

INCREASING FUNCTIONAL DENSITY ACROSS VIRTUALLY ALL ELECTRONIC-OEM SEGMENTS RENDERS VALUABLE SILICON EVER MORE SUSCEPTIBLE TO EVERYDAY, REAL-WORLD HAZARDS. SIMPLE AND RELATIVELY INEXPENSIVE MEASURES CAN PROTECT YOUR PRODUCTS, YOUR COMPANY'S REPUTATION, AND, IN EXTREME CASES, YOUR CUSTOMERS.

CIRCUIT-PROTECTION methods yield more robust products

THE ELECTRONICS INDUSTRY'S evolution toward small-geometry CMOS as the dominant design medium has bolstered signal-processing and computational performance, energy efficiency, economy,

and compactness. At the same time, however, it has reduced ICs' native robustness in the face of common and unavoidable electrical transient hazards.

In broad strokes, transient sources segment into lightning, switching, EMP (electromagnetic pulse), and ESD (electrostatic discharge). Of the four, EMPs are thankfully rare, deriving most famously from nuclear events. But, like EMP, virtually all sources of electrical transients derive from a sudden release of stored energy. Lightning and ESD result from the sudden release of static charge; switching transients typically originate from the collapse of an electrostatic or electromagnetic field

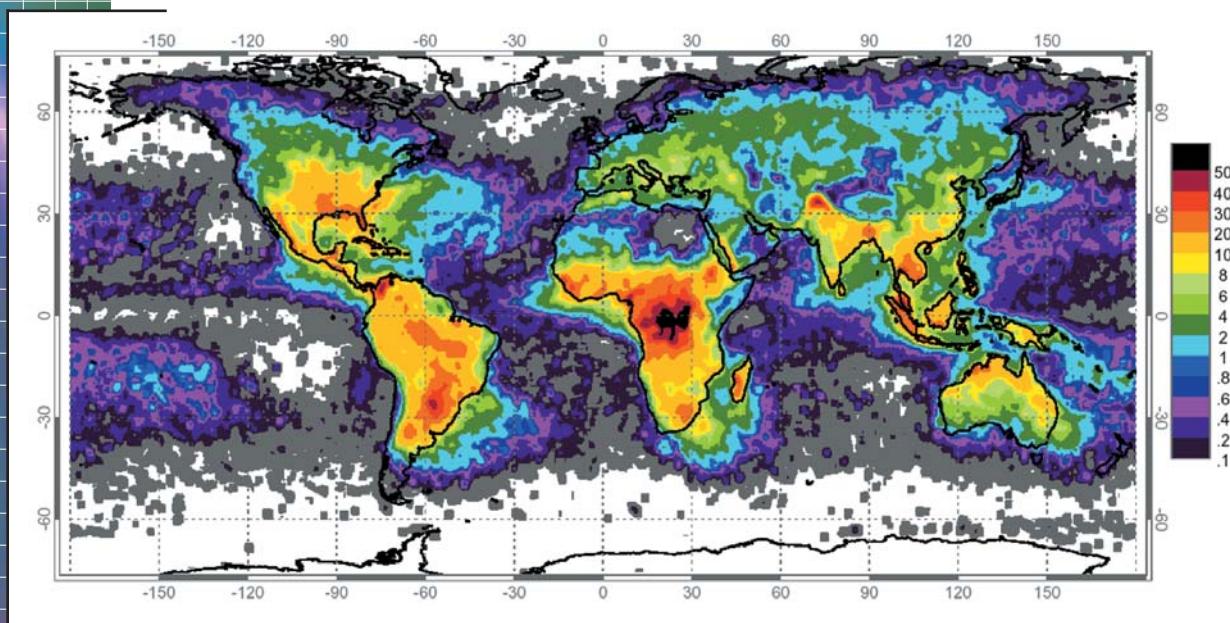


Figure 1

Data from space-based optical sensors reveal the uneven distribution of worldwide lightning strikes (courtesy NASA National Space Science and Technology Center Lightning Team).

due to a sudden change in current or voltage in the presence of explicit or parasitic reactances.

