HARDENING COMMUNICATION PORTS FOR SURVIVAL IN ELECTRICAL OVERSTRESS ENVIRONMENTS

O. Melville Clark
General Semiconductor Industries, Inc.
Tempe, Arizona

ABSTRACT

Greater attention is being focused on the protection of data I/O ports since both experience and laboratory tests have shown that components at these locations are extremely vulnerable to electrical overstress (EOS) in the form of transient voltages. Lightning and electrostatic discharge (ESD) are the major contributors to these failures; however, these losses can be prevented. Hardening against transient voltages at both the board level and system level has a proven record of improving reliability by orders of magnitude. This paper will review the EOS threats, typical failure modes and transient voltage mitigation techniques. Case histories will also be reviewed.

ORIGINS OF ELECTRICAL OVERSTRESS

Electronic systems transmit and receive vital information through sensitive communication ports. These vulnerable interfacing microcircuits are connected directly to signal lines which are often exposed to lightning to a varying degree. Electrical storms produce transient voltages on data lines which can range up to 300V or higher [1]. Failures of line drivers and line receivers occur at transient levels ranging from 40V to 90V [2], a level which is easily attained in long wire lengths which interconnect components of distributed systems.

Lightning discharges can produce high electromagnetic fields which can couple into signal lines. For example, Masters, et al, reported a voltage of 150kV induced on a 460m long open suspended wire caused by a lightning stroke 2.5km away [3]. This amounts to 325V induced for each meter of wire.

Lightning induced short circuit currents are another measure of electrical stress to which data I/O ports are subjected. After dielectric breakdown in the component, current produces excessive heat and damage. Data showing current levels induced into computer signal lines have not been reported; however peak currents induced into telephone subscriber loops have been reported by Bell Telephone Laboratories and are shown in figure 1 [4]. This graph indicates peak transient currents up to 50A can be expected on data lines with outdoor exposure.

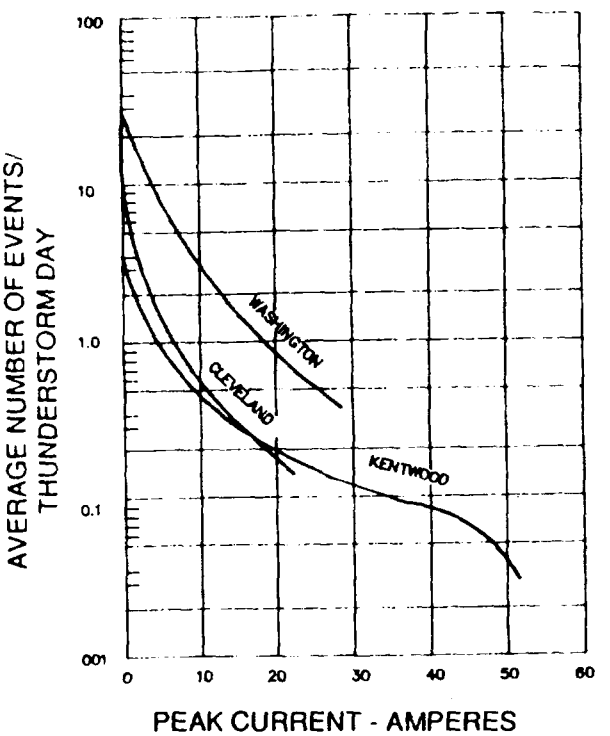

Figure 1. Peak Currents Induced Into Telephone Lines

ESD is also a major threat, producing an estimated 30% to 50% of all electronic equipment failures [5]. This is understandable, considering the low failure threshold levels of microchips reported by the Reliability Analysis Center [6]. ESD failure levels for

