IEEE SPECTRUM
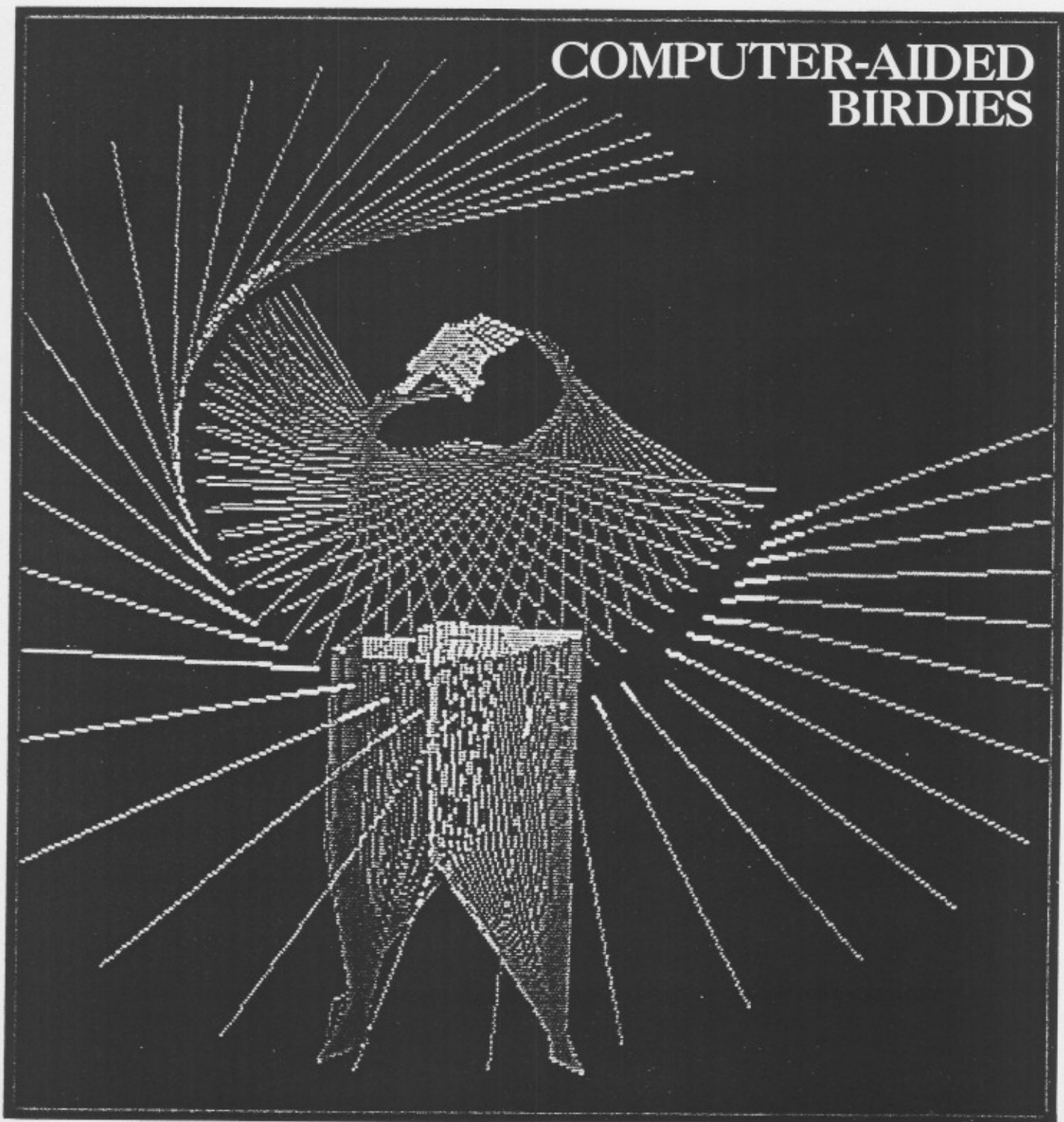
Competing in a global economy
Diagnostic imaging networks for hospitals
Transient-proof computing

