# Data Line Transient Protection

## White Paper 85

Revision 1

by Joseph Seymour


## > Executive summary

Electrical transients (surges) on data lines can destroy computing equipment both in the business and home office environments. Many users appreciate the risk of power surges but overlook data line surges. This white paper explains how transients are created, how they can have devastating effects on electrical equipment, and how surge suppression devices work to help protect against them.


## Contents

*Click on a section to jump to it*



APC white papers are now part of the Schneider Electric white paper library produced by Schneider Electric's **Data Center Science Center**
DCSC@Schneider-Electric.com

Schneider Electric

## Introduction

Electrical disturbances pose a great threat to electrical equipment and data. Electrical disturbances go by various names such as spikes, surges, and transient surge voltages. Regardless of the name, the effects of these disturbances remain the same: disruption, degradation and damage, which inevitably mean equipment downtime. With the increasing popularity of computer networking, the effect of transient surges on communication lines is also of great importance. Communication lines entering a building, whether below or aboveground, can transfer large transients into a home or business facility. Created through various kinds of coupling (transmission of electrical energy from one system to another through magnetic fields), transient surges may cause serious damage to communication interfaces inside a building. Due to the many ways a transient surge may be created, a single surge suppression layer applied to incoming lines may not be appropriate to completely shield the internal lines and equipment from transient voltages.

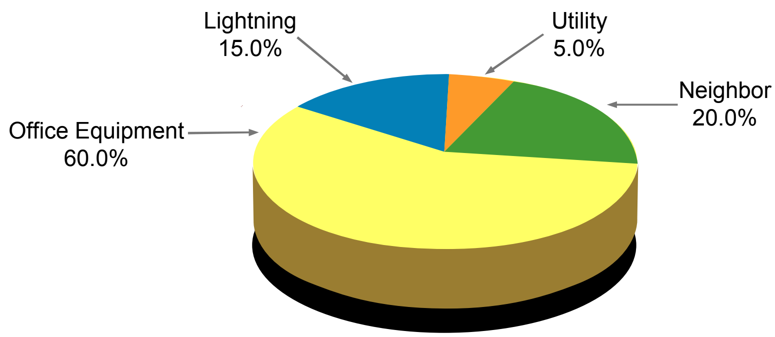
When discussing the specific effects that a transient surge can have on data lines, it is important to understand in general terms what data lines are and how the carry data in the form of electricity. A data line is a conductive communication cable that carries low level voltages for the purpose of communication between attached devices. Some common examples of data cables are coax, CAT5 Ethernet cable, and telephone cable. Data is transferred from one piece of equipment to another by sending varying voltage levels from transmitting equipment across data lines to the receiving equipment on the other end of the cable. The receiving equipment processes the voltage levels, interpreting and translating them into data that it understands and follows.

Even though data lines have a tendency to carry only low voltage levels, they are made of a conductive material and are subject to the same transient surges and spikes that other conductive lines may experience. In general, a transient surge is a short-term deviation from a desired voltage level (or signal in the case of computers and electronic devices). This undesirable deviation can cause an electronic device to malfunction or even fail. Some equipment used to communicate over data lines is only designed to function within a very low threshold of voltage, and can easily be damaged if voltage levels rise above what is desirable. Furthermore, transient voltage surges are created from a variety of sources, which means no configuration of equipment is free from transients.

**Figure 1** illustrates the results of a study produced by Florida Power that separates power quality problems into various groups. The chart shows that lightning attributes 15% of power quality issues, utility sub-stations introducing transients through grid switching attributes only 5%, and that transients generated by office equipment accounts for 60% of all power quality problems.

**Figure 1**

*Florida Power study of the breakdown of power quality problems in the business place*



## How transients are created

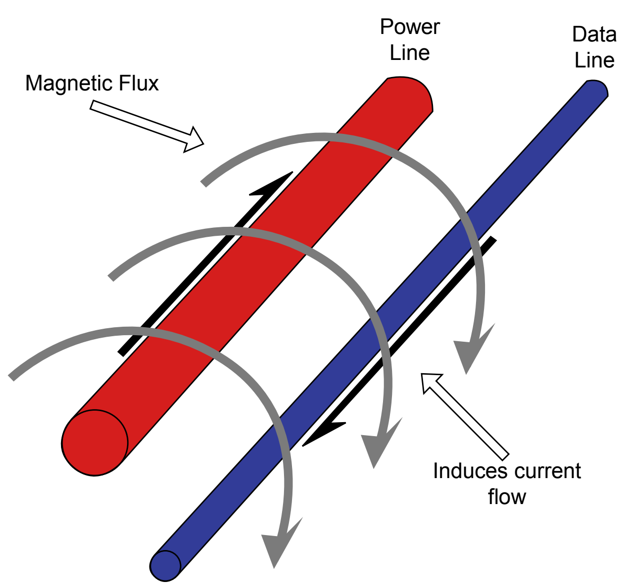
Transients can be present on any conductor such as utility power lines, telephone, data, and signal lines. The types of data lines that exist on many Local Area Networks (LANs) include RS-232, RS-422, Ethernet and Token Ring Cable, closed-circuit TV, surveillance alarm systems, and CNC/machine-tool interfaces.