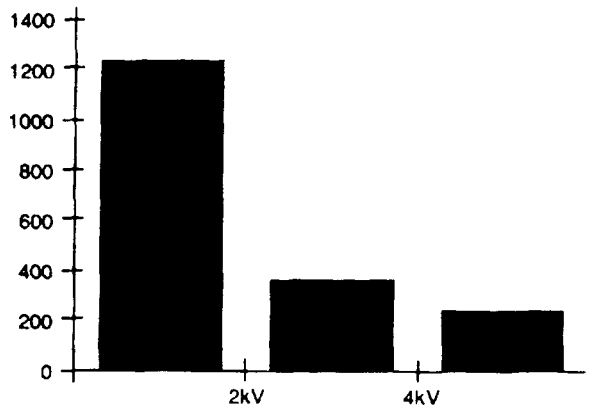

Figure 2. ESD Failure Levels For All Bipolar Devices

bipolar devices are shown in figure 2. In this graph, the vertical scale represents the number of parts which failed at a given level. CMOS structures fail at approximately the same stress levels. Since the fingertip can't feel ESD levels below 3000V, it is possible to kill a device without knowing it.

Line receivers are generally observed to have a higher failure threshold level than line drivers which can latch-up under transient conditions, subsequently producing excessive power dissipation in the device and eventual failure.

Increasing equipment losses have produced a growing sensitivity to data I/O port failures. Although industry is becoming more aware of protection needs, most computers and microprocessor based equipment in use have little or no built-in protection. Normally, only after the need has been established through excessive occurrence of field failures is corrective action taken.

TRANSIENT PATHS

Pathways to communication, or data I/O ports, are by electromagnetic coupling or direct injection into the data lines. Direct hits by lightning are rare, but injection of body generated ESD can happen while handling plugs and sockets of communication ports.

Direct strikes to buildings can also inductively coupled transient voltages into data lines from metal building framework. Since lightning typically has a current of 25kA peak, this is sufficient to produce currents of several kiloamperes through a given segment of building framework which can induce voltages into nearby conductors. In one reported case, the data port of an unprotected printer was damaged by lightning current through structural steel.

Nearby power wiring which runs parallel to data lines has been reported to cause computer system upset [7]. Radiation from the adjacent power lines, caused by load switching, can produce disturbances which corrupt data transmissions.

Transients on power lines have been reported to damage I/O ports of a printer shared with multiple PCs [8]. Failure was attributed to EOS caused by a ground loop since all components were not connected to the same ground window. Protection across the data I/O ports would have prevented this failure.

FAILURE MODES

The three basic failure modes include hard, upset and latent. Hard failures are those components which are permanently damaged and must be replaced to restore equipment to normal operation. Their appearance can be deceiving since microscopic damage cannot be seen from the exterior. An example of this type of failure is shown in figure 3. This is a transceiver chip which failed from induced lightning.

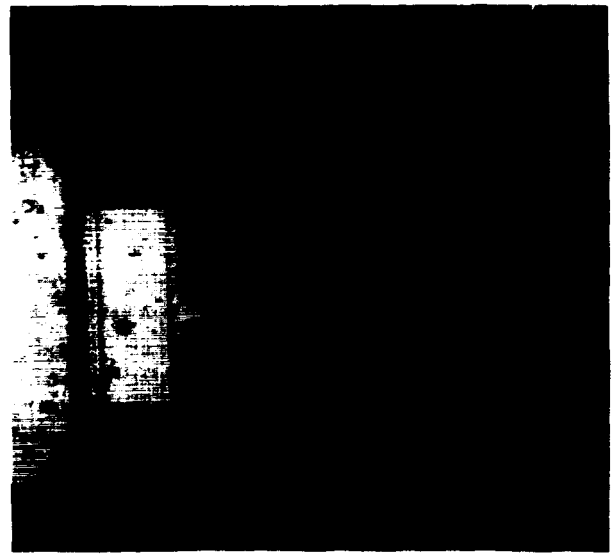

Figure 3. Failed Transceiver Chip

Line drivers which fail in a latch-up mode produce excessive heat and often results in charring of the component along with severe damage to the circuit board material. An example of latch-up failure of an RS-232 line driver is shown in figure 4. This type of failure could be a contributing factor to computer room fires which occur at the rate of 400 per year in the US [9]. Direct hits often cause components to explode or vaporize.

