing upstream and downstream problems). Finally, an STS will typically incorporate redundant design features to ensure high, intrinsic reliability, and sensors to monitor conditions both inside the switch itself, and in the surrounding environment. An internal clock and on-board memory will log power events, and a communications channel (typically fiber-optic) provides links between the logic and the electronics that drive the switch, as well as with UPSs and off-site control systems.

Rack-mounted units can handle up to several kilowatts, while much larger car- and truck-sized devices route major power feeds running as high as 35 MW, and at 15, 25, and 35 kilovolts (kV). These devices can be configured for stand-alone operation. They may switch as needed between two or more primary 'hot' power sources – two different grid feeds and a generator for example. Or they may stand alongside (or be integrated into) UPSs to coordinate power hand-offs among redundant UPS arrays when one unit fails, or to enable "hot swap" maintenance. Rack mounted solid-state switches can perform similar functions directly upstream of end-use devices – servers or telecommunications switches, for example – to select automatically among redundant power feeds so that the failure of any one feed is always invisible to the final load. And at ultra-high power levels – up to 100 MW – enormous arrays of solid-state switches are now being used to interconnect and isolate high-power transmission lines at about 50 grid-level interconnection points worldwide.

Coupled with large capacitors and power-conditioning high-power electronics, complex arrays of solid-state switches become a UPS. When grid power sags or fails altogether, they draw power from alternative sources; they likewise filter out surges and spikes in grid power that may be created by (to pick just one example) lightning strikes on transmission lines.

Figure 18.
Adding Fast Switches

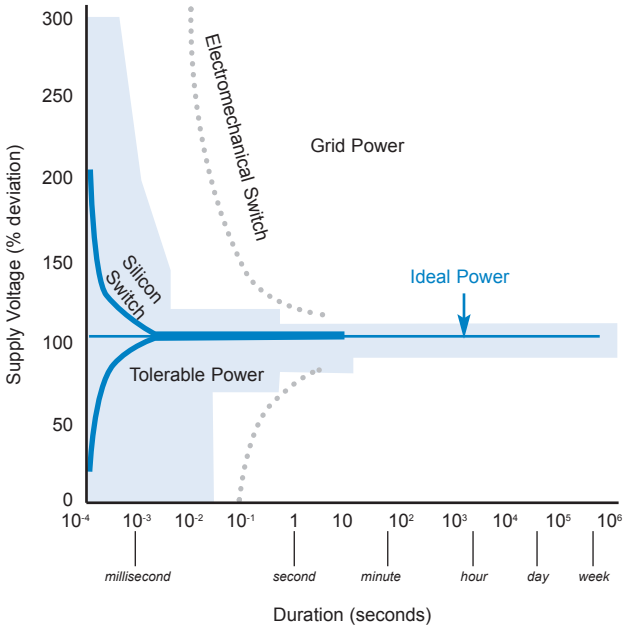
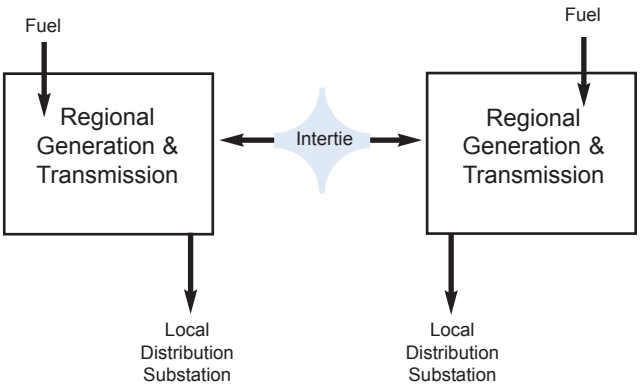


Figure 20



Generation and Transmission

Much of the critical-infrastructure literature refers to the grid as a single structure, and thus implicitly treats it as "critical" from end to end. But as discussed earlier, utilities themselves necessarily prioritize and rank the customers and loads they are expected to serve. Large power plants and high-voltage underground cables that serve densely populated urban areas obviously require more protection before they fail, and more urgent attention after, than small plants and rural distribution lines. In defining priorities and deploying new facilities, collaboration between utilities and critical-power customers is becoming increasingly important. Most notably, power is critical for the continued provision of other critical services – those provided by E911, air traffic control, wireline and wireless carriers, emergency response crews, and hospitals, among others.

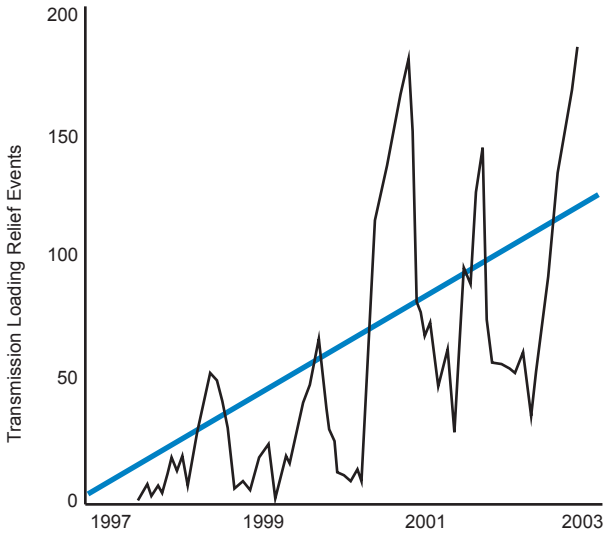
The hardening of the grid begins at the top tier, in the generation and transmission facilities. *(Figure 20)* Much of modern grid's resilience is attributable to the simple fact that interties knit local or regional grids into a highly interconnected whole, so that any individual end user may receive power from many independent power plants, often located hundreds (or even thousands) of miles apart. Promoting development of this resilient architecture is the primary mission of NERC.

Thus, for example, New York's Marcy substation was upgraded in 2002 with high-power silicon switches that boosted the capacity of existing transmission wires by 200 MW.[90] California is now studying the feasibility of adding additional local interties to a major line that already runs from Oregon through Nevada. And after a ten-year wait for multi-state approvals, American Electric Power recently received permission to build a new 765 kV line linking a power-rich site in West Virginia to the power-hungry Virginia loop.

Initiatives like these were being pushed long before 9/11, because rising demand and increasingly strained supply were causing alarming increases in transmission congestion "events." *(Figure 21)* New interties provided an effective way to boost overall reliability and create capacity margins without building new plants; new interties also facilitated the wholesale trading that regulators had authorized in the 1990s. So long as there is sufficient margin in the generating capacity and redundancy in wires, and sufficiently fast and accurate control of key switches that route power and isolate faults, the failure of any one power plant or line in the top tiers of the grid should never be discerned by end users at the bottom.

After 9/11, NERC expanded their recently created Critical Infrastructure Protection Advisory Group (CIPAG) to bring together the various public utilities responsible for securing the 680,000 miles of long-haul, high-voltage wires and the 7,000 transmission-level substations.[91] Among other initiatives, CIPAG has formed a working group to inventory and develop a database of "critical spare equipment." The high-voltage transmission system uses high-power hardware – massive substation transformers, for example – that is often custom-built. Spares, if they exist at all, are rarely close at hand. Much can thus

Figure 21.
Electric Grid Congestion



Source: North American Reliability Council (NERC) Transmission Loading Relief Logs.

Figure 22

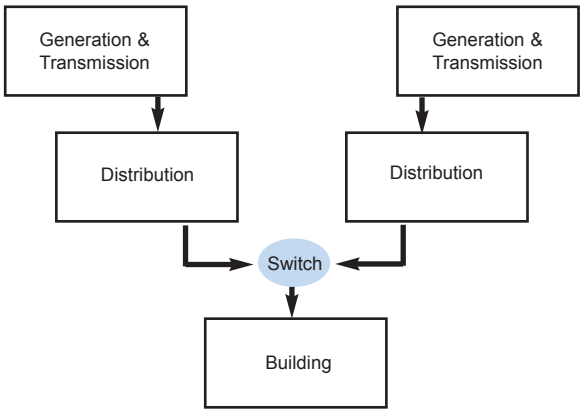
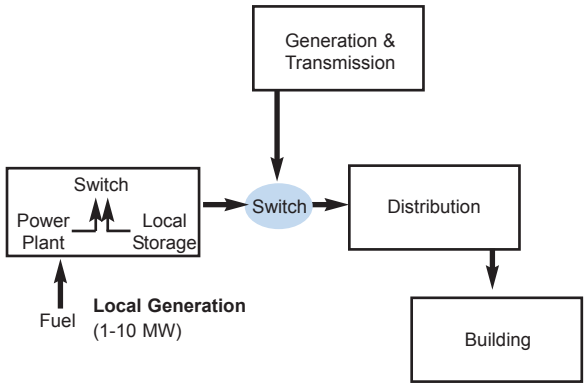


Figure 23



be done to assure overall continuity of operation through the intelligent sharing of stand-by assets.

Complementary discussions are addressing the possibility of creating a critical-equipment warehousing system, with spares warehoused at geographically dispersed locations, and the costs shared by the many potential beneficiaries of such planning. This solution has already been implemented for power line ("telephone") poles. As discussed further below – fleets of generators-on-wheels are now evolving as well.

Distribution and Distributed Generation

Very large end users rely on similar intertie strategies one tier lower down in the grid to help secure their specific critical-power needs. At AOL's campus in Prince William County, Virginia, for example, a dedicated substation takes two separate 115 kV feeds from the grid. AOL also deploys backup generators of its own, but when critical-power loads are located in urban areas where on-site generation is infeasible, redundant connections to separate, electrically independent points on the grid are often the only practical approach for improving reliability. *(Figure 22)*

In such configurations, the key "switch" controlling the dual feeds will often be a dedicated utility substation located on the doorstep of a factory, office park, or data center. The two separate high-voltage feeds to AOL's campus, for example, lead to a dedicated substation that steps the voltage down to 24 kV through redundant transformers, and feeds the power to two 25 kV sets of switchgear. By deploying additional substations in close collaboration with major critical-load customers, utilities shrink the footprint – i.e. reduce the number of customers affected – by failures that occur elsewhere. And more substations create more points at which to interconnect independent parts of the grid, so that distant transmission lines and power plants effectively back each other up.

Substations can also serve as sites for utility deployment of distributed generation. With the addition of its own generating capacity, the substation is "sub" no longer – it becomes a full-fledged "mini-station." *(Figure 23)* Opportunities for deploying new generating capacity at this level of the grid – either permanently or when emergencies arise – are expanding as large electro-mechanical switches and related components are being replaced by new solid-state technologies (described in more detail below) that have much smaller footprints.

Figure 24.
Substation Diesel Gensets

Source: Cummins Power Generation

Utility-scale "generators on wheels" – either diesels or gas turbines – offer an important option for deployment in emergencies. Some substations already play host to small parking lots worth of tractor-trailers, each carrying 1 to 5 MW of generators powered by Cummins or Caterpillar diesel engines. *(Figure 24)* Cummins'

Kawasaki turbines, GE's Energy Rentals division, and Caterpillar's Solar Turbine division offer mobile generating capacity in larger (10 to 25 MW) increments, powered by aeroderivative combined-cycle gas turbines, typically housed in a group of three or four trailers. Even larger turbines are being mounted on barges, for quick deployment at substations located near navigable waters and with suitable gas lines close at hand. Some 74 turbines, with 2,000 MW of capacity, already float on power barges around Manhattan.

For the longer term, the DOE and many utilities are examining other possible sources of substation-level generation and storage. Large fuel cells present a potentially attractive alternative to gas turbines because they operate silently and with very low emissions.[92] Utilities have even tested megawatt-scale arrays of batteries for load-leveling and backup. In one trial a decade ago, Southern California Edison and other utilities assembled 8,256 telecom-type lead-acid batteries in a massive 10 MW array, fifty miles outside of Los Angeles; the idea was to store grid power during off-peak hours of demand, and feed it back into the grid as needed. TVA is scheduled to bring on line this year a massive 12 MW flowing battery-type system called Regenesys (the electrochemistry is based on sodium bromide and sodium polysulphide); it can store 200 MW hours of energy in its 170,000 square-foot footprint.[93] As discussed further below, many of these studies (including two outstanding DOE reports published in 1999 and 2002)[94] have focused either on environmental objectives, or on smoothing out demand to lower prices by making more efficient use of the grid and other utility resources.

By such means, much can be (and is being) done to lower the likelihood of a loss of grid power needed by the most critical loads. As discussed further below, closer collaboration between utilities and their largest customers is now needed to advance such initiatives in the distribution tiers of the grid. Nevertheless, as discussed above, the grid is inherently frail, and there is only so much that feasibly can be done to make it less so. Mushrooming arrays of computer and telecom equipment in switching and data centers increasingly strain the utility's ability to provide sufficient quantities of power even when plants and the grid are all functioning normally. Guaranteeing supplies of critical power at locations like these ultimately means adding on-site generating capacity and storage to back up whatever is being done to improve reliability higher in the grid.