Spikes, a type of transient surge, are short-term over-voltages, which are usually measured in milliseconds. This unwanted excess of electrical energy could be created easily on any conductive line. The energy content of transients can be enormous and can damage equipment, or cause it to malfunction by giving faulty signals due to inaccurate voltage levels. Equipment driven by microprocessors and other integrated circuits (IC) are especially vulnerable to transient voltage surges. Inductive coupling, created from various sources, is usually the cause for transients specific to data lines.

Lesser known than how direct AC power transients are created, is how inductive coupling transients are produced on data lines. Whenever electric current flows through a conductive material, a magnetic field is created. If a second conductor is placed within the magnetic field of the first conductor, and the magnetic field is in a state of flux, then the magnetic field will induce a current on the second conductor. The use of a magnetic field to create current and induce voltage, without actually connecting physically to the other conductive material, is the basis for transformer operation such as the ones used for utility power lines. A transformer produces a magnetic field extending from a coiled wire in the primary, which induces a voltage in the coiled wire of the secondary. Under the same principles, wires that run adjacent to one another within a building can magnetically couple transients, as shown in **Figure 2**. This coupling can be caused by a power line, which induces a voltage in an adjacent data line, or from one data line to another (which is usually referred to as crosstalk).

**Figure 2**

*Inductive coupling*




Lightning can cause a much more powerful kind of magnetic coupling, which can cause sudden damages to multiple items in a single strike. **Figure 3** shows a lightning bolt striking the ground. This lightning bolt is surrounded by a very powerful magnetic field. In much the same way a magnetic field from one conductor can induce transients on an adjacent conductor, the magnetic field of a lightning strike can induce power in an external power line without actually striking the line directly. More importantly, if a lightning strike is close enough to a facility it can induce transients on internal data lines that its magnetic field cuts across. These transients can confuse data being transferred over these lines or likely cause damage to attached equipment. Another term used to describe inductive coupling is Electromagnetic Interference (EMI) or noise.

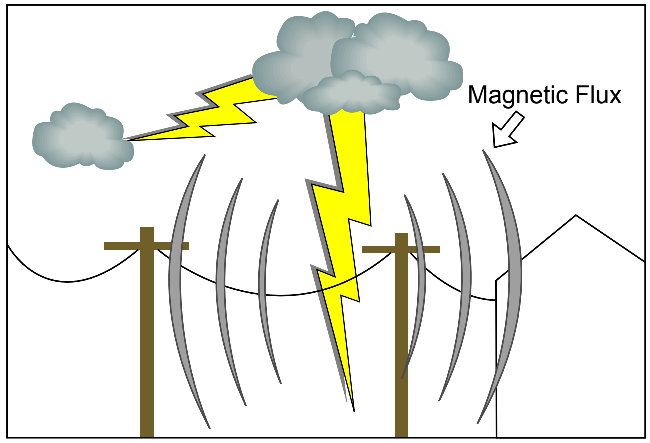



**Figure 3**

*Magnetic field created from a lightning strike*

While coupling occurring between wires and from lightning strikes are two of the better-known sources of data line transients, there are other major sources of coupling that can be detrimental to data infrastructure within a facility. When planning or inspecting the layout of data lines in a facility, the following sources of inductive coupling should be addressed:

- Data lines that are draped over power conduits
- Running data cables near lightning downconductor (downconductors are lines or structures in a building designed to convey lighting discharge current in a building to ground)
- Running data cables near building steel (especially in the vicinity of lightning downconductors)
- Running data lines too close to fluorescent lighting (which emit EMI)

These are some of the major sources of inductive coupling in data lines, but many more sources may exist in any given facility.

## Effects of transients

Much of the electrical equipment seen today in facilities and in some homes is built on integrated circuit and microprocessor technology. Because of certain characteristics common to integrated circuits and microprocessors, this equipment is especially sensitive to transient voltage surges. Microprocessor based and controlled devices can be found in almost every setting. Some of this electronic equipment includes computers and their peripherals, computer and data networks (such as LANs), telecommunications equipment, medical diagnostic equipment, CNC production machinery, radio equipment, televisions, satellite television equipment, electronic cash registers, copy machines, fax machines, etc. Much of this equipment is also commonly found connected to some form of data line for communication purposes.