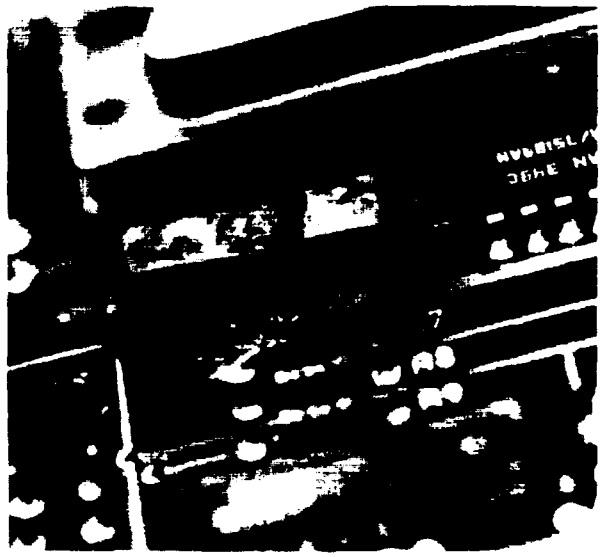

Figure 4. Line Driver Latch-Up Failure

Upset is a temporary malfunction which is usually associated with data loss or file corruption although the results may sometimes be catastrophic. In March 1987, an Atlas Centaur launch vehicle was struck, causing overwrite of the guidance control memory, resulting in destruction of the rocket and its payload [10].

Latent failures are the "walking wounded" which are zapped once but at an insufficient level to cause immediate failure but still causing degradation of the part without noticeable loss of performance. These devices eventually fail but some have survived up to a period of five years [11].

PROTECTIVE DEVICES

Transient voltage suppressor (TVS) devices protect data I/O ports by limiting voltage spikes to levels safely below component destruct thresholds. Suppressor devices also divert unwanted currents away from the protected components and in the process consume part of the transient energy. A properly selected TVS protects by limiting voltage spikes but does not interfere with circuit performance.

The three most commonly used TVS devices include gas discharge tubes, metal oxide varistors (MOVs) and silicon TVSs. For some telephone applications, the use of bilateral voltage triggered thyristors is growing.

Gas discharge tubes are characterized by multikiloampere capability. Impulse firing voltages usually start at 500V which is too high for microchip protection but adequate for nonsensitive circuits. Gas tubes are best suited for and frequently used in multistage protectors which are discussed later.

Metal oxide varistors (MOVs) are voltage dependent nonlinear resistors composed of zinc oxide granules in a matrix of bismuth oxide and other metal oxides. These devices are bilateral and electrically resemble two zener diodes back-to-back. Advantages of MOVs are low cost and high current handling on a limited basis. Their main disadvantage is high clamping voltage when compared to silicon TVS devices. MOVs are best suited for protection across ac power lines.

Silicon TVS devices use large area pn junctions mounted between metal heat sinks to dissipate the heat produced during suppressive action. These components are rated lower in peak current than gas tubes or MOVs; however, they consistently perform at rated levels with virtually no wearout. Silicon TVSs clamp at predictably lower levels than other TVS devices making them ideal for protecting sensitive microchips.

A comparison of clamping ability of both MOV and silicon TVS devices is illustrated in figure 5. Both parts were comparably rated for operating voltage and pulse current rating. Each device was surged with a 1.2/50us transient voltage spike (1.2us rise, 50us for decay to one-half peak value). Peak open circuit voltage is 1500V and peak current is 50A through each device. In this graph, the vertical scale is 5V per division and the horizontal scale is 10us per division.

Clamping under transient conditions is a qualitative measure of protective capability. Note that the MOV clamps at 19V but the silicon suppressor protects at a much lower level of 7V.

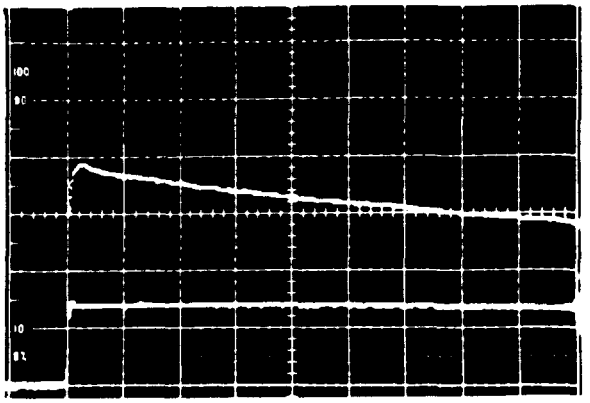

Figure 5. MOV and Silicon TVS Clamping

Some data/communication interfaces are interconnected with lines of one kilometer or more in length, which are exposed to harsh lightning environments. Protectors for these applications are usually multistage, using an up-front high current rated TVS such as a gas discharge tube. A low clamping voltage device such as a silicon TVS is often used in the second stage with an intervening impedance to develop sufficient voltage to fire the gas discharge tube. The topology for this circuit is shown in figure 6.