COMPUTER-AIDED BIRDIES

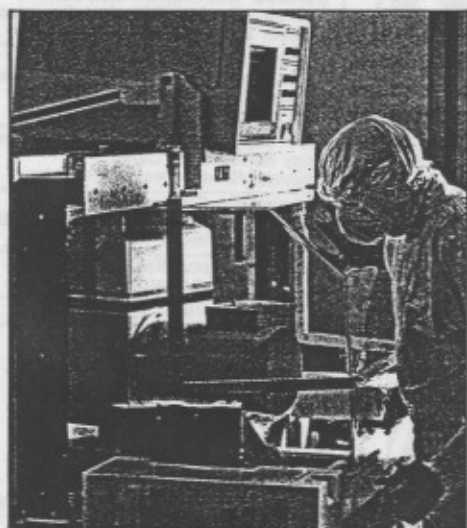# IEEE
SPECTRUM

VOLUME 27   NUMBER 4   APRIL 1990

Cover: *A golfer's swing is analyzed by means of a videotape that is digitized for processing by computer. The computer connects digitized points derived from club, arm, and other significant areas into colored line segments representing the different objects and body parts. Golf is not the only sport to benefit. More on p. 43.*
Photo: Peak Performance Technologies Inc.

Lightning-induced transient destroyed telecom IC's packaging **37**
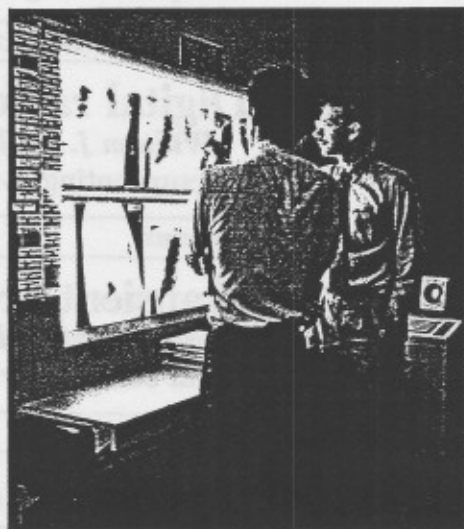
Physicians view multiple X-ray films on a medical center's 'alternator' **33**

Protecting computer systems against power transients

Because small systems have moved from computer rooms into offices, factories, and homes, users and systems designers must deal with the subtle dangers the machines encounter

SYSTEMS
POWER SUPPLIES

For the third time in less than three weeks, the sky darkened and thunder rumbled in the distance. With that ominous warning, the appointed "thunder scout" decided it was time to pull the plugs of the central unit and remote terminals of his CAD/CAM computer system. Better to shut down the operation than risk damage to the system, as had occurred in the two previous storms.

But pulling the plugs did not help. When the storm was over and the system was restarted, permanent damage had been done to it—to the chagrin of both the operator and the service contractor.

In this common example, the damage was caused not by power-line surges but by differences in ground potential at various terminals of the system. The oversimplified assumption that power-line surge problems could be eliminated had led the uninformed operator to attempt a simple prevention step. Not only did it not work, but it created a safety hazard: unplugging the line cords removed the safety ground, leaving the equipment still connected to the data lines where the surges were occurring.

Understanding the general causes of, and remedies for, power transients can help users of small computer systems, especially stand-alones, protect their systems with do-it-yourself methods. More complex systems may need the attention of a specialist. Systems designers should also be aware of the way users hook up their systems, the potential damage that could be caused by power transients, and side effects of incorrectly applied measures.

Growing concern among computer users that power-line surges may damage equipment or cause loss of data has created a market for surge suppressors. But clear performance standards in the industry are lacking, and several standards-writing groups are striving to develop adequate ones. To make a difficult choice among these devices, the consumer should learn some basic rules about selecting and installing a suitable surge suppressor. Even the best surge suppressor, if incorrectly applied, might not work and could cause adverse side effects.