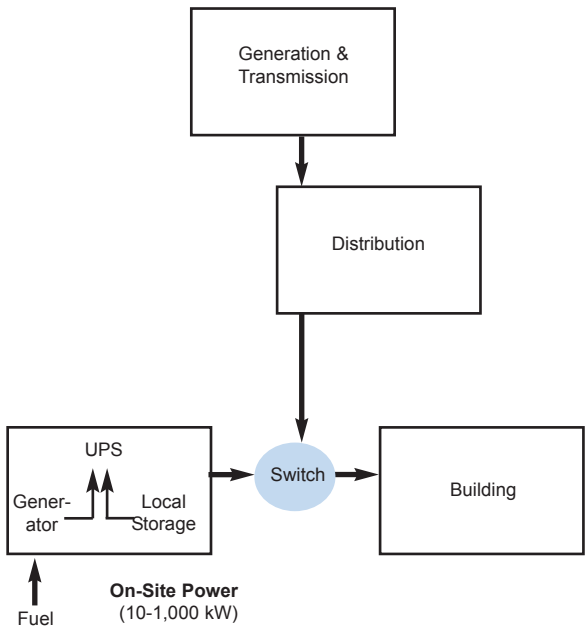
On-Site Power

On-site power begins with on-site supplies of stored electrical, mechanical, or chemical energy. Engines, generators, and suitable arrays of power electronics are then required to generate power and condition it into suitable form. *(Figure 25)*

As noted, the boundaries between grid and on-site power are beginning to blur. Utilities build dedicated substations on the doorsteps of large customers, and may deploy distributed generation facilities at grid-level substations that serve the most critical loads. And while private contractors do most of the planning and installation of the facilities discussed below, utilities themselves are now actively involved in deploying on-site power to help guarantee what the grid alone cannot. According to recent surveys, almost 40 percent of utilities are now offering back-up-power systems to commercial and industrial customers; most of the rest plan to begin offering such product/service contracts within the next few years, in collaboration with genset, microturbine, and fuel-cell manufacturers.[95]

A large technical literature already addresses the elements of on-site power systems. The IEEE's Recommended Practice for Emergency and Standby

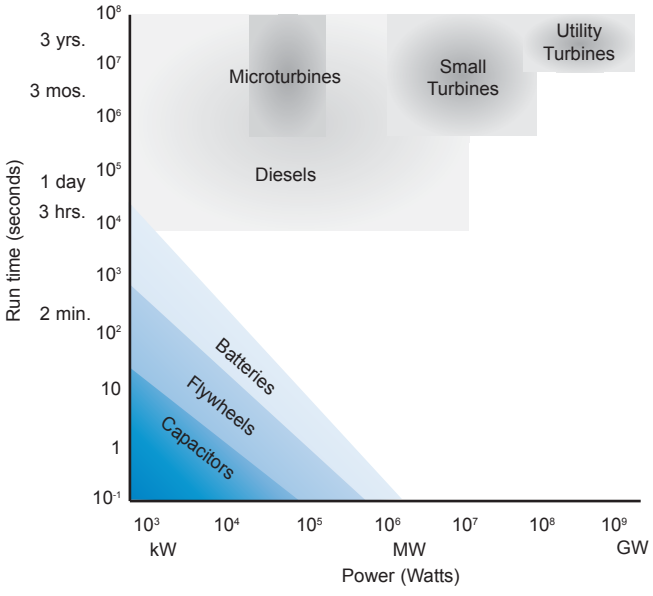
Figure 25



Power Systems for Industrial and Commercial Applications provides comprehensive technical and engineering evaluations of, and guidelines for, engineering, reliability, and operational aspects of on-site power systems. The National Fire Protection Association's (NFPA) Standard for Emergency and Standby Power Systems provides a comprehensive technical analysis of on-site power alternatives.[96] The first edition of the Standard emerged after the NFPA convened a Technical Committee on Emergency Power Supplies in 1976, to address "the demand for viable guidelines for the assembly, installation, and performance of electrical power systems to supply critical and essential needs during outages of the primary power source." The 2002 edition details hardware choices for batteries, generators, fuel tanks, cable connectors, switches, fuses, controls, mechanical layouts, maintenance, testing, and virtually all other aspects of hardware options, installation requirements, and operational capabilities.

Some part of the growth in demand for on-site power can be attributed to lack of adequate transmission-and-distribution capacity. With suitable engineering of the public-private interfaces, private generators not only reduce demand for power, they can also feed power back into the public grid. Some additional part of the rising demand for on-site power is attributable to growing interest in "alternative fuels" (such as fuel cells and photovoltaics) and co-generation. Certainly there has been a long-standing recognition of the role of on-site power for emergencies (caused, for example, by natural disasters) as is implicit in the NFPA document noted above. But in the aftermath of 9/11, the principal imperative for deploying on-site power is to assure continuity of critical operations and services.

Figure 26.
Generating and Storing Electricity



Source: Digital Power Group

Stored Energy

Energy can be stored electrically (in capacitors, for example), electro-chemically (batteries), mechanically (flywheels) and chemically (diesel fuel). By and large, however, these storage technologies fall into two groups that perform distinct functions. *(Figure 26)* Batteries, flywheels, and ultra-capacitors are mainly "ride-through" technologies. They store quite limited amounts of energy, but can provide power quickly, to cover sags and outages that run from milliseconds to minutes or (at the outside) hours. Liquid fuels, by contrast, store large amounts of energy – enough to run backup generators for much longer periods. Diesel fuel and backup generators can thus provide what ride-through technologies cannot – critical-power "continuity" when grid power fails for many hours, days or longer.

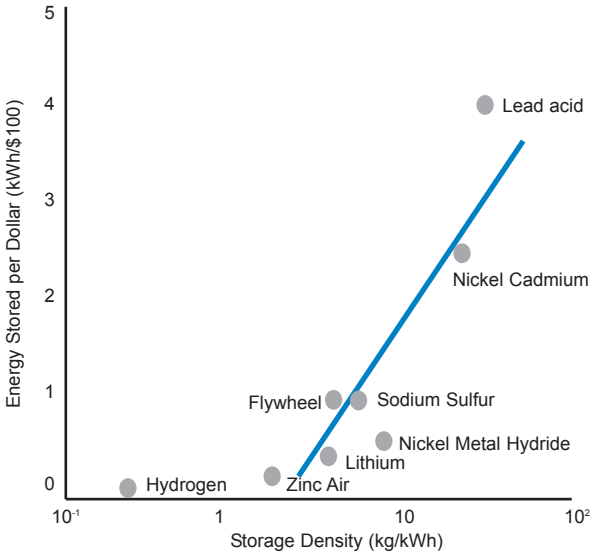
Batteries

Rechargeable batteries remain the overwhelmingly dominant second-source of power. Batteries are widely used to provide ride-through power for the most common grid interruptions and outages, which is to say, the relatively short ones.

Portable devices rely on the exotic, expensive and often unstable battery chemistries of lithium, cadmium, nickel, silver, and zinc. These materials offer very high power densities – so the batteries are commensurately compact and light – but they are very expensive. They store far more energy per pound, but far less per dollar. Lead and acid are comparatively heavy and cumbersome, but they are also affordable, and no other battery chemistry has yet come close to beating them for all around utility. *(Figure 27)*

"Flooded" lead-acid cells store about 20 percent more power than other lead-acid designs, but they vent hydrogen and oxygen (an explosive mixture), and have to be watered periodically, either manually or (increasingly) by way of automated systems. Absorbed-glass-mat and gel-based batteries run sealed – they recombine the electrolytic gases within

Figure 27.
Cost to Store Grid Power



Source: "Metal Fuel Cells," IEEE Spectrum (June 2001); "Portable Power," Buchmann, Cadex Electronics (2000); "Exoskeletons for Human Performance Augmentation," DARPA Workshop (1999), Defense Sciences Office; Electricity Storage Association.

the battery, rather than vent them. These low-maintenance units can go pretty much anywhere safely – in enclosed cabinets, office environments, and basements. *(Figure 28)*

Battery manufacturers continue to pursue new chemistries. The high-temperature sodium-sulfur battery is a candidate to fill the niche between lead-acid and expensive lithium for high-energy storage. In late 2002, American Electric Power deployed the first U.S. commercial installation; a 100 kW system with two massive batteries able to provide seven hours of run time in about one-third the floor space of a lead-acid array.[97] But neither sodium-sulfur nor the sodium-bromide batteries noted earlier, are yet close to matching the venerable lead-acid technology's economical performance or the high reliability that comes with a huge market and a long history of operation.

Figure 28.
Telecom Back-Up Batteries

Source: Enersys

Flywheels

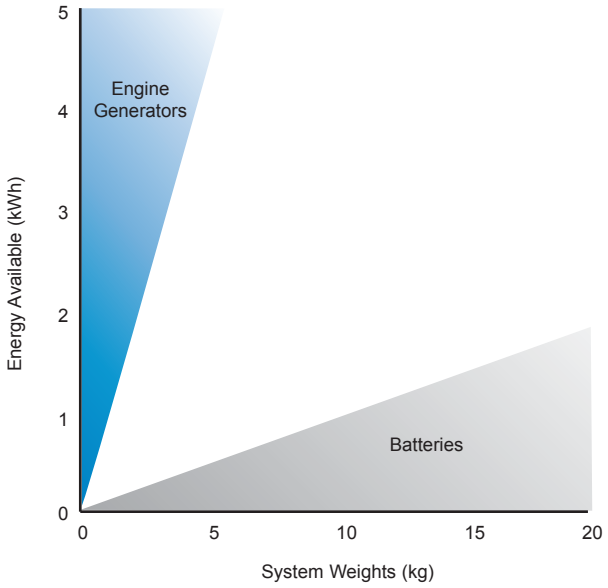
For the most part, flywheels are even more limited than batteries in their practical ability to address the energy deficits created by any extended grid outage. They can and do substitute for batteries, however, to ride-through the short gap between the time when grid power fails and backup generators get up to speed. One of the commercial flywheel-based ride-through power units on the market today consists of two 600-pound steel flywheels, stacked vertically, and spinning silently in a vacuum at 7,700 rpm; the wheels are connected to integrated motor/generators on a single shaft, with an array of electronics beyond the generator that converts the highly variable power generated by the spinning flywheel to the steady AC or DC outputs required by the loads.[98] Such designs can produce as much as 250 kW of power for 15 seconds, or 1 kWh of total energy.

Another emerging configuration uses a blend of static (battery) and active (flywheel) backup systems, with the flywheel used to handle the shortest and most frequent power dips (which range from milliseconds to fractions of a minute), with the batteries taking over for somewhat longer outages. In this configuration, the flywheel's main function is to extend the life-span of the batteries, which are substantially degraded when they are required to respond repeatedly to short-term dips in grid power.

Ultracapacitors

Ultracapacitors are increasingly being used to perform a similar function – to ride-through the gap between the failure of grid power and the start-up of a backup generator. The ultracapacitor's energy storage and performance characteristics are very similar to a flywheel's, but these devices contain no moving parts. Through advanced thin-film technologies, micro-material engineering, and automated production lines, a handful of manufacturers now make one-pound, soda-can-sized capacitors that deliver 2,500

Figure 29.
Storing On-Site Electrical Energy



Farads of capacitance (thousands of times more than conventional capacitor technology), and both price and size continue to fall steadily. Arrays of such capacitors are used, for example, to provide ride-through power in 10 kW computer servers. Once again, ultracapacitors don't eliminate batteries in most applications, but they can greatly improve battery functionality and expand battery markets overall.

Diesel Fuel

With or without the assistance of complementary flywheels and ultracapacitors, batteries store far less energy per unit of volume or weight than liquid hydrocarbon fuels. The battery banks in telecom central offices, which typically provide the office with a reserve time of four to eight hours, push the outer limits of battery backup. Cell tower base stations were originally designed around four-hour battery backup systems, but loads have risen to the point where few towers can run longer than an hour when grid power fails, and an hour of run time is achieved only if the batteries have been well-maintained. With rare exceptions, few facilities can economically rely on battery power for even that long; batteries are too bulky and too expensive to provide power for the even longer grid outages that must now be contemplated in critical-infrastructure planning. *(Figure 29)*

Generators powered by liquid fuels will therefore play the key role in maintaining continuity through major grid outages. They can do so because liquid fuels store huge amounts of energy in very small volumes, because these fuels power the transportation sector for just that reason, and because the United States therefore has in place a huge, distributed infrastructure of trucks and tanks that transport and store primary fuel in quantities sufficient to keep key electrical loads lit for weeks or more. The far-flung, highly distributed infrastructure of diesel storage tanks is effectively invulnerable to the kinds of catastrophic failures that could incapacitate major power lines or gas pipelines.

Most backup diesel generators burn distillate fuel oil, the same fuel used for heating, and for aircraft. Trucks account for about half of U.S. distillate fuel consumption, and distillate fuel storage tanks are therefore already dispersed wherever trucks travel. Nearly 200,000 filling stations, for example, have underground storage tanks and many store diesel fuel specifically. Aviation accounts for another one-third of U.S. consumption; some 18,000 small (and large) airports thus provide a second major tier of dispersed storage. In addition, some 400,000 commercial buildings and eight million homes have storage tanks for their heating oil. And the United States has some 9,000 regional oil distribution centers.[99] Many diesel generators are also configured for dual-fuel operation, and can thus also burn natural gas or propane, and stores of these fuels are extensive and dispersed, as well.

A standard 275-gallon residential heating oil tank, for example, contains enough energy to generate 4,000 kWh, or some 40 times as much as a comparable volume of lead-acid batteries. And fuel tanks can be refilled by truck. If (say) 10 percent of the nation's electric loads are viewed as "critical," then

Table 16. On-Site Power Sources

Type	Power (kW)	Cost ($/kW)	Efficiency (%)	Emissions (lb NOx/1000 kWh)	Fuel
Reciprocating Engine	10-10,000	300-800	25-50	17/6	Oil/gas
Aeroderivative Turbine	10,000-60,000	500-1,700	30-60	1	Gas
Microturbine	20-100	900-1,800	25-30	0.3-0.5	Gas
Fuel cell	10-250	5,000-10,000	50	0.02	H (gas)

Source: "Using Distributed Energy Resources," www.eren.doe.gov/femp/

one week's supply of our national fuel oil consumption would provide roughly one month of critical power.

Backup Generators

Backup diesel generators located in basements and parking lots, and on rooftops, now account for some 80,000 MW of backup generating capacity deployed near critical loads across the United States. There are, by contrast, only about 100 MW of natural gas-powered microturbines and 25 MW of fuel cells (100 units) installed. Diesel gensets are available in a wide range of sizes; on balance, they are cheap, readily available, and reliable, and modern designs run remarkably efficiently and cleanly. *(Table 15)* While all of these technologies are improving year by year, the marketplace has made clear that the diesel genset remains, by a wide margin, the most practical and affordable alternative for most backup applications.

Figure 30.
Diesel Genset

Source: Cummins Power Generation

Diesel Gensets

To provide critical power for longer periods, the backup system of choice is the stand-by diesel generator. Sized from 10s to 1,000s of kilowatts, diesel gensets can provide days (or more) of backup run time – the limits are determined by how much fuel is stored on-site, and whether or not supplies can be replenished during an extended outage. *(Figure 30)*

Diesel generators are strongly favored over other options because they strike the most attractive balance between cost, size, safety, emissions, and overall reliability. Large power plants generate much cheaper power with coal and nuclear fuel, but only because they are very large, and are generally built where land is cheap, far from where most of the power they generate is consumed. They therefore depend on a far-flung grid to distribute their power – and the grid is exposed, and therefore vulnerable. Large gas turbines are attractive alternatives that are already widely used by utilities, but they come in 15 to 150 MW sizes – far too big for all but a tiny fraction of critical loads that require on-site power. And they are no more reliable than the gas pipelines that deliver their fuel.

For these reasons, diesel gensets under 3 MW have emerged to define a huge installed base of generating capacity. *(See Figure 6)* Thus the FAA as earlier noted, for example, relies on nearly 3,000 diesel generators to ensure back up power for its air traffic control centers, and tens of thousands of other diesel gensets are used to backup airport towers, hospitals, military bases, data centers, and other critical-power nodes. If both of the two primary grid feeds fail at AOL's campus in Prince William County, Virginia, the substation turns to power from a thirteen-unit string of 2 MW diesel generators, sitting on five days of fuel oil. Company-wide, AOL alone has 74 MW of backup generating capacity at its current facilities, with 26 MW destined for facilities under construction. In response to serious problems created by a power outage caused by Tropical Storm Isidore in 2002, Jefferson Parish, Louisiana (as just one example of such actions) approved installation of 17 diesel generators at its drainage pump stations.