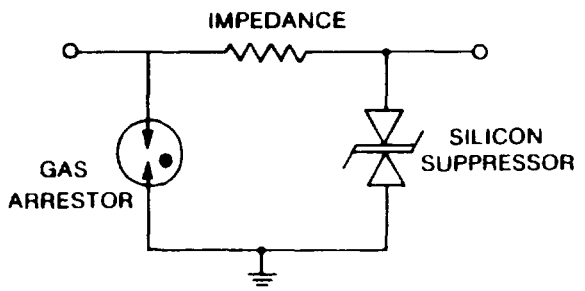

Figure 6. Multistage Suppressor Topology

Typical performance for an RS-232 signal transient voltage surge suppressor (TVSS) using a multistage suppressor containing an up-front gas tube followed by a silicon TVS is shown in figure 7. This illustrates the transient voltage reduction from 1500V down to an acceptable level below 40V, which is the failure threshold for these communication interfaces. The scale is 10V per division vertically and 5us per division horizontally.

During the first 37us of suppressor conduction, normal data flow is lost. The software should recognize this condition and ask for a retransmission.

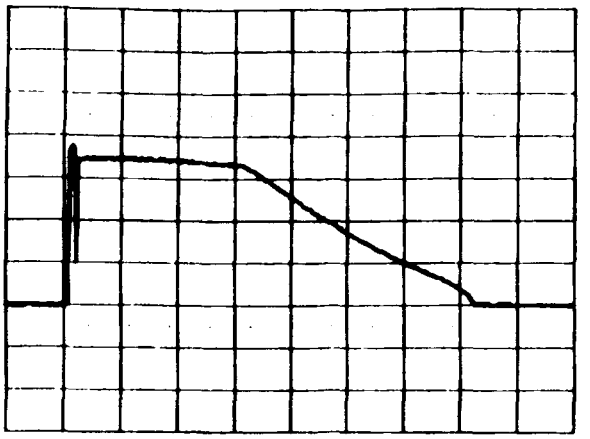

Figure 7. Multistage Suppressor Performance

GUIDELINES FOR TVS SELECTION

The main electrical parameters to be considered in selecting a TVS for I/O port protection are:

1. Maximum operating voltage (Vr)
2. Maximum clamping voltage (Vc)
3. Peak pulse current capability (Ipp)

The maximum operating voltage is the peak voltage, including high side of the tolerance, at which a device is designed to operate without drawing appreciable current. This level is typically ten percent below the minimum breakdown voltage, that voltage at which the device begins to conduct current.

Maximum clamping voltage is the highest voltage that will appear across the protected component under conditions of maximum rated peak pulse current. This is the protection level that is provided to the I/O port across which the device is connected.

Devices are available as unidirectional, for dc line protection and also as bidirectional for ac and other positive and negative going signals. Most data I/O ports use bidirectional devices. For high data transmission rates, the inherent capacitance in low voltage, large area silicon TVS may significantly attenuate signals. Specialized low capacitance TVSs are available for these applications.

These general guidelines for TVS selection apply for both board level and system level protection applications which are described in the following paragraphs.

BOARD LEVEL PROTECTION

Discrete components are available, with operating voltage levels over the range of 5V through 25V which includes most signal lines. These are also available for the higher voltage commercial telecom voltages.

Both through-hole axial lead and surface mount devices are available as industry standard components. Some devices are supplied as multiple components in 8 pin and 16 pin industry standard DIP packages for applications where space is limited.