Transient origins

While the term "transient" is often understood as a transient overvoltage, it is also more broadly interpreted as the occurrence of any disturbance, either on the power line or the computer system's data line.

The most obvious source of an electrical disturbance is a lightning strike, but the lightning bolt need not hit power lines to cause damage. Because the electromagnetic field radiated by the lightning current couples into the conductors of power lines or data lines, it induces transient voltages along these conductors. Also, as the lightning current spreads into the ground, it produces differences in potential at points that are normally at "ground" potential. Conductors spanning some distance between their ends

François Martzloff
National Institute of Standards and Technology
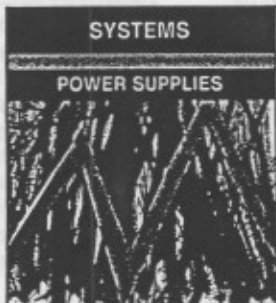
in the area where the lightning current is spreading will be exposed to these differences of potential, or to a transient overvoltage.

Though the direct effects of lightning can be dramatic, their relatively low rate of occurrence can lull one into complacency, and most of their widespread indirect effects can be overcome through sound protection practices. On the other hand, electrostatic discharges, which could be considered miniature lightning discharges, require only the fingertips of mortals rather than an Olympian fistful of lightning bolts to have very serious effects ["How to defeat electrostatic discharge," *IEEE Spectrum*, August 1989, pp. 36–40].

A less obvious but more frequent source of transients is switching sequences in the power system. Switching can be a normal, recurrent operation such as turning a local load on and off, or it could entail occasionally clearing an overload or short circuit.

These switching transients cover a wide range of frequencies and amplitudes. Some have a brief duration (nanoseconds) and involve little energy (millijoules). While they present little risk of damage, their high-frequency spectrum makes them likely sources of interference. Others have a longer duration (microseconds or even milliseconds) and involve greater energy (up to hundreds of joules) with lower frequencies. They have the opposite trait of low risk of interference because of the relatively low frequencies, but because of the longer duration and increased energy, they have a higher damage risk.

Another source of disturbance to computer systems is the occurrence of an undervoltage that could be caused by a nearby startup of heavy loads or by distant faults, such as lightning-induced line flashover, falling trees, or utility lines downed by runaway vehicles. While transient overvoltages can be easily suppressed—a more correct description would be "mitigated"—by a simple added device that diverts the excess energy, the reduced energy associated with an undervoltage cannot be supplemented by a simple device. Different methods are needed for a solution of that problem.

Over the years, the need to learn more about the characteristics of these transients has led to various projects aimed at monitoring power-line disturbances. One result of these projects—which are performed by isolated researchers, sometimes with equipment designed by the researchers rather than commercial equipment—is that their reports are based on different assumptions and definitions of disturbances. Comparing results can thus become difficult and confusing [see table, overleaf].

Leaving the problems of monitoring transients and designing protective devices to the specialists, an informed user can take several steps toward buttressing the reliability and integrity of the system. The first step is to distinguish between mere temporary upset and permanent damage, each of which has a different impact on the user, depending on the relative importance of the operation. For a commercial setup, disrupting the operation can be more expensive than repairing the damage so that protecting

data integrity ranks high. For an engineer working at his home computer, however, damage protection may be more important than some data loss. In this case, limiting the protection expense to avoiding damage and accepting interruptions may be preferred.

Vulnerable stand-alones

Small computer "systems" can be categorized as stand-alone systems or distributed systems. A stand-alone system is typically a one-operator setup consisting of a desktop computer coupled with a printer, or any microcomputer not linked to a network. Distributed systems range from a simple stand-alone augmented by a telephone or other network link to multiple-station systems or process control systems with remote sensors and actuators.