As noted above, power plants-on-wheels are of increasing interest to critical-power planners, because they offer the economies of sharing in much the same manner as fire engines, rescue vehicles, and the "critical spare equipment" program being developed by utilities. Companies like Cummins and Caterpillar have built (still relatively modest) fleets of 2-5 MW, trailer-mounted diesels, and these can be used to generate private, on-site power, just as they can be used by utilities for emergency generation at the substation level of the grid. In the aftermath of power outages caused by floods and hurricanes, the Army Corps' 249th Engineer Battalion (Prime Power) installs emergency trailer-mount generators at hospitals and other critical sites. Given the many obstacles – both cost-related and regulatory – that impede permanent deployment of backup generators, fleets of strategically positioned mobile power units offer the most practical assurance of power continuity for many critical applications.

Microturbines

Refrigerator-sized, gas-fired, air-cooled, very-low-emissions microturbines now come in sizes ranging from 30 to 100 kW. Capstone is the dominant player in this power niche. For tens of thousands of small electric loads in urban areas, these gas turbines represent an attractive alternative option for on-premises power. With very high power density they are 2 to 5 times as compact as the only commercial fuel cell being sold today. And when running on natural gas, just about as clean. They are lighter and quieter than diesel engines – that is why turbines are used to power aircraft – and they can be configured to run on either gas or diesel fuel. With some exceptions, however, they are not yet price-competitive with diesel gensets for most backup applications.

Fuel Cells

Fuel cells present another attractive, but even longer-term alternative. Their main virtue is that they can run very clean and quiet, and can thus be deployed directly on commercial premises. Two 200 kW ONSI units, for example, situated on the fourth floor of the Conde Nast Building, at 4 Times Square in the heart of Manhattan, power a huge sign on the building's façade. Other units under development by the likes of Ballard and Plug Power span the 5 to 250 kW range. Those under development by Siemens Westinghouse Power, and Atek range from 25 kW to 25 MW. FuelCell Energy and the United Technologies' ONSI build for the 200 kW to 2 MW space. But fuel cells remain, for the most part, a novel, relatively unproven, and comparatively expensive technology, and absent large on-premises gas storage tanks, they cannot offer any more continuity assurance than the gas lines that feed them. They are also quite a lot bulkier than diesels – a complete two-module, 2 MW fuelcell set-up from FuelCell Inc. occupies about 4,500 square feet; a 2 MW diesel set-up, by comparison, requires only a 1,200 square feet footprint.

Alternative Fuels and Technologies

Other generation technologies run on the much-promoted "alternative" fuels – sun and wind, most notably. But for now, at least, these alternatives are no more reliable than the fuels themselves, or the backup batteries deployed alongside; they are also uneconomical and – because they rely on such thin fuels – require a large amount of space to generate comparatively small amounts of power. With 2,000 square feet set aside for on-site power, a diesel generator together with ancillary power conversion electronics and a buried fuel tank can provide a megawatt of power for a week (i.e. 100 MWh of total electrical energy). On the same footprint, a solar array with its essential backup batteries can provide only 1/100th as much power, and at roughly 100 times the capital cost.

Over the long term (and discussed briefly later), a more promising alternative to conventional gensets will emerge with the maturation of hybrid-electric trucks, buses, and cars, offering the possibility of linking the transportation sector's mobile, and highly distributed infrastructure of fuel tanks, engines, and generators directly to residences, small offices, and larger buildings.

"Uninterruptible Power"

Dual feeds to the grid, on-site batteries and generators, and the static transfer switches used to knit them together are all deployed to ensure the uninterruptible flow of power to critical loads. But the definition of the word itself – "uninterruptible" – depends a great deal on what kind of load is being protected. As discussed earlier, even a short loss of power can trigger a much longer interruption of business or manufacturing operations, because of the time it takes to reboot computers and restart machines. The purpose of a UPS is to isolate critical loads from even the momentary power interruptions that occur when grid power fails and batteries, generators, or other alternatives kick in, and to provide intelligent mediation between these alternative and redundant sources of power.

UPS typically refers to an AC device, used mainly to power computers; DC power plants perform a similar function in the telecom world. The power plants come in modular units, up to about 100 kW (DC), and 720 kW (AC). They are deployed in scalable architectures, with multiple units to accommodate loads running as high as megawatts. End users have deployed some 20 GW of UPS capacity, which represents an aggregate capital investment of over $4 billion. *(See Figure 5)*

A UPS performs two basic, complementary functions. It conditions power continuously, smoothing out the sags and spikes that are all too common on the grid and other primary sources of power. And by

drawing on limited reserves of stored energy in large capacitors and on-board batteries, the UPS provides ride-through power, to cover for sags or complete power failures typically for up to (but rarely longer than) about 30 minutes. The power conditioning is performed by large arrays of digitally controlled power electronics; for ride through, the UPS dynamically selects and draws power from grid, batteries, backup generators, and other available sources. High-power applications may require multiple UPSs, and ensuring proper electrical synchronization is then a major technical challenge. Architectures must be designed to permit individual modules to be taken off-line for maintenance without removing the load from the conditioned power. The UPS will also monitor battery conditions and prevent destructive power flows (harmonics) among these various sources of power. Efficiency, economy of operation, and inherent reliability are essential. Sophisticated communications channels link the best UPSs to downstream loads, upstream power sources, and the static transfer switches that perform the higher-power switching functions.

At the heart of the UPS is its power conversion electronics – the silicon-based hardware that converts electricity from one form to another. Only in the past decade or so have the core high-power electronics matured to the point where they can provide cost-effective, efficient, reliable, digital-quality performance. The key enablers were the advent of high-performance high-power power chips, on the one hand, and, on the other, sophisticated, low-cost digital logic to provide intelligent control. UPS efficiencies have risen substantially – a significant factor in itself both in terms of heat management, and cost of 24/7 operation. And superior power chips and designs have more than doubled the overall reliability of high-power power-conversion electronics.

In top-of-the-line devices, monitoring and software systems now play as crucial a role as the hardware. The software ensures smooth selection of power sources and load hand-offs. It continuously monitors and diagnoses the state of the grid, batteries, and sources of power, together with the condition of the UPS's own internal electronics. It provides predictive analysis of downstream problems – e.g. current leaks that foreshadow the imminent failure of a capacitor or the insulation on a wire. And it provides automated notification and alarms, e-mails, paging, Web-based alerts, interfaces, and so forth. *(Figure 31)*

Figure 31.
Uninterruptible Power Supply

Source: Powerware

Monitoring, Control, and Reliability-Centered Maintenance

Monitoring and maintenance already play a key role in maintaining power reliability, from the gigawatt-scale tiers at the very top of the grid, down to the UPS and individual loads at the very bottom. Such systems play even more essential roles in the stabilization of still-functioning resources, and the rapid restoration of power to critical loads after a major failure of any significant part of the grid.

Grid-Level Monitoring and Control (SCADA)

At the grid level, SCADA systems are used by utilities and regional transmission authorities to monitor and manage power distribution grids and substations. A control center monitors a utility's generating plants, transmission and subtransmission systems, distribution systems, and customer loads. It oversees the automatic control of equipment in the field, and dispatches trucks as needed for manual intervention. Communication with the field equipment typically occurs over dedicated, utility-owned communications networks – analog and digital microwave and radio systems, and fiber-optic lines. Remote terminal units in the field collect data and communicate with control centers via these networks. New substations and equipment are beginning to incorporate "intelligent electronic devices" that push some of the intelligence and decision making into the field, closer to the action.

SCADA greatly improves reliability and provides the essential control infrastructure for the orderly restoration of power after a major outage in the higher tiers of the grid. But the existence of the control system itself creates new points of vulnerability. The SCADA sensors and control centers themselves have to remain powered, and thus define new critical-power nodes that need exceptionally robust and reliable backup power systems of their own. And the cyber-security of the SCADA computers and communications channels has become a major concern in its own right: The number of cyber attacks on the utility SCADA system has been rising rapidly. Sandia National Laboratories has been designated as the federal entity in charge of studying, providing solutions for and promoting SCADA security.[100]

Monitoring and Controlling On-Site Power Networks

Grid feeds, static switches, batteries, backup generators, and UPSs likewise depend increasingly on embedded sensors and software to monitor their state and coordinate their operation with other components of a power network. Combined with GPS systems and extremely precise clocks, sophisticated analytical engines can determine the location, nature, and trajectory of failures at nearly every level, from specific pieces of equipment on up to the level of the building and beyond. In the past, many customers with critical power loads have been reluctant to let information of this kind leave their premises. But off-site monitoring services bring economies of scale and scope to these information-centered services, and with the advent of highly secure communications networks, use of such services is now growing rapidly. *(Figure 32)*

Figure 32.
Power Management Software

Source: SquareD

Power-management software is increasingly being used as well, to provide overarching supervision and control. At the very least, such products can orchestrate the graceful shutdown of critical systems when power outages extend beyond the limits that on-site backup systems can handle. More sophisticated systems can direct the selective, sequential shedding of on-site loads, so that the most critical functions are the best protected. Recently commercialized solid-state circuit-breaker boxes, for example, permit a highly granular and dynamic triage of downstream loads, so that in the case of an extended outage limited battery power can be reserved for the most critical subsystems, with all others shut down – bringing aerospace levels of power control to building systems.

Extensive sensing and advance wired and wireless communications capabilities support the remote monitoring that is essential for all larger power networks. Such networks permit power-network managers to remotely monitor and control a UPS and all the equipment it protects. On-site power-control networks can link the UPS to power adapters deployed at critical loads, allowing the UPS to monitor key loads and optimize the distribution of power among them. These same power-control networks can communicate with the sensors and microprocessors embedded in static transfer switches, to monitor upstream sources of power, synchronize alternative power inputs, and react immediately to fluctuations or interruptions in supplies of power. The software can then control, stabilize, and isolate problems in real time.

For now, however, the networks that monitor and control on-site power operate entirely apart from those that monitor and control the grid. Given how heavily on-site power networks both depend on, and can interact with, the public grid, a key, long-term objective must be the integration of public and private power-control networks. We return to this issue later.

Reliability-Centered Maintenance

One of the most refractory problems in the assurance of critical power centers on whether or not backup equipment will actually work when a crisis hits. Batteries, for example, are notoriously unreliable unless meticulously maintained, and a key function for power management software is to provide both manual and user-defined battery tests for each

UPS on the network. To address similar problems, the aviation industry relies heavily on "reliability centered maintenance" (RCM) to reduce the risks of catastrophic in-flight failures. RCM is, however, a relatively new concept in the critical-power industry, and it is very much more difficult to implement effectively than one might suppose.

Ironically, many reliability problems are created by maintenance itself, when, for example, technicians neglect to reconnect wires or flip switches after testing systems to establish that they are still working properly. A building's "power distribution unit" (PDU), for example, is an array of wires, mechanical clamps, switches, and circuit breakers that receive electric power from one source and distribute it to multiple loads. One common preventative maintenance policy centers on periodically measuring power flows through circuit breakers. To do so, a technician must open the PDU and clamp a meter to wires leading from the breakers. But that activity itself may unintentionally trip a breaker. Other maintenance-created problems are more pernicious, and will not be revealed until a major outage upstream exposes the concealed vulnerabilities.

Some of the most useful critical-power investments thus center on seemingly routine upgrades that swap older hardware with state-of-the-art replacements, which have built-in digital intelligence and monitoring capabilities. New PDU circuit breakers, for example, integrate sensors on to each wire, allowing the continuous, remote monitoring of current flows through each breaker. Reliability-centered maintenance can then be at least partially automated, with the human element removed to a distance, where it is much more likely to add to reliability than to subtract from it.

Changes as seemingly simple as speeding up the performance of circuit breakers can greatly lower the likelihood of serious continuity interruptions precipitated by the power-protection hardware itself. Standard burn-out fuses – rather than circuit breakers – are the last line of defense in all circuits; when all else fails, power surges must be kept from destroying critical loads. Fuses are used, however, because ordinary circuit breakers flip open relatively slowly in many high-power emergency situations. And, the breaker in this case also creates an "arc flash" producing damaging electrical noise. A standard fuse creates no such noise because it burns out much faster - but the power then stays off until a technician manually replaces it. Recently developed fast-acting circuit breakers that eliminate the arc-flash can replace fuses in such applications, and can be remotely reset when sensors report the problem is clear. *(Figure 33)*

Finally, sensor- and software-driven predictive failure analysis is now emerging, and will certainly become an essential component of next-generation RCM. By continuously monitoring the power waveforms, at every critical node in a system, unique signatures of many emerging problems can be recorded before failures occur. These algorithms cannot, of course, predict deliberate assaults on the network, but by making on-premises grids and backup systems much more robust, they can greatly increase the likelihood that such assaults will not in fact interrupt the delivery of power to critical loads, and they can greatly improve the mean-time-to-repair or recovery.

Table 16. Typical power equipment failure rates*

Equipment	Failure rate (per 1000 units)	Downtime per failure (hours)
Generator	170	450
Small transformer	6	300
Large transformer	15	1000
Motor	7	70
Motor starter	14	60
Battery charger	30	40
Switchgear	1	260
Circuit breaker	4	5
Disconnect switch	6	2
Cable joint	0.8	30
Cable termination	4	10

*representative examples

Source: "IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications" (1995)

Figure 33.
Intelligent Circuit Breaker

Source: SquareD

Resilient Design

There are definite limits to how much reliability can be added by hardware alone, and when systems are poorly designed, monitored, or maintained, more hardware can in fact reduce reliability rather than raise it. One of the most important – and least appreciated – challenges is to determine just how robust and resilient a design really is. It is far easier to declare a power network "reliable" or "robust" than to ascertain with confidence that it really is.

Standby diesel generators, for example, fail with some regularity. Some of the most pampered, carefully maintained backup diesel generators in the world reside at nuclear power plants. Yet about 1 percent of all nuclear-plant diesels fail to start when required, and fully 15 percent of the units will fail if run for 24 hours.[101] The operators and regulators of nuclear power plants are well aware of these limitations, and most nuclear plants have three separate, independent emergency power systems for just that reason. Because they are much less well maintained, diesel generators at hospitals and many other sites have failure rates 10 times higher. The May 2000 FAA report (noted earlier) identified failure rates in some of their diesel-generator-based systems at air traffic control centers that approached the grid's failure rates. More importantly, the same study showed a doubling in the past decade of the mean-time-to-repair for standby power systems.[102]

"Common mode" failures present a second refractory problem, particularly in the post-9/11 environment. For example, the high-voltage power lines and gas pipelines both present very inviting targets for terrorist attack; a simultaneous attack on both could cripple grid power and gas-fired backup generators. In the past, backup systems for commercial premises were often engineered to protect against common-mode failures caused by ordinary equipment failures, and by weather, but rarely engineered to protect against sabotage – and particularly not sabotage of the public infrastructure. A bank or data center might thus engineer a dual-feed to two independent high-voltage transmission lines – but would not plan for the further possibility that a deliberate attack might target both lines simultaneously. In the post-9/11 environment, the risk of more serious forms of common-mode failure must be taken more seriously.

