The ABCs of UPSs

A White Paper prepared by

Liebert Corporation

What does it cost you when a computer freezes, loses data, or “hard crashes”? A recent study projected the cost of such interruptions at more than $4 billion annually, with the annual lost productivity of workers estimated at 37 million hours. The major cause of the costly break in computer services was identified as power disturbances.

Today’s power disturbances come from a surprisingly wide range of sources, and include sags, noise, blackouts, and surges. The ways to address these problems are equally complex, as we will discuss. Although the formula does exist for determining any given load requirement, the answer to your organization’s power protection problems has moved far beyond a single mathematical equation. The solution, like your computing environment, is likely a complex one and will evolve out of a careful study of your organizational makeup, needs, and future expansion plans.

Power Protection Today

Once computer equipment was housed exclusively in specialized environments, often referred to as “glass house” computer rooms, complete with their own air conditioning systems to protect sensitive electronics from temperature and humidity fluctuations and airborne contaminants. However, the explosive growth in the use of personal computers and networks has made data processing an increasingly distributed activity. In recent years, a new concept has emerged. This concept packages uninterruptible power supplies (UPSs) with computer-grade environmental control in an integrated package. The result is a comprehensive computer support system for both individual and clustered network components. Such a system encompasses precise control over air temperature, humidity, and cleanliness; conditioned, uninterruptible power; and improved security for network components. This packaged approach offers numerous advantages over traditional “built-up” systems. In addition, a modular design facilitates growth because additional units can be “clustered” as required.

Another approach to integrated computer support combines UPSs, power distribution units, and air conditioning units. Typical applications include enterprise-wide networking, mid-range computer systems, file servers, large telecommunications equipment rooms, and voice/data/video centers. Such a support structure can be configured with almost any combination of modules to match many floor plans and protection requirements.

Power Facts and Considerations

Power disruptions are behind many of the lost or scrambled data, keyboard freezes, and unexpected shutdowns that computers, and often entire networks, experience. A typical computer and computer network system may experience anywhere from 92.2 to more than 120 power disturbances a month. In fact, there are 344 potentially damaging power glitches in a typical electric line leading to a computer or network.

Power problems overseas can often be far worse, particularly in underdeveloped areas in such parts of the world as India, South America, and the Orient. There, the availability of electricity

from the power grid is unpredictable and both the frequency and voltage levels are often poorly regulated.

And the source of these frightening disturbances? Although external forces like the weather and power utilities play a part, you might be surprised to learn that the most common source of power problems can be found right on your own premises. Studies have shown the majority of all power disturbances are caused by building equipment, including printers, copiers, microwaves, and particularly by industrial or process equipment such as arc welders and large electrical motors. If your building is an older structure, chances are the wiring is not designed to handle networked equipment, compounding the problem. Add to that the risk of internally-generated power disturbances created by a large or more complex network, and you have a greater likelihood for crippling power disturbances even without a natural disaster or unreliable utility supply.

The large number of potential power source problems, in turn, creates an array of power disruptions. Servers, PCs, workstations, hubs, routers, and other sensitive components must be also configured to handle everything from power surges, sags, and brownouts to noise, and other power irregularities.

The Bottom Line

With all of this damaging potential, it's no wonder that AC power-related problems have been estimated to cost U.S. companies more than $26 billion annually in lost time and revenue. Almost half the corporations in a recent U.S. survey estimated their downtime costs due to power problems at $1,000 per hour or more. Nine percent of them estimated downtime costs of roughly $50,000 per hour.

You can estimate these costs for yourself by totaling your direct and indirect costs of losing, then regaining operation of your critical systems.

Hourly Cost Calculation	
First calculate an average hour value in your organization:	
Annual gross revenues/2000 hours = Hourly Contribution	1
Hourly contribution/Number of employees = Average Hourly Employee Contribution	2
Data Loss Calculation	
Hours required to replace lost data	3
Times Average Hourly Employee Contribution *(Line 2)*	x 4
TOTAL	= 5
Employee Downtime Calculation	

Hours the system is down	6
Times Hourly Contribution *(Line 1)*	x 7
TOTAL	= 8
Special Costs	
First calculate an average sales/customer value in your organization:	
Annual gross revenues/Number of sales = Average Sales	9
Annual gross revenue/Number of Customers = Average Customer Value	10
Sales Loss Calculation	
Estimated lost sales x Average Sales *(Line 9)*	11
TOTAL	= 12
Image Loss Calculation	
Estimated lost customers	13
Times Average Customer Value *(Line 10)*	x 14
TOTAL	= 15
Total Costs	
Data Loss *(Line 5)*	+ *
Employee Downtime Loss *(Line 8)*	+ *
Sales Loss *(Line 12)*	+ *
Image Loss *(Line 15)*	+ *
Total Cost Per Hour of Networking Downtime	= *

If the final cost estimate concerns you, weigh this cost against the cost of quality power protection. You may find it's time to evaluate your computer protection options.