Found in offices, laboratories, and homes, stand-alone systems can be disrupted or damaged by two possible causes. First, transients with low amplitudes (less than 1000 volts) are buffered by the computer's power supply but might still couple into circuits and cause glitches. Transients of high amplitudes (over 1000 V) may at worst damage the power input components and are likely to cause glitches at best. Second, power interruptions (sags or outages) can cause a momentary shutdown.

Transient damage protection for these systems is simple to achieve and is probably built in to some degree. However, until the day arrives when equipment has its transient capability stated on the nameplate (which may be sooner than expected because the Europeans are increasingly concerned with electromagnetic

compatibility issues), the user has no way to know the extent of that protection. The European approach, motivated by a 1989 Directive on Electromagnetic Compatibility promulgated by the European Community Council, requires that equipment must operate satisfactorily in a specified environment without introducing intolerable disturbances into that environment. Thus, this ability is likely to be stated explicitly, in addition to the usual voltage, frequency, and current ratings now required.

So far, the approach has been one of purchasing additional peace of mind by inserting a separate surge suppressor (also called spike protector and transient voltage suppressor) on the power cord. Prices for these devices range over an order of magnitude, and claims of performance may include the fastest response (an irrelevant issue) and the lowest clamping voltage (a reliability risk because the transient protector may fail under abnormal power fluctuations).

Though its basic technology does not change rapidly, details of the rating and packaging of a surge suppressor are driven by market competition. Ideally, its rating should reflect three basic requirements: the nominal line voltage, the surge current capability, and the clamping voltage during the surge. All of these should be stated by the maker of the device with due consideration to the user's needs for protection and long-term reliability.
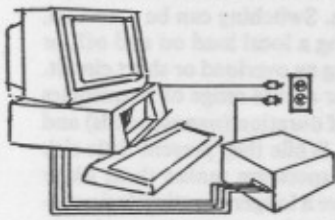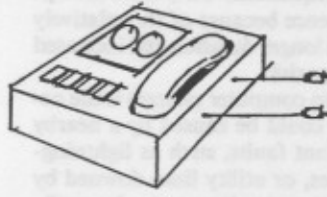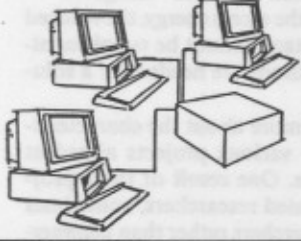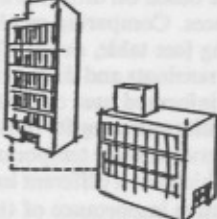
At this time, there is only one performance standard in the United States for transient voltage surge suppressors, UL 1449, which was developed by the Underwriters Laboratories. This standard specifies primarily the safety aspects of the product, but does contain some performance specifications. The UL label on a surge suppressor means that a test has been applied to the device, reflecting industry consensus standards on the severity of the environment. In the UL test, a specified surge current is applied to the device and the maximum resulting voltage is measured; this is then indicated on the product.
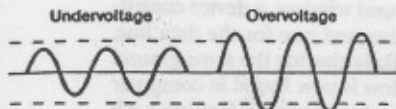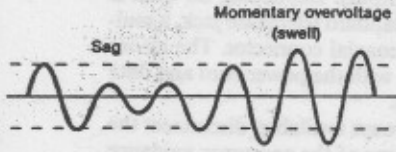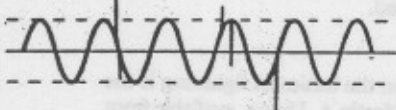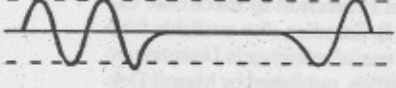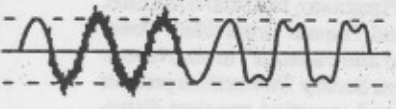
Product literature for some devices, however, makes claims of response time in nanoseconds—even picoseconds—a feature that is not important in a power system. Nanosecond pulses do not propagate very far in power systems, and measuring a picosecond response time in support of the claim would be a technical challenge. Likewise, emphasis on achieving the lowest clamping voltage only demonstrates imbalance in the design goals: the object of a surge suppressor is to lessen the surge level from the thousands of volts that can occur occasionally; it is not to shave off the last tens of volts from the protection level in a "lower is better" bid for ranking in the purchaser's choice. An excessively low clamping voltage introduces the risk of premature aging, even failure, of the device when the power line goes through repeated momentary overvoltages, or "swells."