Common-mode failures point to the more general challenge of analyzing risks of failures in complex, highly interdependent systems. The aviation and nuclear industries have spent many decades developing systematic, quantitative tools for analyzing the overall resilience of alternative architectures, and continuously improving the best ones. As those industries have learned, complex, probabilistic risk analysis is required for a rigorous assessment of reliability and availability. But these analytical tools are still relatively new and widely underused in the analysis of power supplies.

Used systematically, they require power engineers, statisticians, and auditors to physically inspect premises, analyze multiple failure scenarios, and draw on statistical databases to predict likely failure rates of the hardware, the human aspects of operation and maintenance, and external hazards. They must systematically take into account the key (though frequently overlooked) distinction between the reliability of the power itself, and the *availability* of the systems it powers. They must use as their basic inputs the mean-time-to-failure of individual subsystems and components, along with estimates of the risks of entirely human failures, which are often the most difficult to quantify. They must then build elaborate models for how components may interact to aggravate or abate problems.

They must then take fully into account not only the failure, but also the mean-time-to-repair. As discussed earlier, a 1-second power failure can entail a 10-minute reboot of a computer, or a week-long restart of a chip-fab; the availability of what really matters is then far lower than the nominal availability of the power behind it. The most common metric of reliability measures the probability of failure, ignoring the length of the ensuing down time entirely. *(Table 16)* Availability metrics are far more difficult to ascertain, but they are much more useful, in that they attempt to include the time it takes to effect repairs and restart systems once a process is interrupted by a power failure.

With this said, both the analytical tools and the technologies required to engineer remarkably resilient, cost-effective power networks are now available. The challenge going forward is to promote their intelligent use where they are needed.

PRIVATE INVESTMENT AND THE PUBLIC INTEREST

Private-sector spending on homeland security is forecast in the range of $46 - 76 billion for fiscal year 2003.[103] But it is difficult to promote private investment in public security. Surveys of corporate security executives conducted since 9/11 have reported only modest increases in such spending in the first year after the attack.[104] Spending on security is widely viewed as pure expense.[105] New capital investment in electronic screening systems for detecting weapons or explosives in people or packages may be essential, but it neither generates revenue nor improves operational efficiency.

Power is different. The private sector was making huge investments in backup power long before 9/11, because electricity is essential for operating most everything in the digital age, and because the grid cannot provide power that is sufficiently reliable for many critical or merely important operations. Backing up a building's power supplies can be far more expensive than screening its entrances, but improving power improves the bottom line, by keeping computers lit and the assembly lines running.

Likewise, in the public sector, secure power means better service. At the very least, public safety and emergency response services require robust power supplies for their communications systems. Large city governments are run much like large businesses, but small communities are often even more vulnerable to outages, because their grids are more exposed, and because emergency service centers are more thinly dispersed. The city of Rushford, Minnesota, for example, recently approved the installation of four 3,000-hp diesel backup generators to use during emergencies and when demand peaks strain available supplies.[106] The small town of McMinnville, Tennessee, installed 20 MW of diesel engines at a TVA substation for the same reasons.

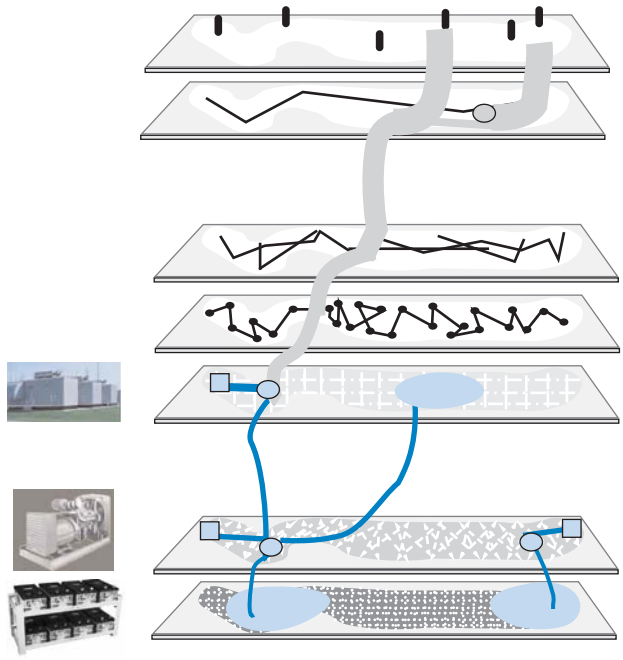
The upshot, as discussed earlier, is that some 10 percent of the grid's capacity (80 GW) is now covered by backup generators. In recent years, roughly 1 MW of off-grid backup capacity has been added for every 6 - 10 MW of central-power-plant capacity brought on line. In addition, we estimate that approximately 3 percent of the grid's capacity (25 GW) is complemented by large UPS systems, with another 2 percent (10 to 15 GW) covered by smaller, desktop-sized units. Sales of long-life, high-performance backup lead-acid batteries have also risen sharply over the past decade; there is now an estimated cumulative installed base of some 30 million heavy-duty stationary backup lead-acid batteries. Most of this investment was made well before 9/11, and much of it falls well short of what is needed to provide adequate assurance of continuity of operations in the new environment. But these capital outlays do nevertheless confirm that the private sector has strong incentives to invest in critical-power infrastructure quite apart from any considerations related to homeland security.

Equally important is that such investments, though undertaken for private purposes, directly increase the reliability and resilience of the public grid as a whole. Larger users with their own on-site generating capacity can – and already do – sign "interruptible" power contracts with utilities; such contracts allow utilities to reduce peak demand by selectively shedding certain loads, rather than "browning out" (lowering the voltage to) large regions, or blacking out smaller ones entirely. In the event of a major assault on the grid, the process of restoring power to all will be speeded up and facilitated by the fact that some of the largest and most critical loads will be able to take care of themselves for hours, days, or even weeks.

Moreover, and even more important, the process of restoring power system-wide has to begin with secure supplies of power at the most critical nodes. Coordinating the response to a major power outage requires functioning telephone switches, E911 centers, and police communications, and the grid itself can't be re-lit unless its SCADA network remains powered. The most essential step in restoring power is not to lose it – or at worst, restore it very quickly – at key nodes and small, subsidiary grids from which the step-by-step restoration of the larger whole can proceed. Many of these nodes and grids are privately owned and operated, and securing their critical-power supplies thus depends, in the first instance, on private investment. Many of the rest are operated by local and state governments, and thus depend on investments made far down in the hierarchy of public sector spending.

Finally, in times of crisis, private generators can not only reduce demand for grid power, they can – with suitable engineering of the public-private inter-

Figure 34.
Adding Resilience From the Bottom



faces – feed power back into limited segments of the public grid. Options for re-energizing the grid from the bottom-up are increasing as distributed generation expands, and as the grid's switches, substations, and control systems improve. *(Figure 34)* As discussed further below, such options will multiply rapidly if hybrid-electric power plants come to be widely adopted in the transportation sector.

In sum, the single most effective way for government to secure the critical power infrastructure is to encourage private sector investment – not just by the relatively small numbers of quasi-public utilities and large federal agencies, but by private entities and state and local governments. Dispersed planning and investment is the key to building a highly resilient infrastructure of power.

Assess Vulnerabilities

Policy makers should be leading and coordinating the efforts of user groups, critical power providers, and utilities to conduct systematic assessments of critical-power vulnerabilities, for specific industries, utility grids, and configurations of backup systems.

As discussed above, planning for infrequent but grave contingencies is exceptionally difficult. Many critical power needs remain unaddressed simply because they have never been systematically examined. The most effective way to promote new private investment in critical power is for policy makers to help analyze and draw attention to limits and vulnerabilities of the grid, the types of loads that most require assured power continuity, and the types of on-site hardware that are capable of providing it.

Utility Protocols for "Electric Service Priority"

Major utilities already make a first – though often unsystematic – attempt to perform part of this assessment when they establish the ESP protocols noted earlier, to prioritize power restoration efforts after a major outage, typically targeting hospitals, emergency services and the like.[107] Such programs implicitly acknowledge that certain users and uses are atypically dependent on supplies of electric power, and suffer unusually serious consequences when their power fails. All such priorities are swept aside, however, when a high-level failure cuts off power to an entire region. Then, the focus is almost entirely on the systematic restoration of power from the top-down, beginning with the highest-power stations, trunks, and switching centers, in a process structured largely to minimize damage to the utility's own, most essential equipment.[108] In such circumstances utilities must – above all – maintain power supplies to their own control centers, communications and SCADA networks.

Thus, a utility's power-restoration priorities provide only limited information about critical-power requirements. Properly assessing underlying end-user vulnerabilities to power outages requires systematic assessment not just of "how important" the user is, but of the likelihood of (a) losing grid power at that user's specific location(s), (b) any backup actually starting/operating, and (c) losing or exhausting one or more of the on-premises components the user has in place to provide backup power.

The Chicago/DOE "Municipal Electric Power Vulnerability Assessment"

A joint study completed by the City of Chicago and the DOE in 2001 maps out the necessary elements of a comprehensive "municipal electric power vulnerability assessment" along just these lines. The study took as its starting point the cause and consequences of the April 1992 events that shut off utility power for weeks in the heart of Chicago. As that outage taught, and as the Chicago/DOE report points

out, large cities have grown far more dependent on electric power than they used to be, in significant part because of urban society's ubiquitous dependence on digital and information hardware.

The Chicago/DOE report starts from the premise that a power vulnerability assessment "combines the information on the status of the electric power system… with information on the critical facilities and power-outage-sensitive individuals." The objective isn't merely to assess "the probability that the power will go out," it is to assess a community's "reliance on the electric power infrastructure and to project what the impacts might be if parts of it were disrupted."

This, the Chicago/DOE report emphasizes, requires a systematic, three-part analysis. The vulnerability assessment must begin with an analysis of the condition of the public grid, including the feeders and substations that serve the community, and an assessment of the extent to which "failures at one or a few substations could significantly affect" the community.

Equally important, is the identification of "critical facilities and power-outage-sensitive individuals," and the analysis of how much they depend on specific feeder connections or substations. In this regard, planners must determine, site by site, "whether several critical facilities and/or power-outage-sensitive individuals are connected to the same feeder," such that "the loss of one feeder might disrupt a number of facilities and sensitive individuals simultaneously."

Finally, the vulnerability assessment must analyze the adequacy of "backup measures in place for critical facilities and power-outage-sensitive individuals" – battery systems, on-site backup generators, portable generators, quick-connect circuit boxes, and so forth. Municipalities will generally perform this review for their own facilities; some municipalities "might find it useful to provide this review as a service to privately owned facilities as well." The Chicago/DOE report includes an appendix containing model forms for gathering basic information to systematize this type of review, but recognizes, as well, the importance of "on-site inspection… to clarify the actual status and condition of the backup measures."

The FAA's Power Systems Analysis

The comprehensive May 2000 FAA analysis, cited earlier, was conducted along similar lines, for the backup-power requirements at the Agency's roughly four dozen major control centers.[109] The report analyzed the historic record of grid power availability at those facilities, and data on the reliability of the backup systems currently in place, and thus the likelihood that the Agency's aging backup systems would perform as required when future outages occur. Subsequently, the FAA initiated a staged program to upgrade the most important and vulnerable systems. As part of that process, the Agency is deploying a network of extremely sensitive instruments for remote monitoring of key power equipment, together with software (originally developed for the U.S. Navy) for real-time predictive failure analysis.

Critical-Power for Telecommunications

Alongside the FAA, telecom regulators and carriers have progressed further than many other sectors in focusing on their critical-power needs and establishing service priorities in consultation with electric utilities.

In 1988, for example, the Federal Communications Commission (FCC) established its Telecommunications Service Priority program (TSP), to identify and prioritize telecommunication services that support national security and emergency preparedness missions. More than 50,000 phone lines have since been identified as critical, and the switching centers that service them have been placed on a master priority list for service restoration during an emergency.[110] Coverage falls into five categories. The top two are for national security; the third covers centers involved in public health, safety, and maintenance of law and order. The nearly 7,000 local dispatch centers ("public-safety answering points") that handle E911 calls, for example, are eligible for listing in this category. The fourth category covers "public welfare and maintenance of national economic posture" and includes, among others, banks and other financial institutions under the sponsorship of the Federal Reserve Board. The fifth is a catchall category for the provision of new "emergency" services.

The DOE and the Office of National Communications Services subsequently established the Telecommunications *Electric* Service Priority (TESP) program, which prioritizes power restoration to critical telecommunications assets – which was subsequently reconstituted in 1994 as the National

Electric Service Priority Program for telecommunications.[111] Some 230 telephone companies, more than 500 electric utilities and regulatory authorities in all fifty states participate. While voluntary, the program maintains a database of the operational status of some 3,500 "critical" assets nationwide, and electric utility emergency priority restoration systems have been revised accordingly.

Yet even in connection with critical telecom services, which depend entirely on their concomitantly "critical" supplies of power, there remain few standards specifying the minimum equipment required to maintain operational continuity in the event of serious grid outages. When backup power requirements are noted at all, they are often given short shrift. The National Emergency Number Association (NENA), which represents operators of E911 call centers, has promulgated backup-power standards that suggest "a minimum of 15 minutes of emergency power for full functionality" and "if budget permits, it is desirable to extend the 15 minutes to as much as 1 hour." Beyond that, NENA merely urges its members to plan for more "prolonged power outages," and recommends (without further specifics) that centers "be equipped with a source for long-term emergency power," which "may consist of a redundant utility power feed or a generator sized appropriately." Members are then advised to consult with "the local utility provider and a qualified power conditioning professional."[112]

According to the FCC's Director of Defense and Security (in the FCC's Office of Engineering and Technology) many E911-center administrators are not even aware that they can enroll in the National Communication System's (NCS) priority service list for access to communications lines and systems. The FCC draws a contrast with the financial industry, which has aggressively pursued priority restoration agreements.[113]

Vulnerability Assessments in Other Sectors

As summarized in *Table 17*, various entities in both the communications and financial industries have indeed completed a number of comprehensive threat assessments – among the most thorough we have seen. Alarmingly, however, most of those studies appear to either assume continuity of the supplies of power required to operate the digital equipment on which those sectors so completely depend, or simply take the position that the local utility is entirely responsible for securing the supply of power. Many of the entities responsible for ensuring critical-facility continuity are lagging well behind in assessing and addressing their underlying need for power, and also in plans to address the statistical certainty of local grid failure, extended outages, in particular.