Sources within a classification tend to exhibit similar time-domain characteristics. Switching transients, for example, tend to be periodic with amplitude and repetition rates that vary by the details of an installation. Lightning and ESD strikes are aperiodic and locationally unpredictable beyond broad geographic trends (**Figure 1**). (**TechFlick:** An animated version of the map in **Figure 1** shows the combined annual strike count per square kilometer as a function of geography. See the video with the Web version of this article at www.edn.com/circuitprotection. Figure and video courtesy NASA National Space Science and Technology Center Lightning Team.)

Lightning and ESD strikes are also difficult to measure and vary over a large range of amplitudes. Various industry segments have developed and promoted a variety of source standards and test methods. Though standards can differ in important areas, such as charge storage and source impedance, for example, they tend to agree in principle on how transient hazards typically appear to otherwise-unsuspecting circuits (**Table 1**). This tabular data doesn't tell the complete story: Transient waveforms are not square but tend to exhibit fast exponential rise times, comparatively slow exponential decays, and little or no dwell times at their peak amplitude.

For any given node that is susceptible to a hazardous transient, a protection method must simultaneously meet several requirements. The method must be able to clamp the protected node to a safe potential. An appropriate protection device, therefore, varies according to the type of circuit it is protecting. The protection device must respond fast enough to the transient's rising edge to keep the node voltage below the destructive threshold. Low-inductance shunt devices and low-capacitance series elements help meet this requirement but only if the pc board's design exploits good high-speed-layout techniques for the protection network. Lastly, the protection method must either be able to ab-

AT A GLANCE

- ▶ Your product's reputation depends on its robustness.

- ▶ Compare your circuit's tolerance for leakage current and shunt capacitance before specifying a transient-protection topology.

- ▶ Compare the speed of candidate protection devices with reasonable models for the transients against which you intend to protect.

- ▶ Beware of IC manufacturers that specify transient-tolerance levels absent the source model and test method. The tolerance level alone doesn't tell you anything.

sorb the energy that a transient event delivers or cause the dissipation to occur in the transient source impedance. For this reason, OEM designers cannot always depend on the semiconductor's on-chip protection cells and often must add pc-board-level protection elements. A prudent first step in determining a protection method for a given transient type, therefore, is to calculate the total strike energy that your circuit must absorb. Also consider the likely repetition rates and thermal time constants to ensure that clamping elements don't overheat in the heat of the moment.

The most commonly susceptible nodes are a system's exposed ports. These in-

clude the power entry and signal I/Os. They can also include internal nodes that are near an insulating surface as is the case in keyboards and displays. Transients needn't originate on a particular lead to damage its associated circuitry. Transients occurring on leads connected to one subsystem can capacitively couple to leads connected to other subsystems before breakdown or can inductively couple during the current ramp that immediately follows breakdown. In such cases, protecting the primary victim may not suffice. For example, if an installation bundles signal leads with power feeds, then a power-line transient induced by, say, a motor could couple to a signal node, albeit at reduced amplitude.

High-speed circuits are challenging to protect because they can be sensitive to the additional shunt-capacitance loading that clamping schemes add to the protected node. This reason is one of several that fiber-optic feeds are attractive in high-speed communications, even for short-haul applications, such as rack-to-rack links (**references 1 and 2**).

Isolated front ends, common in industrial and medical signal-conditioning applications, block large common-mode voltages and pass the signal's differential-mode component. The common-mode component appears across the isolation barrier, which offers a finite breakdown voltage, often in the range of 500V to 2 kV. Transients that exceed the isolation barrier's breakdown voltage, such as from an ESD strike, will discharge to the