Trends In Power Protection Choices

The network or computer systems that run the organizational structure of today, with its interactive workflow and tight deadlines, requires a new level of protection reliability. Devices should be connected to equipment that conditions and filters line power, as well as provides continuous, computer-grade power. There are many choices for power conditioning and protection, ranging from simple line filtering to power backup to combinations of both.

Surge protectors, voltage regulators, line conditioners, and filters will provide some level of utility power conditioning. However, none of these options protect against all types of power disturbances. And none will protect your data should a brownout or blackout shut down your computer or electronic equipment.

Standby generators can supply power for extended periods of time should utility power be removed. These devices, however, must be turned on and will take several minutes to stabilize before they supply power to a computer or network, as frequency varies. If a generator is powering an electronic device during stabilization, the device will still experience power disturbances. Also, because they are off-line until needed, standby generators do not condition the utility power that is currently going to the attached load.

UPSs Of Today

What is the right power protection solution for you? In configuring the most cost-effective and reliable means of protection, you must also consider all of your computerized needs against a range of available applications, including the most appropriate UPS technology, control software, load size and battery time.

Then there are the factors which, taken together, can serve as a solid foundation for an overall power protection strategy. Current considerations which may affect your long-term satisfaction encompass UPS configuration (e.g, rack, tower, or desktop); size (accounting for the types of systems in use, the range of applications, as well as the number of nodes in one or multiple locations); communication level (from simple shutdown capabilities to highly intelligent, SNMP-based monitoring and control); upgradeability; and support (determining the scope and availability of service locations, as well as the supplier’s reputation for reliability and support).

By matching all of these capabilities and options with your current and future needs, the right UPS can protect almost any class of computing and networking equipment. Among the most popular types of UPS devices, are the on-line, stand-by, and line-interactive protection systems.

On-line protection. This alternative provides the highest levels of network protection, conditioning and UPS available. In an on-line UPS, the inverter -- a device that converts DC to AC -- supplies conditioned power to attached devices all of the time. Most on-line UPSs supply five to 10 minutes of battery backup, which is more than enough for 98% of all blackouts, as studies show these situations typically last no longer than two minutes. For the other 2% of blackouts, on-line UPSs are available with extended battery capabilities. On-line technology is often the best choice to protect critical applications -- those systems that simply can not be “down.”

Stand-by protection. Off-line, also called stand-by, is a cost-effective choice for small, non-critical stand-alone applications, for example, isolated PCs and peripherals. While these computers can be connected to a network, communications is usually not a necessary component and a stand-

by UPS provides sufficient back-up. This type of UPS typically powers the load from the utility input when available, but switches to the inverter (supplied by the battery) when the utility fails. Stand-by UPSs include a battery charger to maintain the charge.

Line-interactive protection. For highly effective power conditioning plus UPS back-up, there is line-interactive technology. This is particularly applicable in areas where power outages are rare, but where there are frequent power fluctuations. For instance, power-hungry equipment in most industrial applications switches on and off frequently, causing voltage fluctuations that, while not as damaging as a complete loss of power, can still result in destroyed data or system-wide corruptions. Network

communications is available in line-interactive UPSs, though often not necessary.

Network-wide protection. Today, many UPSs protect their entire networks, including computers, routers, hubs, and other attached electronic equipment. Interoperability is a key requirement for any device that many connect to a network. While network-wide power protection can be represented in a simple shut-down interface, today's increasingly complex networks have a real need for built-in network communications to ensure reliability and compatibility among all the various devices connecting to it. The standard communications protocol UPS vendors are using is called Simple Network Management Protocol (SNMP). Because this standard defines how UPSs and other devices communicate over all networks, SNMP capability, in turn, enables UPSs to do more than ever before -- and to do it more "intelligently." UPSs with SNMP communications, for example, can log events, continuously monitor power quality, report on battery status, load, and temperature, and perform self-management diagnoses.