For the most part, other government, industrial, and commercial sectors have done very much less to assess their power vulnerabilities. Many older wastewater treatment facilities still lack the emergency power sources required to maintain pumping capability when grid power fails. In 1997, a number of public utility commissions called for backup power standards for newer water facilities, or for sufficient on-site fuel to cover extend outages.[114] The FEMA report cited earlier (which addresses the crippling impact of the 1998 Northeast ice storms),[115] pointed to across the board deficiencies in on-site auxiliary power capacity. Because of the outage duration, lack of on-site power even forced closures of many of the schools frequently designated as disaster shelters.

As the FEMA report emphasizes, the longer the outage, the more "critical" the lack of power tends to become. Many sites – including especially emergency response sites – that can ride through grid outages that last an hour or day become increasingly dysfunctional when power outages persist for longer periods. Again and again, the FEMA report emphasizes the need to assess power requirements and weigh the need for backup power where there was none at all, redundant backup systems where they found critical facilities depending on fundamentally unreliable backup generators (calling for the classic redundancy, defense-in-depth, common in military, aviation and nuclear industries), and most particularly for capability to operate for extended periods of time (beyond the minutes and hours typical where there was any backup at all).

Federal Initiatives and Oversight

Many of the reports just described provide useful models for what is required, but they also serve to highlight what is missing. In the current geopolitical environment, the analyses required to secure critical-power infrastructure can no longer wait until after the major outages materialize. In the aftermath of 9/11, critical-power infrastructure must be analyzed and secured in anticipation of significant threats, not just in reaction to their actual occurrence. The National Strategy for Homeland Security announced by the

White House in July 2002, and substantially expanded in February 2003,[116] specifically directs federal agencies to "[f]acilitate the exchange of critical infrastructure and key asset protection best practices and vulnerability assessment methodologies." The National Strategy notes the "modeling, simulation, and analysis capabilities" on which "national defense and intelligence missions" rely, and declares that such tools must now be applied to "risk management, and resource investment activities to combat terrorism at home," and particularly with regard to "infrastructure interdependencies."

The responsibility to pursue vulnerability assessments would now logically lie with the Infrastructure Analysis, Information Assurance (IAIP) directorate of the DHS. The IAIP includes the CIAO (originally created in 1996), the former National Infrastructure Protection Center (NIPC), and representatives from four other federal government agencies. It coordinates the efforts of federal, state and local government officials and the private sector in protecting the nation's critical infrastructures. To that end, it brings together the capabilities needed "to identify and assess current and future threats, to map those threats against existing vulnerabilities, issue timely warnings and take preventive and protective action."[117]

TISP should be engaged in this effort as well.[118] Members include local, state, and federal agencies, the Army Corps of Engineers, professional associations, industry trade groups, code and standards organizations, professional engineering societies, and associations that represent the builders and operators of infrastructure facilities, among others. Among other goals, the organization seeks to "encourage and support the development of a methodology for assessing vulnerabilities," and to improve "protection methods and techniques" relevant to "domestic infrastructure security."

Establish Critical-Power Standards for Facilities Used to Support Key Government Functions

Federal and local organizations should work with the private sector to establish guidelines, procedures, and (in some cases) mandatory requirements for power continuity at private facilities critical to government functions.

Much of the private sector already has strong incentives to secure its critical-power requirements; for the most part, the government's role should be to inform and facilitate voluntary initiatives. At the same time, however, many federal, state, and local agencies have independent responsibility to ensure that private-sector facilities used to support key government functions can be relied on in times of crisis. This necessarily implies some form of governmental auditing or standard-setting for the backup-power systems that ensure continuity of operation of the chips, fiber-optics, radios and broadcast systems within privately owned telecom, data, computing, and financial networks on which key agencies at all levels of government rely.

Though they have yet to issue any specific, power-related standards, federal financial agencies have repeatedly noted the importance of power in maintaining the continuity of financial networks in times of crisis, and have affirmed their authority to audit the physical infrastructure on which key institutions rely. Federal regulators have general authority to examine all aspects of risk management at federally insured banks, including "use of information technology and third party service providers," and the evaluation can include systems in place to assure "business continuity." A January 2003 report by the GAO,[119] for example, notes that the "financial services sector is highly dependent on other critical infrastructures," particularly telecommunications and power. A follow-up GAO report concludes that the "business continuity plans" of many financial organizations, have "not been designed to address wide-scale events."[120] An April 2003 paper by the Federal Reserve stresses the importance of "improv[ing] recovery capabilities to address the continuing, serious risks to the U.S. financial system posed by the post-September 11 environment," with particular attention to the threat of "wide-scale disruption" of "transportation, telecommunications, power, or other critical infrastructure components across a metropolitan or other geographic area."[121]

Within the financial services community itself, however, securing power supplies is still – all too frequently – viewed as someone else's responsibility. The technology group of the Financial Services Roundtable and the Financial Services Information Sharing and Analysis Center (FS/ISAC) fully recognizes that the financial sector "increasingly depends on third-party service providers for… telecommuni-

cations and electrical power,"[122] and accepts that "the core infrastructure of the banking and finance sector must be examined to identify and assess areas and exposure points that pose systemic risk." Nevertheless, many of this sector's business-continuity efforts still, essentially, assume grid power and proceed from there.

If such attitudes are still encountered even in sophisticated, well-funded financial circles, they dominate elsewhere, in planning for service continuity in local government agencies, wastewater treatment plants, schools that double as disaster recovery centers, broadcast facilities, hazardous chemical storage, and even many medical facilities. Government agencies at all levels have significant financial stakes in these services, and in the underlying facilities used to provide them, and thus share responsibility for ensuring that adequate preparation is made for emergencies.

In this regard, the Chicago/DOE study, discussed above, provides a model for the analysis, guidelines, and standards that municipal governments can play a key role in developing. It makes no attempt to tell utilities how to make the public grid more reliable; rather, it focuses on identifying critical-power users, conducting site-specific vulnerability assessments, and assessing technology alternatives – batteries, generators, dual feeds, and so forth – that can keep key loads lit when the grid fails. The Chicago/DOE report does not go on to establish mandatory standards for the private facilities on which the City of Chicago itself relies. But power-related mandates of that character must emerge in due course to define the private facilities required to ensure operational continuity of public services in times of widespread disruption to the public infrastructure.

Share Safety- and Performance-Related Information, Best Practices, and Standards

Utilities, private suppliers, and operators of backup power systems should develop procedures for the systematic sharing of safety- and performance-related information, best practices, and standards. Policy makers should take steps to facilitate and accelerate such initiatives.

The federally run Centers for Disease Control (CDC) compiles epidemiological databases and performs the analyses that public health officials can rely on in formulating responses. To that end, the CDC obtains information from state agencies, private entities, and individuals, with suitable protections in place to protect both privacy and proprietary information. In similar fashion, aviation safety has been greatly enhanced by a systematic government process for investigating all significant equipment failures and major accidents, and sharing the information industry wide. The National Transportation Safety Board investigates and maintains a comprehensive database of accidents and incidents that extends back to 1962; industry participation is mandatory, but the information generated in the process is used only for improving safety system wide; it may not, for example, be used in civil litigation.[123] The Aviation Safety Reporting System (ASRS) is a complementary, voluntary program that collects, analyzes, and responds to less serious incident reports. The program focuses mainly on human factors and guarantees confidentiality; more than 300,000 reports have been submitted to date.[124]

The government's National Communications System works closely, and in similar fashion, with the private National Security Telecommunications Advisory Committee to ensure the continuity of the telecommunications services on which the most important government users depend.[125] The two groups are jointly charged with ensuring the robustness of the national telecommunications grid. They have been working together since 1984 and have developed effective means to share information about threats, vulnerabilities, operations, and incidents, which improves the overall surety of the telecommunications network. Comparable programs should be developed to analyze – and learn from – failure at every tier of the electric infrastructure, including distributed generation and on-site power.

In the electric power sector, the nuclear industry developed a similar, comprehensive, information-sharing program in the aftermath of the 1979 events at Three Mile Island. The Institute for Nuclear Power Operations established a comprehensive system for the sharing of safety-related information, best practices, and standards among utilities, equipment vendors, architect/engineers, and construction firms.[126] The Institute's information sharing programs include an equipment failure database and a "Significant Event Evaluation and Information

Network." These and other assets have sharply reduced duplicative evaluation of safety- and performance-related events.[127] Since the establishment of these programs, the nuclear industry has maintained a remarkable, two-decade record of safe operations, while also dramatically improving the availability – and thus the economic value – of its facilities.

In light of the growing importance of on-site power, the providers and users of this equipment should now seriously consider establishing a national advisory group comparable to the utility sector's NERC/CIPAG (discussed above) and empowered to work with CIPAG to coordinate the complementary development of on-site power-protection infrastructure. Independently, the NFPA Standard for Emergency and Standby Power Systems, noted earlier, sets out what amounts to a best-practices guide to on-site power; it also classifies different backup systems and configurations by run time. It is difficult to see how CIPAG can properly fulfill its stated mission – "to advance the physical and cyber security of the critical electricity infrastructure of North America" – without a systematic process for coordinating grid-level and on-site power-protection initiatives. The same holds for other NERC activities, including those of the Electricity Sector Information Sharing and Analysis Center (which gathers and interprets security-related information and disseminates it within the industry and the government) and NERC's best-practices advisories for the business community.[128] On-site power has emerged as a new, essential tier of the power infrastructure, and the security of the system as a whole can no longer be analyzed without due consideration of on-site power facilities.

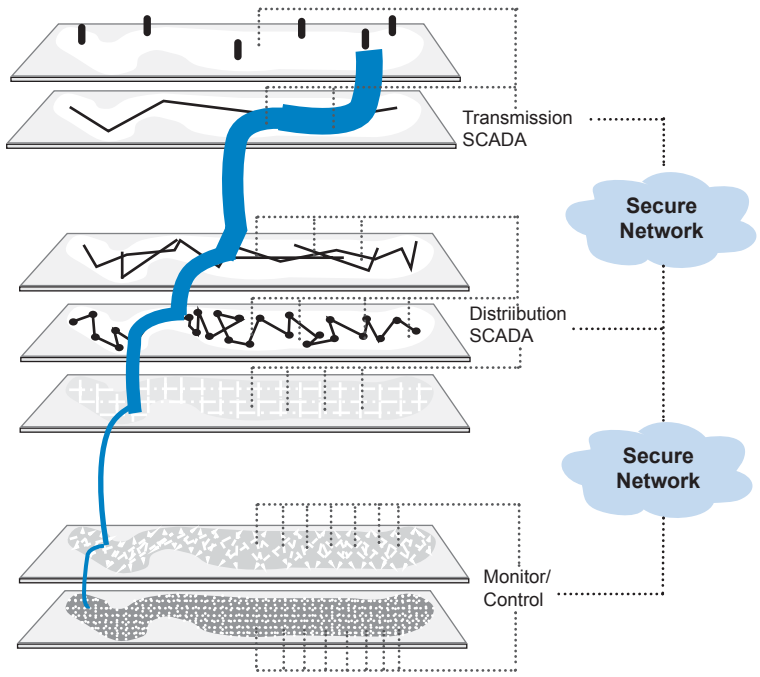
More generally, as discussed in the 1997 Presidential Commission report, Critical Foundations,[129] the hardening of critical infrastructure will depend on "creation of a trusted environment that … allow[s] the government and private sector to share sensitive information openly and voluntarily." To that end, the 1997 report proposed changes in various laws that currently inhibit the protection of confidential information, and thus discourage participation in information sharing. The report specifically flagged, as areas of potential concern, the Freedom of Information Act, insufficient protection of trade secrets and proprietary information, classified information, antitrust laws, civil liability, and potential national security issues arising from participation by foreign corporations in information sharing arrangements. Little was done to follow up on these proposals in 1997; they should be acted upon now.

Interconnect Public and Private Supervisory Control and Data Acquisition Networks

The supervisory control and data acquisition networks operated by utilities and the operators of backup power systems should be engineered for the secure exchange of information, to facilitate coordinated operation of public and private generators and grids. Policy makers should take steps to facilitate and accelerate that development.

As described earlier, SCADA systems are used by utilities and regional transmission authorities to monitor and manage power distribution grids and substations. Extensive arrays of sensors and dedicated communications links feed information to the major control centers that monitor the overall state of the grid, and control its constituent parts. Very simi-

Figure 35.
Networking the Tiers



lar data networks and supervisory systems perform the same functions on private premises, supervising and controlling grid feeds, static switches, batteries, backup generators, and UPSs.

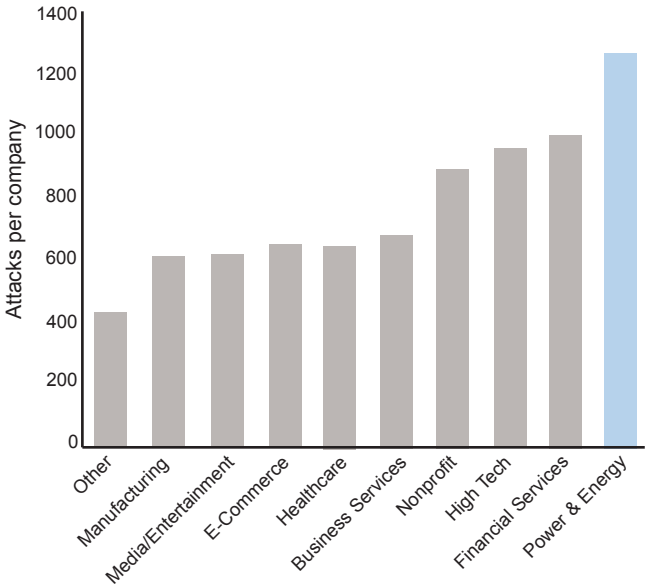
At present, there is very little direct, electronic linkage between the public and private networks that supervise and control the flow of power. This is a serious deficiency, and one that should be comparatively easy to rectify. Better communication is essential if utilities are to collaborate more closely with the owners of private generators, to shed loads (or even to draw privately generated power back into the grid) when large power plants or major transmission lines fail. And the owner-operators of private generators and grids would be much better positioned to protect their facilities from major problems propagating through the grid. *(Figure 35)*

Among other advantages, advanced networking of this kind would make possible dynamic updating of service-restoration priorities. At present, for example, the telephone-service priority program rules require service users to revalidate their priority status every two years. Most utility ESP protocols are equally static, and therefore much less useful than they might be. Critical-power needs can obviously change month to month, or even hour to hour. Responses to widespread outages cannot be optimized on the basis of two-year-old information. By way of analogy, some private companies rely on private weather reporting services to provide site-specific, real-time weather alerts to assist in power management and control. Thor Guard's service, for example, can provide localized forecasts of lightning hazards,[130] allowing enterprises with on-site power to disconnect from the public grid when the risk of dangerous transients is high. More efficient and dynamic exchanges of electronic information between the various public and private tiers of the grid could greatly improve the resilience of the whole.