The three factors which contribute to transient sensitivity of IC (integrated circuit) based machines are:

1. The spacing of IC and circuit board traces
2. The applied operating voltage limit
3. The use of a clock cycle to synchronize certain operations (such as in computers).

## The spacing of IC and circuit board traces

The first common factor to contribute to IC based equipment's sensitivity to transients is that the spacing between components of an integrated circuit and circuit board traces is extremely small. In many cases the spacing is much less than the thickness of a human hair. Power is passed through a circuit board using conductive tracks or traces. These traces, internal and external to an IC and on the circuit board itself, have a certain threshold for expansion and contraction. Heat created by the flow of power through the circuit boards components causes some expansion, and the lack of this flow then causes contraction. If a transient enters these traces it may cause them to become overheated, causing microscopic fractures in the circuit board structure, which can cause the normally isolated traces to cross. This creates internal shorts that could make the device inoperable. In some cases these microscopic fractures do not do any immediate damage, but slowly increase in size due to common expansion and contraction of the components, or produce more fractures, which will cause the device to slowly fail over time until inoperable.

## The applied operating voltage limit

The second factor to contribute to IC sensitivity is the gradual decrease in operating voltage that IC devices need to operate. As computer components were reduced in size and made more efficient, and in an effort to conserve power, the operating voltage needed to run these components has gradually been reduced. A common operating voltage of 5VDC for some internal computer devices has been reduced to 3.3VDC and may continue to decrease. This means the threshold of what voltage an IC based system can handle has also been reduced. If a transient were to increase the voltage level to 5VDC in a 3.3VDC based system, it could easily cause damage.

## The use of a clock cycle

The third factor for sensitivity in IC based devices is the use of a clock cycle to synchronize internal component operations. Most computer operations are synchronized around a clock cycle, which is based on a voltage that is running at a particular frequency. EMI can sometimes imitate a computers clock cycle at given frequencies, which will cause the computer to interpret these fake clock cycles as commands. These false commands can cause many logic errors that may manifest as a keyboard lockup, crashed programs, or system lockup. Inversely, EMI may cause the computer to miss certain valid commands, which may also lead to similar problems.

## Common failures produced by transients

The most common failures produced by transients within electronic devices are disruptive, dissipative, and destructive.

**DISRUPTIVE EFFECTS** — are usually encountered when a transient enters the equipment by inductive coupling (either over data or power lines). The electronic components then try to process the transient as a valid logic command. The result is system lock-up, malfunctions, erroneous output, lost or corrupted files, and a variety of other undesirable effects.

**DISSIPATIVE EFFECTS** — are associated with repeated stresses to IC components. The materials used to fabricate ICs can withstand a certain number of repeated energy level surges, but not for an extended period. Long-term degradation will eventually cause the components to be rendered inoperable.

**DESTRUCTIVE EFFECTS** — include all conditions where transients with high levels of energy cause equipment to fail immediately. Often, there is physical damage apparent, like burnt and/or cracked PC boards and components, melting of electronic components, or other obvious indications.

## Transient suppression and protection

A transient voltage surge is a short, often large, change from a desired voltage or signal. The greater the magnitude of a transient is, the greater the chance of it disrupting or damaging electronic equipment. As mentioned previously, transients can occur on any conductive material, so they affect not only devices connected to utility power lines, but also devices attached to telephone lines, Ethernet cables, coax cables, serial communication cables, etc.

### Surge protective devices

A Surge Protective Device, or SPD, attenuates the magnitude of these surges to protect equipment against their damaging effects. But an SPD doesn't necessarily reduce the surge to zero amplitude. The SPD simply reduces the transient to a level that can safely be passed through to the attached electrical load. This is because the threshold for power can vary in a device and attenuating the voltage to zero would be impractical for continuous operation of the attached equipment. Instead the SPD will attenuate the transient to a reasonable level given the equipment that it is designed to protect. Some higher-end SPDs also provide noise filtering to reduce any inconsistencies caused by EMI in the power waveform so that it is not passed to the attached equipment.