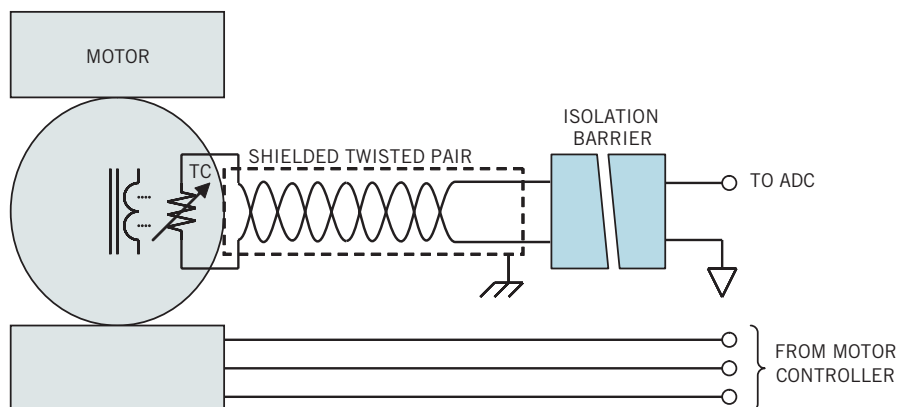
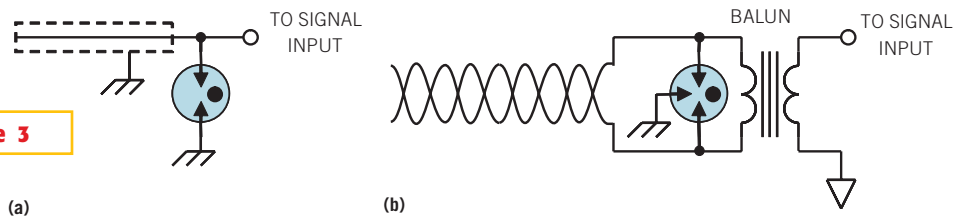


Figure 2

A thermocouple monitoring a motor's stator temperature exemplifies applications in which small signal inputs are subject to large switching transients. Galvanic isolation eliminates common-mode terms.

system-side ground through a path that the isolation barrier's design determines (Figure 2). The predictability of such a path may vary depending on the type of barrier: optical, capacitive, or magnetic.

Figure 3



Single- (a) and triple-pole (b) gas-discharge tubes protect coaxial and balanced twisted pairs.

FIGHTING FIRE WITH FIRE

In both peak voltage and peak current, lightning strikes are the largest transient sources against which you may need to protect. Even at substantial distances from the strike site, lightning-induced surges deliver substantial energy, and few protection devices can themselves survive the experience—much less perform sufficiently to protect the nodes to which they attach. Table 2 shows a further breakdown of the lightning characteristics in Table 1.

The most likely nodes to experience transients from lightning attach to power entries or to long, outdoor signaling feeds, such as in POTS (plain-old-telephone-system), DSL (digital-subscriber-line), or cable-television systems. Although POTS feeds have modest bandwidth requirements, DSL deployments are supposed to piggyback on the POTS infrastructure, so protection devices must contribute a minimum shunt capacitance, as is the case for cable TV. GDTs (gas-discharge tubes), also known as gas-plasma arrestors, are good first lines of defense for such large distributed systems.

Under normal operating conditions, the shunt impedance of a GDT is on the order of 1 TΩ in parallel with 1 pF or less. The GDT's low leakage current—typically less than 1 pA—and low capacitance vary little with applied potentials less than the gas-ionization, or “glow,” voltage. Once the tube reaches the glow voltage, the impedance drops precipitously, resulting in a current through the gas. Increasing current causes the gas mass to form a plasma, which causes the voltage across the device to drop further to the neighborhood of 15V. The plasma self-extinguishes when the source can no longer sup-

ply the plasma current. The net effect is a crowbar behavior that can limit the voltage during a transient event to the neighborhood of 15V in less than 1 μsec. One key advantage of the GDT is that it forces most of the dissipation to occur in the transient's source impedance and not in either the protective device or the protected circuitry. A combination of the signal's voltage-rise rate (dV/dt), the tube's electrode spacing, the gas type, and the gas pressure determine the actuation voltage (Reference 3). Devices can sustain currents as large as 20 kA.