Secure Automated Control Systems

The necessary integration of SCADA networks operated by utilities and the operators of backup power systems requires high assurance of cyber-security of the networks in both tiers. Policy makers should take steps to advance and coordinate the development of complementary security protocols in the public and private tiers of the electric grid.

Figure 36.
Cyber Attacks (From 1/1/02 to 6/30/02)



Source: "Riptech Internet Security Threat Report: Attack Trends for Q1 and Q2 2002," Riptech, Inc. (July 2002).

More efficient exchange of information between public and private power-control networks is clearly desirable, but at the same time, the very existence of highly interconnected control networks can create new vulnerabilities that must be assessed and addressed.

As part of its more general charge to improve the surety of the nation's energy infrastructure, Sandia National Laboratories has focused specifically on the cyber-vulnerabilities of the electric power industry's SCADA networks.[131] In addition to identifying significant security issues specific to particular systems, Sandia has explored the more general problems inherent in the trend toward fully-automated, networked SCADA systems, increasing reliance on fully automated control, loss of human expertise, reliance on equipment of foreign manufacture, and the difficulty of performing meaningful security inspection and validation.

SCADA systems, Sandia notes, "have generally been designed and installed with little attention to security. They are highly vulnerable to cyber attack… [S]ecurity implementations are, in many cases, non-existent or based on false premises." Sandia also cites public reports that these systems have been the specific targets of probing by Al Qaeda terrorists. Over 1,200 cyber attacks were detected *per energy company* over a six month period in 2002 – 20 percent more than against an average financial company, and twice as many as an average e-com-

merce company; moreover, a disproportionately high fraction (70 percent) of the attacks on energy company SCADA networks were classified as "severe."[132] *(Figure 36)*

To address some of these problems, Sandia is working with international bodies to develop open but secure standards for these networks. This initiative is, clearly, an essential complement to the further development of utility SCADA networks, and an equally essential predicate to any interconnection of public and private control networks.

Share Assets

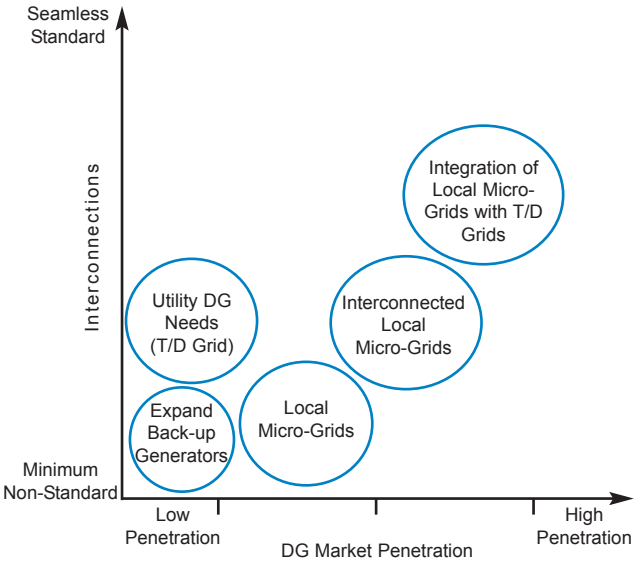
Policy makers and the private sector should take steps to promote sharing of "critical spares" for on-site generation and power-conditioning equipment, and to advance and coordinate the establishment of distributed reserves and priority distribution systems for fuel required to operate backup generators.

As noted earlier, the utility industry's CIPAG has formed a working group to inventory and develop a database of high-power "critical spare equipment" used in the high-voltage transmission system. Such programs address the straightforward, serious challenge of locating spares in times of emergency, and getting them quickly to where they are needed. The intelligent sharing of stand-by assets shortens response times and can greatly reduce the collective cost of preparing for rare but serious interruptions.

The CIPAG program was initially developed from a 1989 FBI request to NERC, to identify and locate equipment (specifically, the large and hard-to-replace extremely-high-voltage transformers) that might be available for loan in the event of a terrorist attack. NERC's spare equipment database, which is now accessible on a secure Web site, has since grown to include over 900 transformers.[133] The CIPAG initiative has recently included "emphasis on deterring, preventing, limiting, and recovering from terrorist attacks"[134] and the class of critical equipment is to be expanded to incorporate all other grid-critical equipment.

Comparable programs could, in similar fashion, significantly improve operational resilience in the lower tiers of the grid. Power plants on wheels (or on barges) offer the economies of sharing in much the same manner as fire engines and rescue vehicles, and bypass the many cost-related and regulatory

Figure 37.
Distributed Generation and the Public Grid



Source: "Grid of the Future White Paper on Interconnection and Controls for Reliable, Large Scale Integration of Distributed Energy Resources," Transmission Reliability Program Office of Power Technologies (December 1999).

obstacles that impede permanent deployment of backup generators.

Fuel supplies for backup generators present similar challenges, and similar opportunities. As recently noted in The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets,[135] "[a]ssuring electric service requires operational transportation and distribution systems to guarantee the delivery of fuel necessary to generate power." The DOE addressed an analogous problem in a program initiated in 1998. Concerned about potential interruptions (or price run-ups) in supplies of home heating oil, the Department established four new regional heating oil storage terminals – in effect a mini Strategic Petroleum Reserve – containing a total of 2 million barrels of reserve fuel.[136]

Enhance Interfaces Between On-Site Generating Capacity and The Public Grid

Improved technical and economic integration of on-site generating capacity and the public grid can back up critical loads, lower costs, and improve the overall resilience of the grid as a whole, and should therefore rank as a top priority for policy makers and the private sector.

Many utilities are already offering backup-power

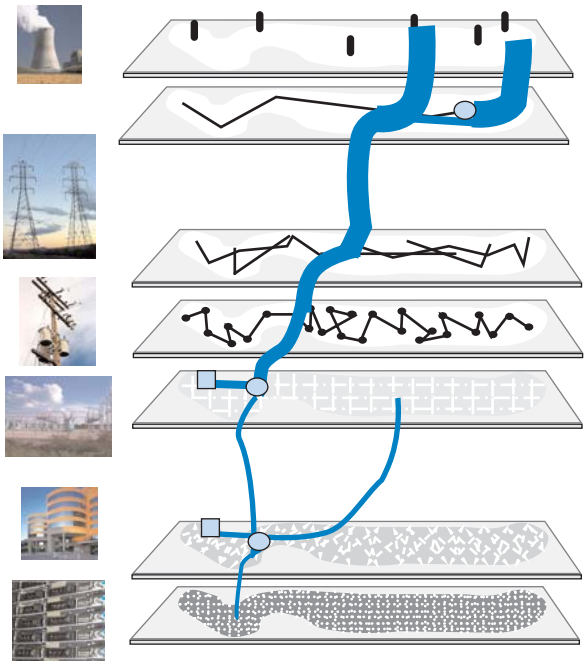
services to commercial and industrial customers, or plan to begin doing so within the next few years. Additional impetus for utility and private development of "distributed" or on-site power has come from growing interest in fuel cells, photovoltaics, and co-generation. With suitable engineering of the public-private interfaces, and appropriate tariffs in place, on-site generators can back up critical loads, lower costs, and improve the overall resilience of the grid as a whole.

Wisconsin Public Power, Inc. (WPPI) for example, now offers large (>250 kW) customers long-term contracts for the installation and maintenance of on-site standby generators, together with remote monitoring and control. WPPI also fires up the units during periods of peak demand or high price.[137] In Orlando, Cirent Semiconductor backs up the most critical loads in its much larger (35 MW) facility with an array of 2 MW diesel gensets. In cooperation with the Florida Power Corporation (FPC), these generators are now being used for peak shaving as well: In return for lower rates, Cirent fires up the units during times of peak usage to displace up to 6 MW of demand from FPC's public grid.

Such opportunities have been systematically explored in two excellent papers written by the DOE: A 1999 white paper prepared in collaboration with a consortium of the national laboratories, Integration of Distributed Energy Resources,[138] and an outstanding September 2002 report, Distributed Energy Resources Interconnection Systems: Technology Review and Research Needs.[139] While surprisingly silent on the subjects of critical power and homeland security, the latter report includes a detailed survey of distributed-power technologies, a complete analysis of the technologies required to interconnect distributed capacity to the grid, and a thorough set of recommendations for both the technical and the policy-making communities with regard to interconnection standards. *(Figure 37)*

Federal and state regulators, together with private standards-setting bodies, are now actively developing programs to facilitate such arrangements, and to make them profitable to all participants. As noted earlier, an IEEE publication sets out comprehensive definitions of technical standards for reliable on-site industrial and commercial power systems.[140] More recently, the IEEE approved a new Standard for Interconnecting Distributed Resources With Electric Power Systems.[141] California, New York, and a number of other states have interconnection tariffs and procedures in place; most of them defer to bilateral agreements between the utility and the owner of the distributed generating capacity, with disputes handled case-by-case by the public utility commission. At the federal level, FERC likewise relies heavily on volun-

Figure 38.
Power Regulators and Players



Regulators	Players & Standards
Federal Energy Regulatory Commission (FERC), Department of Energy (DOE), Department of Transportation (DOT), Nuclear Regulatory Commission (NRC), U.S. and State Environmental Protection Agencies (EPAs), National Association of Regulatory Commissions (NARUC) (e.g., pipeline safety), State Public Utility Commissions (PUCs), Local Governments (county and city) (e.g., zoning, siting)	Critical Infrastructure Assurance Office (CIAO- DHS), Infrastructure Analysis, Information Assurance (IAIO - DHS), Critical Infrastructure Protection Advisory Group (CIPAG - NERC)
FERC, DOE, DOT, EPAs, NARUC, PUCs, Local Governments (e.g., zoning, siting)	Electric Power Research Insitute (EPRI), Telecommunications Electric Service Priority (TESP), Insitute of Electrical and Electronics Engineers (IEEE), Electrical Generating Systems Association (EGSA), National Electrical Manufacturers Association (NEMA)
FERC, National Fire Protection Agency (NFPA), Underwriter's Laboratory (UL), DOE, Department of Labor (OSHA), EPAs, PUCs, Local Governments (e.g., health, safety)	Information Sharing and Analysis Center (ISAC), National Fire Protection Agency (NFPA), International Electrotechnical Commission (IEC)

tary arrangements, but the Commission is also developing a model interconnection agreement that would create a streamlined process for interconnection of under-20-MW facilities, and an even simpler process for facilities under 2 MW.[142]

Over the longer term, the emergence of hybrid-electric trucks, buses, and cars will offer the possibility of linking the transportation sector's mobile, and highly distributed infrastructure of fuel tanks, engines, and generators directly to electrical breaker boxes and UPSs in residences, small offices, and larger buildings. As discussed earlier, one of the diesel genset's main attractions is that it runs on the transportation sector's fuel, and can thus draw on that sector's huge, distributed, and therefore resilient infrastructure of fuel storage and delivery. The hybrid car designs already on the road – the Toyota Prius, Honda Insight and Civic, and shortly available Ford Escape – have 10 to 33 kW power plants, with primary fuel on board in the gas tank. Emerging larger vehicles will have 100 kW. If and when they eventually arrive, simple, safe bridging from the transportation sector's power plants to building-level electrical grids will offer potentially enormous improvements in the resilience and overall reliability of electrical power supplies.

One cannot underestimate either the technical or the economic challenges involved in connecting distributed generating capacity to the grid. At the technical level, generators must be very precisely synchronized with the grid; otherwise they can create destructive reverse power flows damaging grid equipment for all (or cause catastrophe on the small generator side). Isolation switches are essential to protect utility workers from the hazards of privately generated power moving up the lines during a grid outage. Economic integration is equally challenging. Large, centralized power plants and the grid itself are shared capital-intensive resources, and their costs must be allocated rationally. But with these important qualifications noted, the orderly physical and economic integration of utility and on-site power systems offers an enormous opportunity to secure critical-power at no net cost to either utilities or end-users.

Remove Obstacles

Private investment in critical-power facilities creates public benefits, and policy makers should explore alternative means to remove obstacles that impede private investment in these facilities.

Zoning and environmental regulations, and related issues of insurance, often present serious obstacles to deployment of on-site generating facilities. State and local fire codes may prevent on-site fuel storage. Companies storing fuel oil for backup generators or vehicle fleets may have to prepare written Spill Prevention Control and Countermeasure (SPCC) plans to comply with the Clean Water Act, as well as a maze of local, state and federal environmental regulations.[143] Municipal zoning and safety regulations affect where storage tanks can be sited, and how large such tanks may be.

As standby or emergency facilities, backup diesel generators are exempt from some emissions related regulations, but the exemptions typically limit annual operations to 80 or 120 hours per year, depending on the air district,[144] and thus eliminate the possibility of reducing costs by using the same facilities to generate power during high-price periods of peak demand. Noise abatement is becoming an issue as well.[145]

Some of these obstacles can readily be addressed – insurance problems, for example, can be addressed by liability limits. Others will require a systematic reassessment of priorities – how to strike appropriate balances, for example, between air quality and homeland security in the new, post-9/11 environment. The various obstacles noted above often fall under the jurisdiction of separate federal, state, and local regulatory authorities. Regulators at all levels of government should work more closely to simplify and accelerate the process of providing regulatory clearance for private investment in critical-power facilities. Federal regulators should, as necessary, be prepared to assert preemptive authority here, to ensure that parochial regulatory concerns do not unduly impede investment in facilities that contribute materially to the overall resilience of the interstate power grid. *(Figure 38)*

In striking these balances, it bears emphasizing, once again, that private investment in on-site generating facilities creates public benefits too: In the event of a major assault on the public grid, these facilities will relieve demand, and maintain the resilient islands of power required to restart the rest of the system. To the extent that competing public policies – environmental regulations, for example – reduce incentives to private investment here, policy makers

should search for other mechanisms to increase them. Because power generation facilities are so capital intensive, allowing accelerated depreciation (or immediate expensing, or similar favorable treatment) for tax purposes would have a substantial impact. A proposal to that effect was included in both the White House's National Strategy and GAO's Critical Infrastructure Report.[146]

Table 17. ELECTRIC POWER VULNERABILITY

Reports and analyses with vulnerability assessments that note or focus on electric power.

(First column indicates whether the indicated report includes or notes the role/importance of on-site critical power.)