The second type of distur-

Common troublesome scenarios

	Typical system configurations	Threat	Solution
	Stand-alone with peripherals		
	in same outlet	Line transient	Spike suppressor
	in different outlets	Ground potential differences	Local ground window
	Power-line and data-line interfaces (such as a facsimile or answering machine)	Differences in ground potential during surges, even with individual line protection	Local ground window
	Distributed system with remote terminals (such as three PCs connected to a printer or three dumb terminals linked to a central processing unit)	Line transients in individual cords; operation of built-in suppression raises "ground" potential	Local ground window at each terminal; an optical-fiber link is an alternative
	Systems in separate buildings	Line transients in individual cords; ground potential differences	Special grounding (a specialist's task) because of problems due to ground grid design, National Electrical Code issues, installation, and so on; an optical-fiber link is an alternative

Types of disturbances and effective protection equipment

Waveform	Type of disturbance	Type of equipment affected	Effective protection equipment
Undervoltage / Overvoltage	Undervoltage or overvoltage are conditions of abnormally low or high voltages lasting more than a few seconds and caused by circuit overloads, poor voltage regulation, and intentional reductions by the utility (brownout)	All equipment is affected, although most equipment is designed to tolerate 120 volts ± 10 percent	Voltage regulator, line conditioner, or uninterruptible power supply (UPS)
Sag / Momentary overvoltage (swell)	Voltage sags (voltage decreases outside normal tolerance lasting less than a few seconds) that are often caused when heavy loads are started, by lightning, and by power system faults; swells are brief voltage increases often caused by sudden load decreases or turn-off of heavy equipment	Sags affect power-down-sensing circuitry on computers and large controllers and can cause equipment to shut down; swells can damage equipment (including spike suppressors) that have insufficient tolerance	Voltage regulator, ferroresonant transformer, line conditioner, or UPS
Spikes, impulses, surges	Spikes (impulses, switching surges, or lightning surges) are microsecond- to millisecond-long voltage increases, ranging in amplitude from 200 to 6000 volts and caused by lightning, switching of heavy loads, and short circuits or power system faults	Electronic loads can be destroyed and transformer or motor insulation broken down	Spike suppressor (also called surge suppressor), or some line conditioners
Outage	An outage is the complete loss of power for several milliseconds to several hours and may be caused by power system faults, accidents involving power lines, transformer failures, and generator failures. Some sensitive equipment may be disrupted by outages as short as 15 ms	All equipment is affected	UPS or standby power supply
Electrical noise, harmonic distortion	Electrical noise is a distortion of the normal sinewave power and can be caused by radar and radio transmitters, fluorescent lights, power electronic control circuits, arcing utility and industrial equipment, loads with solid-state rectifiers, and switching power supplies typically used in computer systems	Electrical noise disturbs microprocessor-based equipment, such as microcomputers and programmable controllers; harmonic distortion causes motor loads, such as compressors, pumps, and disk drives, to overheat	Filter, isolation transformer, UPS, or some line conditioners

bance, a sag or outage, cannot be corrected by a surge suppressor. The computer operation is interrupted when the sag or outage exceeds the capability of the internal dc supply to power the logic and memory circuits. Most computers have a built-in capability to maintain operation for a short time when this power is lost, but that supply is drained out if the interruption is long enough. If the computer is using a disk drive when the sag occurs, a shutdown is likely; in an office using several identical machines, some ride through a disturbance while others, especially those reading from a disk, shut down and have to be restarted. Protection against such sags and outages requires an uninterruptible power supply (UPS), which is now readily available. In fact, the volume of UPS production as well as competition has brought prices down so low that purchasing one becomes a viable solution and, for users dependent on the continuity of their operation, a must.