GDTs are available in both single- and triple-pole forms (Figure 3). The triple-pole GDT is a deceptively simple device that maintains a differential pair's balance during those critical moments when all hell is breaking loose: Small asymmetries can allow a transient to couple preferentially to one side of a balanced feed, imposing an enormous differential signal as a result. Slight differences in the response behavior of two protection devices can also allow a destructive amplitude to appear at a system's input terminals, even when the transient event appears symmetrically on the balanced line. The triple-pole GDT provides one

differential and two shunt devices in one tube with a common gas volume. Any condition that causes conduction between a pole pair causes conduction between all three poles, because the gas' state—insulating, ionized, or plasma—determines the tube's behavior.

GET A MOV ON

MOV's (metal-oxide varistors) are non-linear voltage-variable resistors. Sintered metal oxides form a structure that models as a series pair of back-to-back zener diodes. Under normal operating conditions, MOVs exhibit a typical leakage current on the order of 10 μA and a shunt capacitance in the region of 45 pF. A voltage that increases beyond the MOV's threshold causes one of the distributed diodes to avalanche, which causes the device to clamp the protected node. Increasing current eventually causes the voltage across the device to rise—a limiting factor common with most bulk materials.

As a clamp device, an MOV largely absorbs the transient energy, as opposed to a gas-plasma device, which causes most of the dissipation to occur in the transient's source resistance and in the resistances between the transient site and the protected node. In applications, such as power, POTS, and industrial sensors, that can tolerate a MOV's leakage and shunt capacitance, MOVs provide good secondary protection from lightning-induced transients in concert with GDTs because they trigger an order of magnitude faster than do gas-plasma arrestors. Excess heating of an MOV can degrade its behavior in ways that accumulate over repeated thermal over-

TABLE 1—EXAMPLES OF TRANSIENT SOURCES AND TYPICAL MAGNITUDES

	Voltage	Current	Rise time	Duration
Lightning	25 kV	20 kA	10 μsec	1 msec
Switching	600V	500A	50 μsec	500 msec
EMP	1 kV	10A	20 nsec	1 msec
ESD	15 kV	30A	1 to 5 nsec	100 nsec

Source: Littelfuse

TABLE 2—LIGHTNING-STRIKE CHARACTERISTICS

Percent of strokes	90	50	10
Crest current (i)	2 to 8 kA	10 to 25 kA	40 to 300 kA
Rate of current rise (di/dt)	2 kA/μsec	8 kA/μsec	20 to 300 kA/μsec
Duration of single pulse	100 to 600 μsec	0.5 to 3 msec	20 to 400 msec
Total stroke duration	10 to 100 msec	100 to 300 msec	0.5 to 1.5 sec
Number of pulses per stroke	1 to 2	2 to 4	5 to 34

Source: Ezell, TF, Survey of Lightning Characteristics, SC-TM-67-630 (August 1976).

stresses. Therefore, be sure to carefully analyze the transient specification you plan to support, determine the amount of energy you require an MOV to absorb and the worst-case transient repetition rate, and conservatively specify the device.

FINGER LIGHTNING

The most common transient hazard for

OEM electronics is ESD. When designing protection schemes that prevent ESD damage, you have to address three problem areas: First, the availability of numerous standards means that multiple source models exist. You must determine early on in the design cycle which source model and test method is most relevant to your application. In the event that your IC suppliers specify their parts with other source models, you need to assess how reliably they're likely to perform to the source model and test

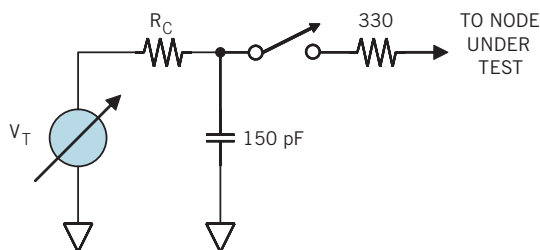


Figure 4

Testing ESD susceptibility to IEC 61000-4-2 requires a variable high-voltage source that charges a 150-pF capacitor through a large resistor, R_C . The standard allows for air-discharge and direct-contact testing. The switch allows the operator to choose the discharge mode. In either case, discharge is through a 330 Ω resistor.

method you choose. If robustness in the face of ESD is important to your customers, you may need to test working prototypes of I/O-port subsystems and elements of the human interface.