☑	Title	Source/Author	Date	Selected Quote(s)
	Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System	Federal Reserve; Securities & Exchange Commission	April 7, 2003	"The agencies believe that it is important for financial firms to improve recovery capabilities to address the continuing, serious risks to the U.S. financial system posed by the post-September 11 environment." "Back-up sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, and electric power) used by the primary site."
✓	Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants	General Accountig Office (GAO)	February 2003	"To begin work necessary to resume financial market operations, telecommunications carriers then had to obtain generators and use emergency power to support network operations and to coordinate with financial institutions to facilitate the resumption of stock exchange activities by September 17, 2001."
	The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets	The White House	February 2003	"Almost every form of productive activity-whether in businesses, manufacturing plants, schools, hospitals, or homes-requires electricity." "Re-evaluate and adjust nationwide protection planning, system restoration, and recovery in response to attacks"
	Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats	General Accountig Office (GAO)	January 2003	"… financial services sector is highly dependent on other critical infrastructures. For example, threats facing the telecommunications and power sectors could directly affect the financial services industry." "…the widespread and increasing use of supervisory control and data acquisition (SCADA) systems for controlling energy systems increases the capability of seriously damaging and disrupting them by cyber means."
✓	Distributed Energy Resources Interconnection Systems: Technology Review and Research Needs	Department of Energy, National Renewable Energy Laboratory	September 2002	"[Distributed energy resources are] playing an increasing role in providing the electric power quality and reliability required by today's economy."
	Banking and Finance Sector National Strategy	National Strategy for Critical Infrastructure Assurance	May 13, 2002	"The banking and finance sector increasingly depends on third-party service providers for … telecommunications and electrical power."
	Information and Communications Sector: National Strategy for Critical Infrastructure and Cyberspace Security	Telecom consortium: CTIA, ITAA, TIA, USTA*	May 2002	"…many customers in New York found that their communications problems stemmed not from destroyed telecommunications hardware but from power failures and stalled diesel generators." "The Telecommunications Electric Service Priority (TESP) initiative requests that electric utilities modify their existing ESP systems by adding a limited number of specific telecommunications critical facilities."
	The Electricity Sector Response to The Critical Infrastructure Protection Challenge	North American Electric Reliability Council (NERC)	May 2002	"…work cooperatively with government, those within our industry, and other business sectors to identify and address roles, interdependencies, obstacles and barriers." "Interdependencies between other infrastructures and the electricity sector are complex and require continued review and assessment."
✓	Analysis of Extremely Reliable Power Delivery Systems:	Electric Power Research Institute (EPRI)	April 2002	"develop a framework for understanding, assessing, and optimizing the reliability of powering new digital systems, processes, and enterprises"
✓	Security Guidance for the Petroleum Industry	American Petroleum Institute	March 2002	"organizations increasingly rely on networked computer systems …. Computer systems have unique security issues that must be understood for effective implementation of security measures." "… refinery facilities or assets that may be subject to potential risk include: … Electrical power lines (including back-up power systems)."
	Making the Nation Safer: The Role of Science & Technology in Countering Terrorism	National Academy of Sciences, National Research Council	2002	"The impact of a prolonged interruption in the electric power supply to any region of the country would be much larger than the economic loss to the energy sector alone." "Simultaneous attacks on a few critical components of the grid could result in a widespread and extended blackout." "While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years."

☑	Title	Source/Author	Date	Selected Quote(s)
✓	National Fire Protection Association (NFPA) Standard for Emergency and Standby Power Systems	National Fire Protection Association (NFPA)	2002	"Organized in 1976 by the NFPA in recognition of the demand for viable guidelines for the assembly, installation, and performance of electrical power systems to supply critical and essential needs during outages of the primary power source."
	Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center	U.S. Department of Energy	November 8, 2001	
✓	Power Systems Sustained Support, Investment Analysis Report	Federal Aviation Administration (FAA)	May 23, 2000	"The FAA cannot rely solely on commercial power sources to support NAS facilities. In recent years, the number and duration of commercial power outages have increased steadily, and the trend is expected to continue into the future."
✓	National Information Assurance Certification and Accreditation Process (NIACAP)	National Security Telecommunications and Information Systems Security Committee	April 2000	"The contingency plan evaluation task analyzes the contingency, back-up, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA."
✓	Interconnection and Controls for Reliable, Large Scale Integration of Distributed Energy Resources; Consortium for Electric Reliability Technology Solutions, Grid of the Future White Paper	U.S. Department of Energy	December 1999	"Customers will use distributed resources in the near term to improve the quality of power to sensitive equipment, to firm up poor reliability, to reduce their demand charges, and to take advantage of "waste" heat associated with on-site power generation, thus increasing cost effectiveness."
	Electric Power Risk Assessment	National Security Telecommunications Advisory Committee, Information Assurance Task Force	1998	"… few utilities have an information security function for their operational systems." "A clear threat identification, combined with an infrastructure vulnerability assessment and guidelines for protection measures, is critical to stimulating effective response by individual utilities."
✓	1998 New York Ice Storm: Mitigation Issues & Potential Solutions	Federal Emergency Management Agency (FEMA)	1998	There is no requirement to maintain a secondary redundant power supply. "Local news updates were not available because many stations did not have sufficient backup generator capacity." "Hospitals are not currently required to have on-site auxiliary power capacity sufficient for maintaining all their power systems" "Many pre-1978 wastewater treatment plants and pumping stations do not have alternative emergency power sources." "There is no inventory of existing generators at these facilities."
	President's Commission on Critical Infrastructure Protection, Critical Foundations	The White House	October 1997	"The significant physical vulnerabilities for electric power are related to substations, generation facilities, and transmission lines." "While the transportation system has long been dependent on petroleum fuels, its dependency on other infrastructures continues to increase, for example, on electricity for a variety of essential operations and on telecommunications to facilitate operations, controls, and business transactions." "As farsighted and laudable as these [earlier infrastructure vulnerability] efforts were, however, interdependencies within the energy infrastructure and with the other infrastructures were not studied, nor was the energy sector's growing dependence on information systems."
✓	Generic Standards for E9-1-1 PSAP Equipment	National Emergency Number Association (NENA)	June 20, 1996	"[plan for] prolonged power outages" "[centers to] be equipped with a source for long-term emergency power," which "may consist of a redundant utility power feed or a generator sized appropriately"
✓	IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications	Institute of Electrical and Electronics Engineers (IEEE)	December 12, 1995 (Revision of IEEE Std 446-1987)	"The nature of electric power failures, interruptions, and their duration covers a range in time from microseconds to days." "In the past the demand for reliable electric power was less critical." "…industrial and commercial needs contained more similarities than differences."

* Cellular Telecommunications and Internet Association (CTIA); Information Technology Association of America (ITAA); Telecommunications Industry Association (TIA); United States Telecom Association (USTA)

NOTES

[1] Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, House Energy and Commerce Committee, Subcommittee on Oversight and Investigation, Hearing on Creating the Department of Homeland Security (DHS) (July 9, 2002).
[2] *Critical Infrastructure Protection in the Information Age,* Executive Order 13231 (October 2001).
[3] *Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center,* Department of Energy (DOE) (November 2001).
[4] *Information & Communications Sector: National Strategy for Critical Infrastructure and Cyberspace Security*, Cellular Telecommunications & Internet Association (CTIA), Information Technology Association of America (ITAA), Telecommunications Industry Association (TIA), United States Telecom Association (USTA) (May 2002).
[5] Includes nearly 1,000 stations affiliated with the five major networks – NBC, ABC, CBS, FOX, and PBS. In addition, there are about 9,000 cable TV systems. CIA World Databook (1997), http://www.cia.gov/cia/publications/factbook/geos/us.html.
[6] CIA World Databook (1998), http://www.cia.gov/cia/publications/factbook/geos/us.html.
[7] *Trends in Telephone Service*, Federal Communications Commission (FCC) (May 2002), http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/trend502.pdf.
[8] *Industry Statistics,* NCTA (November 2002), http://www.ncta.com/industry_overview/indStat.cfm?indOverviewID=2.
[9] *Background on CTIA's Semi-Annual Wireless Industry Survey*, CTIA (December 2002), http://www.wow-com.com/industry/stats/surveys.
[10] May not include pico cells. *CTIA Semiannual Wireless Industry Survey* (December 2002), http://www.wow-com.com/industry/stats/surveys.
[11] Assumes 1 BSC per every 75 base stations. "…BSCs… are responsible for connectivity and routing of calls for 50 to 100 wireless base stations." *VII GSM Call Processing*, http://www.privateline.com/PCS/GSMNetworkstructure.html#anchor3381743.
[12] There are approximately 4,500 land-based transponder sites worldwide, evenly divided between North America, Western Europe, and the Asia Pacific region, with television programming backhaul accounting for half of total use. *Teleports and Carriers Market Facts*, World Teleport Association.
[13] *Internet Data Centers,* Salomon Smith Barney, (August 3, 2000). Eagle, Liam, *Tier 1 Releases Hosting Directory, Data Center Report*, (April 4, 2002), http://thewhir.com/marketwatch/tie040402.cfm.
[14] *The Internet – What Is It?* Boardwatch Magazine (2000).
[15] *CIA World Databook*, http://www.cia.gov/cia/publications/factbook/geos/us.html.
[16] *Directory of Internet Service Providers,* Boardwatch Magazine (2000).
[17] *Directory of Internet Service Providers,* Boardwatch Magazine (2000).
[18] Estimate based on Energy Information Administration (EIA) commercial building data. Figure is 10 percent of >100,000 sq ft buildings.
[19] *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* General Accounting Office (GAO) report (GAO-03-173) (January 2003).
[20] *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO (GAO-03-173) (January 2003).
[21] *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO (GAO-03-414) (February 2003).
[22] *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO (GAO-03-173) (January 2003).
[23] *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,* Federal Reserve (April 2003).
[24] Registered hospitals as of December 2002, American Hospital Association, http://www.hospitalconnect.com/aha/resource_center/fastfacts/fast_facts_US_hospitals.html.
[25] Estimate derived by multiplying nationwide hospital total by 4, a ratio we found in select U.S. cities.
[26] Not a comprehensive count of all elderly care facilities, but nursing homes provide 24/7 care. *JAMA Patient Page: Nursing Homes*, The Journal of the American Medical Association, http://www.medem.com/MedLB/article_detaillb.cfm?article_ID=ZZZV2MOS1UC&sub_cat=392. See also, American Association for Homes and Services for the Aging, http://www.aahsa.org/index.shtml.
[27] *Facts and Figures*, National Emergency Numbers Association (NENA), http://www.nena.org/PR_Pubs/911fastfacts.htm
[28] *A Needs Assessment of the U.S. Fire Service: A Cooperative Study*, Federal Emergency Management Agency (FEMA) U.S. Fire Administration (USFA), National Fire Protection Association (NFPA), FA-240 (December 2002).
[29] Assumes an average of 5 important government buildings per 100,000 people.
[30] *1998 New York Ice Storm: Mitigation Issues & Potential Solutions*, FEMA Region II (1998), http://www.app1.fema.gov/reg-ii/1998/nyice4.htm#ELECTRIC.
[31] *A Needs Assessment of the U.S. Fire Service: A Cooperative Study*, FEMA, USFA, NFPA, (FA-240) (December 2002).
[32] Of the 12 automated systems that are considered mission-critical, one has already been made compliant, one will be upgraded, three have been retired, four more will be retired, and three will be replaced. Testimony of Kathleen Hirning, Chief Information Officer Federal Energy Regulatory Commission, before the Subcommittee on Technology Committee on Science; U.S. House of Representatives (May 14, 1998), http://www.house.gov/science/hirning_05-14.htm.
[33] North American Electric Reliability Council (NERC), http://www.nerc.com.
[34] NERC, http://www.nerc.com.
[35] NERC, http://www.nerc.com.
[36] EIA (2000), http://www.eia.doe.gov/cneaf/electricity/ipp/html1/t17p01.html.
[37] "Between 20 and 100 miles separate pumping stations, depending on the pressure at which the pipeline is operated and upon the terrain over or through which it runs." Association of Oil Pipe Lines, http://www.aopl.org/about/questions.html. We used a 60-mile separation to derive estimate.
[38] Compressor station every 60 miles for high-pressure natural gas transmission pipelines. *PennWell*, http://www.pennwell.com.
[39] *National Transportation Statistics 2002,* Bureau of Transportation Statistics (BTS), http://www.bts.gov/publications/national_transportation_statistics/2002.
[40] *National Transportation Statistics 2002*, BTS, http://www.bts.gov/publications/national_transportation_statistics/2002.
[41] *Economic Reports: Operators & Producing Wells,* Independent Petroleum Association of America (IPAA) (2002), http://www.ipaa.org/info/econreports/usps.asp?Table=Chart03.
[42] *Economic Reports: Operators & Producing Wells,* IPAA (2002), http://www.ipaa.org/info/econreports/usps.asp?Table=Chart03.
[43] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[44] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[45] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[46] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[47] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[48] *Fueling the Future*, American Gas Association, http://www.fuelingthefuture.org/contents/ExpandingNaturalGasDelivery.asp
[49] U.S. Geological Survey, http://ga.water.usgs.gov/edu/tables/mapwwfac.html.
[50] American Water Works Association, http://www.awwa.org/Advocacy/pressroom/waterfax.cfm, http://www.awwa.org/Advocacy/pressroom/TrendsIssues/.
[51] The Federal Aviation Administration (FAA) has 4 Air Route Traffic Control Centers (ARTCC) and 19 Air Traffic Control Towers (ATCT), http://www2.faa.gov/index.cfm/1042/. See http://www2.faa.gov/index.cfm/1043/ for ATCT list. FAA also has Automated Flight Service Stations, Automated International Service Stations, and Terminal Radar Approach Control Facilities, http://www2.faa.gov/index.cfm/1042; 19 Airport Traffic Control Centers (ATCC) http://www2.faa.gov/index.cfm/1043/; 24 Automated Flight Service Stations (AFSS); http://www2.faa.gov/index.cfm/1044; 3 Automated International Flight Service Stations (AIFSS) http://www2.faa.gov/index.cfm/1045; 6 Terminal Radar Approach Control (TRACON) Facilities http://www2.faa.gov/index.cfm/1046
[52] There are nearly 20,000 airports nationwide, but only 5,300 are designated for public use. We estimate that roughly 75 percent of these, or 4,000, have control towers.
[53] Class I rail. Number of rail control centers assumes one per 1,000 miles of track. *National Transportation Statistics 2002,* BTS, http://www.bts.gov/publications/national_transportation_statistics/2002.
[54] Municipal DOTs as well as private companies such as Metro Networks, which runs 68 centers nationwide, operate traffic control centers. Traffic data is gathered by electronic and human means, crunched, and then transmitted to radio and TV stations, Web sites, and wireless service providers. Dan Baum and Sarah Schmidt, *Free-Market Gridlock*, Wired (November 2001), http://www.wired.com/wired/archive/9.11/usa-traffic.html. There are, for example, 3 VDOT operated traffic control centers in VA http://www.virginiadot.org/infoservice/news/newsrelease-stc-alerts.asp and 8 GDOT traffic centers in GA.
[55] *Security Guidance for the Petroleum Industry*, American Petroleum Institute (March 2002).
[56] See in particular the work at the Energy and Critical Resources program at the Sandia National Laboratories, http://www.sandia.gov/programs/energy-infra.
[57] Marsh, R. T., *Critical Foundations: Protecting America's Infrastructure*, President's Commission on Critical Infrastructure Protection (October 1997), http://cyber.law.harvard.edu/is03/Readings/critical_infrastructures.pdf.
[58] *Information & Communications Sector: National Strategy for Critical Infrastructure and Cyberspace Security* (May 2002).
[59] *Chicago Metropolitan Area, Critical Infrastructure Protection Program: Critical Infrastructure Assurance Guidelines For Municipal Governments Planning For Electric Power Disruptions*, DOE, Metropolitan Mayors Caucus, City of Chicago (February 2001).
[60] *Energy: The First Domino in Critical Infrastructure*, Computer World (September 2002).
[61] 790 GW is net summer capacity at electricity-only plants. Total capacity for all sectors is 855 GW, which includes independent power producers, commercial plants, and industrial plants. *Annual Energy Review 2001*, EIA, http://www.eia.doe.gov/emeu/aer/contents.html.
[62] Total additions to grid capacity were 12 GW in 1999, 31 GW in 2000, and 48 GW in 2001. *Annual Electric Generator Report - Utility* and *Annual Electric Generator Report – Nonutility*, EIA (1999, 2000, 2001).
[63] *U.S. Industrial Battery Forecast*, Battery Council International (April 2002).
[64] Hurricane Fran left 792,000 Progress Energy customers without power and was designated by FEMA as the "largest concentrated power outage caused by a hurricane in U.S. history." Progress Energy, http://www.progress-energy.com/aboutenergy/learningctr/stormtips/hurricanespast.asp. See also National Oceanic and Atmospheric Administration, http://www.noaa.gov/hurricaneandrew.html. Ice storms in the Northeast in 1998 and in the Carolinas in 2002 left hundreds of thousands without power.
[65] *IEEE Recommended Practices for the Design of Reliable Industrial and Commercial Power Systems,* Institute of Electrical and Electronics Engineers (IEEE), (IEEE Std 493-1997).
[66] *IEEE Recommended Practices for the Design of Reliable Industrial and Commercial Power Systems,* IEEE, (IEEE Std 493-1997).
[67] *Making the Nation Safer: The Role of Science & Technology in Countering Terrorism,* National Academy of Sciences, National Research Council (2002).
[68] *1999 Commercial Buildings Energy Survey: Consumption and Expenditures,* EIA.
[69] *Manufacturing Consumption of Energy 1998,* EIA.
[70] *IEEE Recommended Practices for Emergency and Standby Power Systems for Industrial and Commercial Applications*, IEEE (Revision of IEEE Std 446-1987) (December 1995).
[71] *IEEE Recommended Practices for Protection and Coordination of Industrial and Commercial Power Systems*, IEEE (IEEE Std 242-2001).
[72] *1999 Commercial Buildings Energy Survey: Consumption and Expenditures*, EIA.
[73] Statistical average calculated from total sub-sector annual electric use based on assumption of 100 hr/wk operation of all buildings yielding an approximation not accounting for peak building demand or high (or low) duty cycle buildings.
[74] *The Cost of Power Disturbances to Industrial & Digital Economy Companies,* Electric Power Research Institute (EPRI), prepared by Primen (June 2001).
[75] *Manufacturing Consumption of Energy 1998*, EIA.
[76] The Manufacturing Institute, *The Facts About Manufacturing,* http://www.nam.org/secondary.asp?TrackID=&CategoryID=679.
[77] University of Delaware's Disaster Research Center quoted in *Disaster Recovery for Business, Operation Fresh Start,* DOE, http://www.sustainable.doe.gov/freshstart/business.htm.
[78] See *Dig More Coal, The PCs are Coming*, *Forbes* (May 31, 1999), and more recently *Silicon and Electrons* (February 2003), http://www.digitalpowergroup.com/Downloads/Silicon%20and%20Electronics.html.
[79] *Analysis of Extremely Reliable Power Delivery Systems: A Proposal for Development and Application of Security, Quality, Reliability, and Availability (SQRA) Modeling for Optimizing Power System Configurations for the Digital Economy,* EPRI, Consortium for Electric Infrastructure to Support a Digital Society (April 2002).
[80] Huber, Peter and Mark Mills, *Silicon and Electrons* (February 2003), http://www.digitalpowergroup.com/Downloads/Silicon%20and%20Electronics.html.
[81] *Office Equipment in the United Kingdom, A Sector Review Paper on Projected Energy*