Silicon TVSs are rated in terms of peak power capability, which is associated with the cross sectional area of the suppression element. The types normally used on PC boards for data I/O port protection are the 500W and 600W rated types. For example, an SMBG24CA surface mount silicon TVS would be a good selection for protecting RS-232 I/O ports as this device operates at +/- 25V and can handle pulse currents of 75A for 8/20us waveforms.

Placement of the protector is extremely important for optimum protection. The shunt current path through the protection circuit must be minimum for optimum protector performance [12]. Parasitic inductance in the suppressor leads contributes to L(di/dt) effects which can be significant for fast rise-time transients originating from ESD and NEMP.

The protector should be placed as close as possible to the signal input terminations on the board to minimize radiation into other components on the board. The ground reference should likewise furnish a low impedance path between all suppressors as illustrated in figure 8.

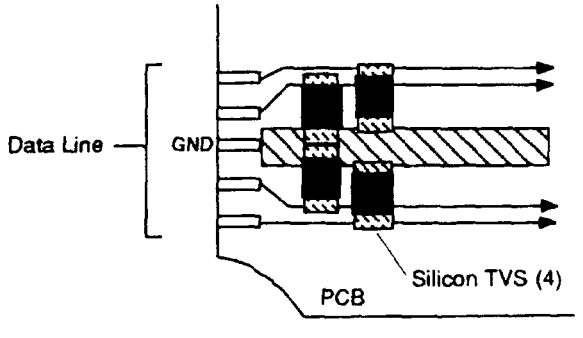

Figure 8. On-Board Suppressor Installation

A well designed protection scheme should protect I/O ports from body generated ESD and induced lighting into a system which is all contained within the same building structure. For distributed systems, which includes interconnected equipment in several separate buildings, additional higher current protection is required as described in the following section.

SYSTEM LEVEL PROTECTION

Networked and distributed systems usually have long interconnecting lines between equipment locations, often between several buildings. High voltage spikes produced by harsh lightning exposure should be suppressed at the point the signal lines enter the building as shown in figure 9. For these applications, multistage protectors, often called transient voltage surge suppressors (TVSSs) are required to handle these high current threats.

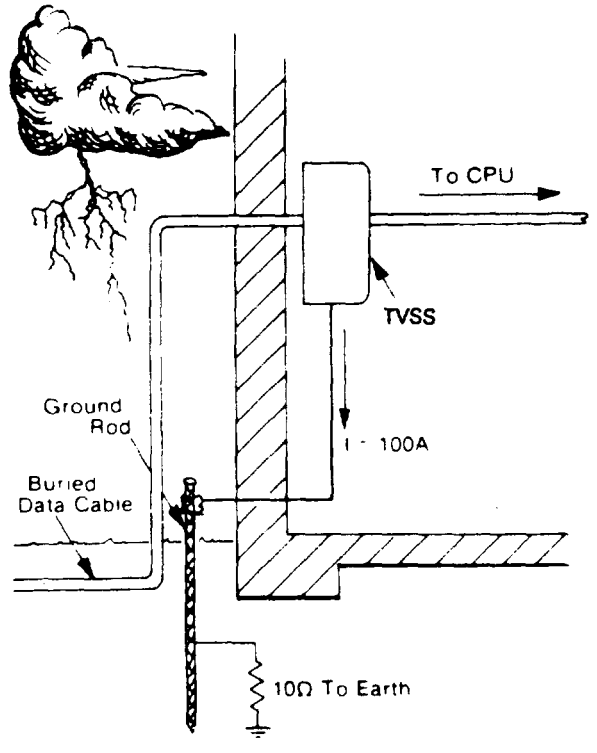

Figure 9. Transient Voltage Surge Protector for Signal Lines

If the TVSS is connected to a separate ground from the system, a common mode transient voltage will develop from current flowing through the ground resistance. This can be illustrated by a current of

100A flowing through a ground resistance of 10 Ohms producing a rise in voltage of 1000V above the user equipment frame ground. This is calculated using Ohms law as shown below:

$V = iR$

Where:

i = instantaneous peak current of 100A
R = Resistance of 100 Ohms

Then:

$V = 100A \times 10\Omega$
$V = 1000V$

Without additional secondary protection at the equipment inputs to reduce the 1000V to a safe level of 40V or less, the communication interface chips will be destroyed.