Second, modern high-speed I/O ports tolerate little ac loading without suffering substantial signal degradation, so

protective devices must add little extra shunt capacitance. Assess your application's sensitivity to additional shunt capacitance at the I/O port by considering the signal's source impedance under normal operating conditions in the context of the port's required bandwidth.

Finally, the silicon processes that have enabled high-speed I/Os exhibit low damage thresholds, so be sure that your protection method clamps fast enough and fixes the protected node to a sufficiently low voltage. Virtually all ICs have ESD-protective cells, which can substantially aid

your design. But not all vendors subscribe to the same source models and test methods, so be clear on a candidate IC's native robustness before you design it into your application. You may also want to limit a contract manufacturer's freedom to substitute ICs that attach to susceptible nodes unless the selection crite-

SAFETY FIRST

Lithium-ion chemistry represents one of the greatest advances in portable power sources since the invention of the battery. Unmatched for volumetric power density and mass, lithium-ion cell stacks power everything from digital cameras to cell phones to laptop computers. Though this battery chemistry has proved a major boon to productivity, designing these power sources into portable systems comes with a certain responsibility to ensure safe operation over the full range of anticipatable operating conditions.

The consequences that result from overcurrent conditions, including rapid self-disassembly, in lithium-ion power systems are potentially dire (**TechFlicks**: Two videos of lithium-ion batteries subjected to overcurrent conditions in a laboratory environment appear at www.edn.com/circuitprotection. Videos

courtesy Texas Instruments.)

Yet properly designed lithium-ion packs, including well-designed and -manufactured cells with adequate venting, good charge control and cutoff circuits, and good mechanical design, prevent failures of safety features that might result from mechanical shock.

Unfortunately, expensive replacement packs have inspired counterfeit-battery manufacturers that do not necessarily take the same precautions that your company does when specifying a pack design. As a result, for example, Verizon Wireless last June recalled 50,000 counterfeit LG phone batteries, and Kyocera in October recalled as many as a million counterfeit phone batteries (**references A and B**). Other incidences abound, including more than 100 that the Consumer Product Safety Commission has investigated since 2002.

Lithium-ion-pack specifiers can use several ways to protect their customers and their company's reputation. Some pack manufacturers have developed design and manufacturing standards that result in safer packs. One such manufacturer, Micro Power, has codified its design and manufacturing requirements under the name SecuraPack. SecuraPack uses premium cells from qualified vendors, sample-tests incoming cells, ultrasonically welds pack enclosures, provides component traceability, ensures design for extended-temperature ranges, and adheres to the IEEE 1625-2004 standard for rechargeable batteries for portable-computing requirements. SecuraPack also provides failure-mode and -effects analysis on the battery-system design and on the manufacturing process.

A second level of protection

is available by means of peripheral-authentication chips, such as those from Maxim's Dallas Semiconductor division and Texas Instruments. These devices allow your system to interrogate removable devices, including batteries. OEMs can still authorize aftermarket battery-pack suppliers that meet the company's safety standards.

REFERENCES

- A. "CPSC, Verizon Wireless Announce Recall of Counterfeit Cell Phone Batteries," Recall Alert, US Consumer Product Safety Commission, June 24, 2004, revised Nov 16, 2004, www.cpsc.gov/cpsc/pub/prerel/prhtml04/04559.html.
- B. "CPSC, Kyocera Wireless Corp. Announce Recall of Cell Phone Batteries," CPSC, Kyocera Wireless Corp Announce Recall of Cell Phone Batteries, Kyocera, Oct 28, 2004.

ria take matters of robustness and reliability into account.

ESD source models divide into three categories, according to the charge source: the HBM (human-body model), CDM (charged-device model), and MM (machine model). CDMs and MMs describe ESD hazards that can accrue in manufacturing environments or by allowing charge to collect on a finished product's insulating surfaces, most notably by triboelectrically displacing electrons. The HBM is the most common description for the hazards products face after their manufacture. That said, the groupings are hardly mutually exclusive, and you'll want to consider, for example, what exposure your product will have to sources and scenarios that correspond to each of the three model types. For example, the MM can also describe events in which a human charge source discharges through an intermediary conductor, as can be the case when technicians use small hand tools without first dispensing their accumulated charge to a nearby ground terminal.