Unexpected problems

A power outage or sag on distributed systems has the same effect as for stand-alone systems. A more subtle problem, however, has crept in for some sophisticated systems that include automatic restart, or rebooting, after a power interruption. Anecdotes have circulated of damage caused by repeated sags during the automatic rebooting sequence, typically occurring because of multiple lightning strokes or during fault clearing with automatic reclosing by the utility system.

In the case of surges, as soon as a simple stand-alone system is augmented by peripherals, additional remote terminals, networking, and sensors that require a data link, the threat that the system will be affected increases. Even what may appear as a stand-alone system, such as a simple desktop pair of a PC linked with a printer, might be at risk if the two units are plugged into different power receptacles fed by separate branch circuits from the breakers.

In addition to the risk of interference or damage from surges on the power line, the data-line input and output ports are also vulnerable. Several mechanisms can inject interfering or damaging transients into the data lines of distributed systems. First, a problem could result because data lines act as antennas that can collect energy from electromagnetic fields and feed it, as noise or surges, to the data port's input or output, the driver or the receiver of the computer, or its peripherals.

The problem's severity increases with the length of the data link.

Within the same room, the risk of damage is minimal. But as the communication link reaches farther out, the risk increases that a surge would not only interfere with a system but could damage it. Though there may be an unknown (to the user) built-in protection or inherent capability of the data port components to withstand these surges, little is known about the occurrence of surges on data lines, compared to that on ac power lines, which makes the task of designing protection difficult.

For users of computer systems in the same room or the same corner of a building, the built-in capability probably suffices. For systems with longer reach, the ultimate protection is an optical-fiber link with no metallic jacket, which provides immunity against noise collection as well as possible surge damage. For these complex systems, however, the do-it-yourself approach should be replaced by one that has been designed by a specialist.

Another mechanism that could cause trouble is the difference in the potential of objects at nominal "ground" potential occurring during surge events. Most data links operate with the signal reference conductor (shield or one wire of a group) connected to the chassis of the equipment. This chassis is in turn connected to the grounding conductor of the power cord supplying the equipment, a requirement of the National Electrical Code. Thus, if lightning or power system faults inject a high current in the site's ground conductors, the potential of the "grounded" points at the two ends of the data link differs. This potential difference causes a current to flow into the data link, possibly exceeding the capability of the input or output components.

The user can stay with conductors for the data link or convert (or initially design) it to an optical-fiber link, an approach that is becoming increasingly popular as hardware costs fall with economies of scale. However, if the conversion electronics at the ends of the fiber link are disturbed by electrical noise, that noise will be faithfully transmitted, not blocked.

If a conductive data link is to remain, the remedy is to insert protective devices that are complementary for the power line and data line. These devices typically operate by limiting the overvoltage or attenuating the higher frequencies by filtering, which works effectively on the power line but not on the data link. Here, filtering is not possible because it would affect the signals; limiting the overvoltages will eliminate that damage risk, but might still let through a spurious signal. Thus, data integrity may be more difficult to achieve unless the software includes inherent immunity or fault tolerance.

Side effects

Avoiding damage with protective devices may then seem to require only the insertion of a power-line surge suppressor at the wall receptacle and a data-line surge suppressor at the input to the computer. This apparent simplicity, however, is deceptive because the very operation of this device, if incorrectly installed, can have a side effect that would put the data link components at risk, a mechanism that is only beginning to be fully recognized.