The best alternative approach to high level surge protection is to have the TVSS ground connected through a short, low impedance bond to the frame ground of the user equipment. Then the entire system rides up in potential with ground current and the system is safe because it is all at the same potential. An illustration of this system is shown in figure 10.

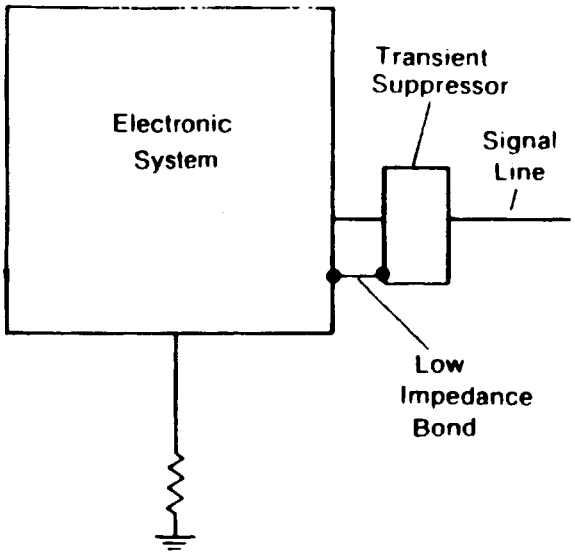

Figure 10. Low Impedance Bond

When the TVSS is located close to the equipment and some distance from the building wall, it is usually necessary to shield with metal conduit those data lines running from outside of the building. Otherwise, transients will be radiated inside the building and possibly coupled into other lines, increasing the risk factor for normally reliable equipment. For redundant high speed data lines, i.e., 1 MB and up, experience has shown that best performance is achieved with protectors attached directly to equipment frame ground.

Locating the position of the protector a significant distance from the user equipment can build up high voltages across the ground wire as shown in figure 11. Wires connecting protector grounds to frame grounds should not exceed 2 feet [13]. The self inductance of a straight wire is only 1.2uH/m, but this can result in high impedance of ground wires during high current fast rise-time transients. This develops high common mode voltages on the data lines similar to the condition previously described for high ground resistance paths.

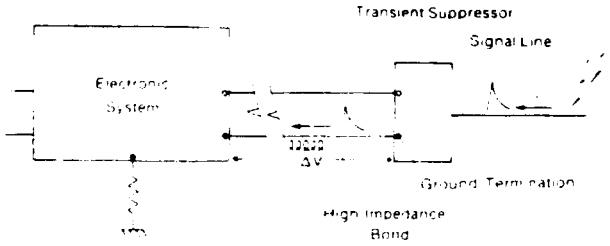

Figure 11. High Impedance Bond

For example, a potential of 3600V resulting from L(di/dt) effects will be developed across a 6m long straight wire carrying a transient current of 500A rising to peak in 1us.

Protection from infrequent strikes to buildings or near lightning hits is recommended for communication interfaces where indoor runs are longer than 10m. Although it rarely happens, all I/O ports in a single system have been destroyed by a single, nearby strike.

If protection is not built-in, it can be provided with add-on TVSSs which are readily available for RS-232 data systems using 25 pin "D" connectors. These add-on protectors are normally connected directly to the computer/peripheral at the I/O port.

Some TVSSs on the market combine protection for both the signal and power lines within the same enclosure. The advantage to this configuration is that the ground window, or ground potential reference, is common for both power and data which optimizes transient protection.

INSTALLATION PRECAUTIONS

Transient disturbances on ground and protector input wires produce radiating electromagnetic fields which are induced into nearby wiring and equipment. The results can cause upset or permanent damage. For this reason a few basic precautions must be taken during installation and routine maintenance of equipment.

Configure the wiring so that the protector output ("clean wires"), are routed away from the input and ground wires which carry the transient current. Surge currents flowing through input and ground wires will couple into the protector output if they are installed close and parallel to each other. Run them at right angles to minimize coupling. Also, keep noisy power lines away from data lines.