Facility-wide Protection. Designed to handle unbalanced and 100% non-linear loads, these UPS devices provide conditioned power instantly to the continually shifting levels of power demand common to most facility-wide systems. With an input power factor over 90% even at a partial load, the units offer smaller wiring requirements and lower installation costs. They also can help with power factor correction, a welcome balance against the rising rate of most facility utility bills. And there is a growing trend toward custom-designed facility protection packages. Not only are they tailored to your exact specifications, but they often include such custom services as delivery of the UPS unit complete with standby power systems and even power distribution cables cut to specified lengths. Other expert services can include installation, testing, some start-up services, preventive maintenance, and operator training as well.

Multiple Levels of Power Management

Just as power protection is a complex issue unique to every organization, network communications and control must also be suited to the needs of each network.

Today, multiple levels of communication options are available, from basic to highly intelligent monitoring and management technology.

Some organizations need a simple shutdown interface, such as an add-on or optional feature that sends a signal by cable from the UPS to a protected device. Other, more decentralized or complex networks might need to explore a UPS communications package that includes monitoring as well as shutdown capabilities. In this level of protection, the UPS status and alarms are monitored and logged on a protected device or the network server.

The most advanced power protection systems now extend to highly intelligent forms of network monitoring and control. One option is to monitor and control your UPS via network management software, the best of which is based on the universal Simple Network Management Protocol or SNMP. The most advanced SNMP-based systems not only give computer and network operations managers control of UPSs and environmental support functions, but they also allow the monitoring of other vital network protection systems such as water detection, smoke and fire protection devices, access controls, or just about any electronically-controlled equipment.

The very latest UPS technology even extends beyond the UPS itself. Now users also can monitor temperature and humidity in critical spaces, remotely reset locked equipment, and remotely schedule on/off cycles. For example, Liebert's SiteNet Integrator™ provides protection and network management capabilities to software that oversees network operations. This advanced package lets you control uninterruptible power supplies and environmental control systems, as it allows you to monitor up to 10 other vital protection systems.

Power Planning

The final element in choosing the right power protection system is to define what functions and applications are mission critical within your organization and which are not. To determine this (and therefore what level of protection is necessary for your entire organization or in specific locations), place each of your major company operations into one of three categories of importance: business continuity ("If it isn't running, my business stops"); mission critical ("It has a significant impact on the business"); or non-critical "It's inconvenient but of no major consequence"). Examples of operations under the business continuity category would be 1-800 telephone order fulfillments or real-time MRPII systems. Electronic cash registers and unitary data analyses, on the other hand, would be examples of mission critical operations. Non-critical operations might be defined as individual workstations or printing functions.

Once you've categorized your business operations, you can begin to identify the network equipment and equipment protection vital to each. For instance, for your non-critical operations, off-line or line-interactive UPSs, with five to 10 minutes of battery back-up would certainly be sufficient. On the other end of the spectrum, those operations that are critical to running the business would need to be matched with a system of comprehensive communications and at least an on-line UPS, standby generation or 90+ minutes of battery back-up, as well as security or environmental protection.

A rule of thumb is to allocate 4-7% of your total budget to power protection, with the higher percentage going to networks that have substantial functions that could be classified under "mission critical" or "business continuity."

Solutions, Not Simple Answers

In the end, there are no hard and fast rules. As the systems which are our productivity tools of today grow and change in size and complexity, power protection devices must also be flexible enough to meet those changing needs. The growing popularity of the decentralized work environment means power protection needs to be more widespread and reliable than ever. The task of identifying what is worth protecting and what level of protection is the most cost-effective for your organization is not simple. Not only must you take into consideration today's critical demands, but also you must configure solutions that you can live with tomorrow. But is it critical.

The direct and hidden costs associated with “fixing” what amounts to the lifeline of your business over and over again, is too great a risk to ignore.

Because today’s complex computing and networking systems are so crucial to business operations, businesses need UPS systems to deliver the clean, uninterruptible flow of power today’s equipment demands. Networks can’t afford to be down, and network managers will find that UPSs are an important tool in keeping their networks up and running.

Liebert Corporation is an independent subsidiary of Emerson Electric Co., headquartered in Columbus, Ohio. Represented in more than 100 countries, Liebert designs, manufactures, services and distributes systems that control temperature and humidity, condition power, guard against outages, and monitor and control access to critical spaces. According to end-user research conducted by Venture Development, Liebert ranked among the top vendors in product quality and service.

For more information, contact Liebert Corporation at (800) 877-9222.