Still another mechanism can be demonstrated by a scenario that can occur in any building with power and telephone service. The incoming telephone line is provided with surge suppressors (carbon blocks or gas tubes) that divert surges to the nearest grounded conductor, generally a nearby water pipe. The manufacturer of the computer or modem used for the computer–telephone-line linkup may have provided a protective device within the equipment. Alternately, the surge-conscious user may have inserted a protective device in the power cord. But should a surge occur on either the data line or the power line, the corresponding protective device will dutifully divert that surge to the nearest ground. Since the "nearest ground" may not be the same for the connection of the two suppressors, the surge current in the ground connection raises the potential of one side with respect to the other, placing the data input at risk.

The solution is a miniature setup of the "ground window" concept developed by telephone companies in protecting their central station switches: all cables entering a room or a complete floor in a building are routed through a single "window" where grounding conductors, shields, and ground connections of protective devices are bonded together. In this manner, there cannot be any potential difference between the various ground reference points within the room or floor.

Some surge suppressor manufacturers have adapted that concept to a portable version of the ground window, a device consisting of a suppressor for the power line and one for the data line, but packaged in a single box most likely sharing the same ground connection. This local ground window is now found in computer or hobby stores and is easily recognizable because it features both a power connection (male plug for connection to a wall receptacle and female receptacles for powering the loads) and a pair of data link connectors (input and output). Depending on what is needed, these connectors can be a standard telephone jack, a multipin RS232, or a cable television coaxial connector. The device is then inserted near the computer, with the power cord and data link routed through its connectors.

Another protection scheme is always available: disconnect the system when not in use! In fact, some of the consumer guidance folders inserted by the utilities with their monthly bills mention that approach. That option may not be practical for commercial operations, where some link could be left connected, creating the risk of ungrounded equipment. Thus, if applied, every link to the outside world must be disconnected.

To probe further

A good source of information on the basics of lightning is the book *Understanding Lightning* by Martin A. Uman, available from Academic Press, New York, 1971. Solutions to noise problems are given a general treatment in the second edition of *Noise Reduction Techniques in Electronic Systems* by Henry W. Ott, available from John Wiley & Sons, New York, 1989. Fundamentals of surge protection techniques are treated in *Protection of Electronic Circuits from Overvoltages* by Ronald B. Standler, also available from John Wiley & Sons, 1989. Another useful reference is *Uninterruptible Power Supplies* by David C. Griffith, published by Marcel Dekker, New York, 1989.

Guidance on the nature and severity of transients (not specifications for protective devices) is given in the *IEEE Guide for Surge Voltages in Low Voltage AC Power Circuits*, American National Standards Institute, C62.41-1980, available from the IEEE Service Center, 445 Hoes Lane, Box 1331, Piscataway, N.J.; 800-678-IEEE.

A paper by François Martzloff and Thomas Gruzs titled "Power Quality Site Surveys: Facts, Fiction and Fallacies" in the November 1988 IEEE *Industry Applications Society Transactions* presents a review of recording, analyzing, and reporting transient disturbances on power lines. Another paper, "Coupling, Propagation, and Side Effects of Surges in an Industrial Wiring System," by Martzloff in the same *Transactions* is in press. The journal is available from the IEEE Service Center.

About the author

François Martzloff (F), an electronics engineer at the National Institute of Standards and Technology (NIST) in Gaithersburg, Md., is responsible for a program of power quality and surge protection. He serves as chairman of the IEEE Working Group on Surge Characterization and as Secretary of a Working Group on Electromagnetic Compatibility (on characterization of the electromagnetic environment) of the International Electrotechnical Commission, contributing to the development of related standards. Before joining NIST, he worked in corporate R&D for General Electric Co. in Schenectady, N.Y., working on transient measurements, surge protection of electronics, and application of varistors. He holds a B.S. from the Ecole Spéciale de Mécanique et d'Electricité, Paris, an M.S.E.E. from Georgia Institute of Technology, Atlanta, and an M.S. in industrial administration from Union College in Schenectady. The concepts in this article are based on his research work and troubleshooting experience, as well as years of discussion with IEEE colleagues. ◆