CASE HISTORIES

I. A manufacturer of high-end laser printers was having an unacceptable level of field failures which were traced to human body ESD events injected into RS-422 data I/O ports. Installing 500W rated silicon TVS devices at the board level provided the needed protection and eliminated the ESD caused failures

II. A supplier of petrochemical tank level gauging systems was losing line drivers to lightning caused transient voltages. The transient caused latch-up and subsequent overheating which resulted in severe damage to the board. Adding on-board protection plus TVSS protectors for severe environments boosted reliability by orders of magnitude by virtually eliminating losses which normally occurred during electrical storms.

III. A high volume supplier of raw materials to the plastics industry converted its facility to total computer operation incorporating extensive use of TVSS protective devices to ward against induced lightning failure. A successful changeover was made during the winter months; however, when electrical storms began in late spring, equipment outages occurred.
System failures were attributed to improper routing of the data lines at the TVSS location. The protectors were installed with both field input wiring and the "clean" outputs to the computer in the same raceway for lengths of up to 8 feet. This allowed transients to couple into the TVSS outputs and subsequently to the computer I/O ports. Separating the input and ground transient conducting wires from the outputs eliminated this problem.

CONCLUSION

Signal I/O ports are easily destroyed by transient voltage spikes because of the inherently small geometries of microchips. Latch-up is also caused by voltage spikes resulting in damage and potential fire hazards. The major causes of this destructive electrical overstress are ESD and induced lightning; however, properly selected and installed protectors can virtually eliminate I/O port failures.

A broad range of off-the-shelf TVS protective components are available for board level protection while add-on TVSS assemblies can be installed by the user on unprotected ports. Depending on design and installation, some TVSS surge protectors can handle currents of more than 1 kiloamp on data lines exposed to harsh lightning conditions.

Location and installation of adequately rated protective devices must be optimum to provide effective system reliability under adverse transient voltage conditions.

REFERENCES

[1] M. Tetreault and F. Martzloff, "Characterization of Disturbing Waveforms on Computer Data Lines", Proceedings of Electromagnetic Compatibility, Zurich, March 1985, p. 426.

[2] M. Tetreault and F. Martzloff, p. 425.

[3] M. J. Master, et al, "Voltages Induced on an Overhead Line by the Lightning Stepped Leader", IEEE Transactions on EMC, Vol EMC-28, No. 3, August, 1986, pp. 168-171.

[4] "Bell Telephone Laboratory Journal", No. TR-EOP-000001, Issue 2, 1987 p. 9.

[5] M. Clarke, "DOD Raises Stakes in On-Chip ESD Tolerance", EDN, August 24, 1989, p. 70.

[6] W. Crowell, Electrostatic Discharge Susceptibility Data, VZAP-90, Reliability Analysis Center, Prepared under contract to Rome Air Development Center, 1990, p. 2-5.

[7] I. Hertzoff, "Electricians: a Net's Nemisis?",

Network World, November 5, 1990.

[8] F. Martzloff, "Coupling, Propagation and Side Effects of Surges in an Industrial Building Wiring System", IEEE/IAS Conference Proceedings, October 1988, pp. 1467.

[9] R. E. MacArthur, et al, "Fire Stats: Are EDP and Telecom Equipment Really Hazards?", Compliance Engineering, Vol. VII, Issue 4, Summer 1990, p. 36.

[10] R. J. Hanson, "Conducted Electromagnetic Transient-Induced Upset Mechanisms: Microprocessor and Subsystem Level Effects", Proceedings of EOS/ESD Symposium, EOS-9, 1987 p. 104.

[11] P. Gammill and J. Soden, "Latent Failures Due to Electrostatic Discharge in CMOS Integrated Circuits", Proceedings of EOS/ESD Symposium, EOS-8, 1986, pp. 78-79.

[12] O. M. Clark and J. J. Pizzicaroli, "Effect of Lead Wire Lengths on Protector Clamping Voltages", FAA/FIT Workshop on Grounding and Lightning Technology, Report No. FAA-RD-79-6, March 1979, p. 72.

[13] W. Lewis, Reported in Presentation at University of Wisconsin Program on Surge and Transient Immunity in Computer Systems, 1987.