Consumption For the Department of the Environment, Transportation, and the Regions," (January 2000).

[82] *Electricity Use Soars*, Crain's New York Business (May 19-25, 2003). "New York's electric demand continues to rise and shows little sign of abating. Unless significant generating capacity is added to the system—and soon—demand is going to overwhelm supply and reliability will be at risk," said William J. Museler, NYISO President and CEO. "Because of the two-to-three year lead time to build large baseload plants, if New York is to remedy this situation it needs to get a new siting law in place, plants approved and construction commenced immediately." *New York Independent Operator Announces Summer Electricity Forecast*, NYISO Press Release (February 25, 2003).

[83] *Digital Economy 2002,* Economics and Statistics Administration, U.S. Department of Commerce (February 2002), http://www.esa.doc.gov/508/esa/DIGITALECONOMY2002.htm.

[84] Oliner, Stephen D. and Daniel E. Sichel, *Information Technology and Productivity: Where Are We Now and Where Are We Going?* Federal Reserve Board (May 10, 2002), http://www.federalreserve.gov/pubs/feds/2002/200229/200229pap.pdf.

[85] *Annual Energy Outlook 2003,* EIA, DOE (January 2003), http://www.eia.doe.gov/oiaf/aeo/pdf/0383(2003).pdf.

[86] *Top Security Threats and Management Issues Facing Corporate America*, Pinkerton (2002), http://www.pinkertons.com/threatsurvey/default.asp.

[87] *Revalidation of CIP F-11, Power Systems Sustained Support (PS 3) Program,* FAA (November 12, 1998).

[88] *Power Systems Sustained Support, Investment Analysis Report*, FAA (May 23, 2000).

[89] *Power Systems Sustained Support, Investment Analysis Report,* FAA (May 23, 2000).

[90] For the 'bible' on high-power silicon systems for grid-level upgrades, see: Hingorani and Gyugyi, *Understanding FACTS: Concepts and Technology of Flexible AC Transmission Systems*, IEEE Press (2000).

[91] NERC was designated as the federal government's "Electricity Sector Information Sharing and Analysis Center," to gather and interpret security-related information and disseminate it within the industry and the government. NERC has developed a best-practices document - *Security Guidelines for the Electricity Sector* (June 2002), http://www.nerc.com/~filez/cipfiles.html.

[92] Currently, United Technologies' 200 kW ONSI is the only commercially available fuel cell; roughly 100 of these molten carbonate systems are installed

[93] *Environmental Assessment: The Regenesys Energy Storage System*, Tennessee Valley Authority (August 2001), http://www.tva.com/environment/reports/regenesys/chapter_2.pdf.

[94] See for example: *Interconnection and Controls for Reliable, Large Scale Integration of Distributed Energy Resources; Consortium for Electric Reliability Technology Solutions, Grid of the Future White Paper*, DOE (December 1999); *Distributed Energy Resources Interconnection Systems: Technology Review and Research Needs*, DOE National Renewable Energy Laboratory, (September 2002).

[95] *Onsite Power for C&I Customers,* Chartwell Inc. (2002)

[96] *Standard for Emergency and Standby Power Systems,* NFPA (2002).

[97] *AEP Dedicates First U.S. Use of Stationary Sodium Sulfur Battery*, PRNewswire (September 23, 2002).

[98] See Powerware UPS systems incorporating the Active Power flywheel.

[99] Data from DOE/EIA *Commercial Building data*, Petroleum Distributors Association and the FAA. .

[100] *Sandia SCADA Program: High-Security SCADA LDRD Final Report*, Sandia National Laboratories (April 2002), http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/2002/020729.pdf.

[101] Fairfax, Steven. *Credit Cards Lessons for Life-Support Systems*, Mtechnology (July 30, 2001).

[102] *Power Systems Sustained Support: Investment Analysis Report*, FAA (May 23, 2000).

[103] *Private Sector Spending*, Homeland Security & Defense (July 16, 2003) (From a June 2002 analysis by Deloitte Consulting).

[104] *Skeptical of Attacks…* Homeland Security & Defense (October 23, 2002) (Less than half of 230 companies surveyed by the Council on Competitiveness are spending any more on security than they were a year ago).

[105] Survey sponsored by ASIS International, an Alexandria, Va., organization of security professionals.

[106] Winona Daily News (June 15, 2003), http://www.winonadailynews.com/articles/2003/06/15/news/03lead.txt.

[107] Pacific Gas and Electric, for example, first targets restoration of generation and distribution facilities serving public service and emergency service agencies like hospitals, police, fire, water pumping stations, communication facilities, and critical service to small groups or individuals. (http://www.pge.com/004_safety/004c9_restoration_po.shtml) The Rockland Electric Company of Rockland New Jersey offers a 24-hour hotline and first priority status for restoration of service to residential customers who rely on life support equipment such as kidney dialysis machines, apnea monitors, oxygen concentrators, respirators, ventilators, and infusion feeding pumps. (http://www.oru.com/publications/RECO-RR2001.pdf) Tampa Electric restores power first to hospitals, disaster centers, and police and fire stations. It then concentrates on water and sewer installations, followed by telephone service and residential customers who depend on power for life-support systems. (http://www.tampaelectric.com/TENWRelease091499a.html)

[108] See for example: *Blackstart Regional Restoration Plan,* Southeastern Electric Reliability Council (March 14, 2003).

[109] *Critical Infrastructure Assurance Guidelines For Municipal Governments: Planning For Electric Power Disruptions,* Washington Military Department, Emergency Management Division (February 2001), http://emd.wa.gov/3-map/a-p/pwr-disrupt-plng/14-app-b-franchise.htm.

[110] *Power Systems Sustained Support, Investment Analysis Report*, FAA (May 23, 2000).

[111] See www.tsp.ncs.gov

[112] See http://www.ncs.gov/Nstac/IssueReview98/PreviouslyIssues.html

[113] *Generic Standards for E9-1-1 PSAP Equipment*, National Emergency Number Association (NENA) (June 20, 1996).

[114] See www.fcc.gov/hspc/emergencytelecom.html. More information appears at tsp.ncs.gov.

[115] The Wastewater Committee Of The Great Lakes – Upper Mississippi River Board Of State And Provincial Public Health And Environmental Managers, http://www.dec.state.ny.us/website/dow/10states.pdf

[116] *1998 New York Ice Storm: Mitigation Issues & Potential Solutions*, FEMA (1998), http://www.app1.fema.gov/reg-ii/1998/nyice4.htm#ELECTRIC.

[117] *The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets,* The White House (February 2003).

[118] See http://www.nipc.gov/sites/newrelatedsites.htm.

[119] See http://www.tisp.org.

[120] *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO (January 2003).

[121] *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO (February 2003).

[122] *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,* Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency; and Securities and Exchange Commission (April 7, 2003).

[123] *Banking and Finance Sector National Strategy,* The National Strategy for Critical Infrastructure Assurance (May 13, 2002).

[124] See http://www.ntsb.gov/aviation/report.htm.

[125] See http://asrs.arc.nasa.gov/overview_nf.htm.

[126] See generally: *National Strategy for Critical Infrastructure and Cyberspace Security,* CTIA; ITAA; TIA; USTA (May 2002).

[127] See http://www.nei.org/index.asp?catnum=2&catid=57.

[128] See http://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1982/gl82004.html.

[129] See, for example, *Security Guidelines for the Electricity Sector,* NERC (June 2002), http://oea.dis.anl.gov/documents/Security_Guidelines_for_the_Electricity_Sector_June_2002.pdf.

[130] *Critical Foundation*s, President's Commission on Critical Infrastructure Protection (October 1997).

[131] See http://www.weatherdata.com/products/index.php; http://www.thorguard.com/about.asp; http://www.meteorlogix.com/products/mxinsight.cfm.

[132] Statement of Dr. Samuel G. Varnado, Sandia National Laboratories, United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations (July 9, 2002).

[133] *Internet Security Threat Report: Attack Trends for Q1 and Q2 2002,* Riptech (July 2002).

[134] See http://www.serc1.org/minutes/mic-0303/mic0303a.pdf.

[135] *Critical Infrastructure Protection Advisory Group Scope*, NERC (January 17, 2003).

[136] *The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets*, The White House (February 2003).

[137] *Report To Congress On The Feasibility Of Establishing A Heating Oil Component To The Strategic Petroleum Reserve*, DOE (June 1998).

[138] http://www.newrichmondutilities.com/business_customers/default.asp?CategoryNumber=3&SubcategoryNumber=1.

[139] *Interconnection and Controls for Reliable, Large Scale Integration of Distributed Energy Resources,* Consortium for Electric Reliability Technology Solutions, Grid of the Future White Paper, DOE (December 1999).

[140] *Distributed Energy Resources Interconnection Systems: Technology Review and Research Needs*, National Renewable Energy Laboratory (September 2002).

[141] *IEEE Recommended Practices for the Design of Reliable Industrial and Commercial Power Systems*, IEEE (December 1997).

[142] See http://www.energy.ca.gov/distgen/interconnection/ieee.html.

[143] See http://ferc.gov/Electric/gen_inter/small_gen/RM02-12-000.pdf.

[144] In 1995, the EPA conducted a survey of oil storage facilities potentially subject to the Agency's SPCC regulation. The survey found approximately 438,000 facilities, and estimated that there were well over 1 million underground storage tanks in the country subject to SPCC oversight.

[145] See http://www.distributed-generation.com/regulatory_issues.htm.

[146] Broadcast Engineering, http://broadcastengineering.com/ar/broadcasting_ups_backup_power.

[147] The Security Industry Association and Real Estate Roundtable are lobbying passage of a bill introduced this past March to amend federal tax laws to allow full deduction for homeland security expenses (Public Safety and Protection Act, HR 1259). The bill would provide for 100 percent expensing of a wide variety of security-related costs ranging from hardening physical premises, to software, biometrics, and "computer infrastructure."