Of the standards that describe HBM sources, the one the IC industry most commonly cites is IEC-64000, which includes air-discharge and direct-contact test methods. The model specifies a 150-pF charge reservoir behind a source resistance of 330Ω (Figure 4). Most ESD models include a high-impedance charge path so that the charging circuit doesn't influence the test and vice versa.

By comparison, military standard 883 uses a 100-pF charge reservoir and a 1.5-kΩ source resistance, which limits the total energy and peak current to a fraction of the amplitude IEC-

THE DIRECT-CONTACT METHOD ALLOWS YOU TO TEST SPECIFIC NODES ON A DENSE ASSEMBLY, WHEREAS THE AIR-DISCHARGE IS LESS CONTROLLABLE.

64000 allows. These two source models demonstrate that an ESD specification is uninformative if it gives only a test voltage. A manufacturer must identify the source model and test method to give you a context in which to evaluate the ESD specification. Other common ESD standards include EIAJ IC121 for MMs and US ESD DS 5.3 for CDMs (Reference 4).

Though the air-discharge test method is more familiar, as Semtech Applications Engineering Manager Bill Russell points out, "The direct-contact method is more repeatable, it models the most severe test conditions, and it represents real-world discharges. We have more [OEM] customers that use the direct-contact test method exclusively during design and don't worry about the air-discharge method than the other way around. The direct-contact method also allows you to test specific nodes on a dense assembly, whereas the air-discharge is less controllable. IEC 61000-4-2 level 4 requires contact discharges of 8 kV, but nowadays lots of manufacturers aren't stopping there: They're testing

to 10 or 12 kV, particularly in portable electronics." Though ESD voltages can be high, the total energy is fairly modest. For example, using the IEC 61000-4-2 HBM model, a 10-kV strike imparts 7.5 mJ and varies as the voltage squared.

TVSs (transient-voltage suppressors) are avalanche diodes. Traditionally a TVS's shunt capacitance was several tens of picofarads, but some current devices add less than 10 pF. Leakage currents tend to be 100 μA or more for the lowest voltage parts, but these numbers tend to fall to 5 μA or less for parts that operate at 12V or more.

The current trends in TVSs include greater integration to support dense portable devices. Multiple devices in chip-scale packages set node spacing to better match the protected IC or the interface connector. Integrated TVS and EMI filters address two critical challenges in one package and simplify your task to route buses through I/Os. Due to their compactness, multi-*TVS* packages have become the most common protection devices for dense assemblies. □

REFERENCES

1. Israelsohn, Joshua, "Fiber lights the short haul," *EDN*, March 21, 2002, pg 61, www.edn.com/article/CA200388.html.
2. Israelsohn, Joshua, "The alchemy of glass," *EDN*, Dec 26, 2002, pg 37, www.edn.com/article/CA265496.html.
3. "Surge Arrester Technologies," Application Note AN-111, SRC Devices, undated.
4. "Introduction to Circuit Protection," Littelfuse, undated.

TALK TO US

Post comments via *TalkBack* at the online version of this article at www.edn.com.



FOR MORE INFORMATION...

For more information on products such as those discussed in this article, contact any of the following manufacturers directly, and please let them know you read about their products in *EDN*.

AVX

www.avxcorp.com

Bourns

www.bourns.com

California Micro Devices

www.calmicro.com

Fuji Semiconductor

www.fujisemiconductor.com

Jensen Devices

www.jensendevices.com

Littelfuse

www.littelfuse.com

Maxim Integrated Products

www.maxim-ic.com

Micro Power

www.micro-power.com

Microsemi

www.microsemi.com

On Semiconductor

www.onsemi.com

Philips Semiconductor

www.semiconductors.philips.com

ProTek Devices

www.protekdevices.com

Raychem

www.raychem.com

Semtech

www.semtech.com

SRC Devices

www.srcdevices.com

Texas Instruments

www.ti.com

Vishay

www.vishay.com