In the simplest terms, SPDs prevent damaging transient voltage surge levels from reaching the devices they protect. SPDs accomplish this task by either absorbing the excess voltage, diverting it, or a combination of the two. **Figure 4** shows an arrow being fired into a straw target. The straw target represents the SPD and the arrow is the transient voltage spike. When the arrow impacts with the target it is absorbed and sticks in the target. However, it is the thickness of the target that will determine if the arrow is stopped without coming through the other side. Also, the arrow will always damage the target in this scenario and the target may not work as well to stop the arrow in the future. Now imagine a metal shield in front of the target. When the arrow is fired, it will strike the shield and ricochet harmlessly to the side of the target. This is the basic operation of most SPDs. SPDs either absorb the energy and, (depending on how well they are made, could prevent the surge, but will still sustain damage), or shunt the voltage to the facilities ground wire. In most cases SPDs use a combination of devices for absorbing and shunting transient surges.

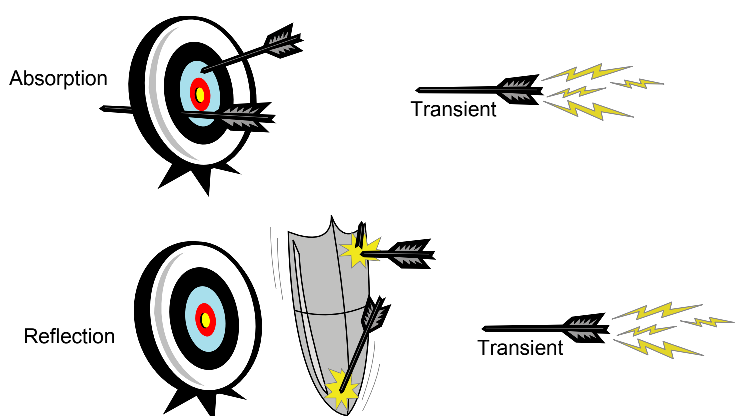



**Figure 4**

*Absorbing and reflecting transients*

Clamping is a function that SPDs use to limit transient voltages. Clamping is the process by which internal components of an SPD reduce transients to a lower voltage level that is acceptable to the attached electrical equipment being protected. The energy passed to the attached electrical equipment, after passing through the transient surge attenuation of an SPD, is referred to as let-through voltage. Again, with most SPDs, this process does not lower the transient voltage to zero volts, or below levels needed for the attached load to function. Attenuating transients excessively below needed levels can cause unnecessary strain on the SPD itself.

One of the most commonly used components used in SPDs are Metal Oxide Varistors (MOV). A MOV is a non-linear resistor with particular semi-conductive properties. The MOV will remain in a nonconductive state, allowing power to pass normally, until a transient surge enters the line. At this point the MOV begins to conduct, passing excess voltage to ground. As the amperage level increases so does the amount of clamping voltage, which keeps the let-through voltage passed to the equipment at acceptable levels until the transient surge subsides.

MOVs are often combined with thermal fuses that are placed inline with the path of power to the protected equipment to cut power to the attached equipment in the event of a catastrophic transient surge. If a transient is large, and constant enough, it may reach the peak operating voltage of the MOV at which point the MOV would vent open. If this failure occurs, the heat would cause the thermal fuse, which is often close or attached to the MOV, to break the flow of power and prevent any further power from being passed to the protected equipment. MOVs are used in SPDs because of there consistent nature. A MOV will continue to let-through the same amount of voltage, and will begin to conduct at the same level of excess voltage, consistently until its point of failure is reached.

SPDs do not solve every power quality problem. They cannot cure sags (under-voltages) and swells (long term over-voltages) in the AC power provided by electrical utilities. They also cannot reduce the harmonic conditions produced by non-linear loads like motors and switching-mode power supplies within computers and some fluorescent lighting systems. If there is a loss of utility line voltage, a device such as a UPS can be used, which has a battery to temporarily provide power until utility power is restored.

## Grounding

One of the largest power environment issues, especially in reference to SPDs, is grounding. Grounds are a necessary element of any power, signal, or data network. All voltages and signal levels are referenced to ground. Most SPDs also use grounding lines in a facility to shunt excess voltage during transient events. Without proper grounding, these SPDs may not be able to function properly.

Ground connections within a facility should only be connected to a single tie point located at the electrical service entrance panel. This single-point connection to earth ground precludes the inadvertent development of multiple ground points. Multiple ground points can create differences in utility voltage, causing undesired currents to flow on low voltage data lines. These unwanted currents flow in the less damaging forms such as noise that contaminates the transmission of data, or as larger transient surges that can damage the equipment the transmitting lines. **Figure 5** illustrates an example of a ground loop. Each piece of equipment has an independent earth ground (each power receptacle references a different ground). A problem can occur if the equipment is linked through some kind of grounded (and conductive) data line. In **Figure 5** the computer is linked to a printer using a parallel communication cable. If there is a potential difference between the grounds (difference in charge) of the equipment used, then current may flow from one device to the next through the parallel cable to attempt to equalize the charge. This is referred to as a “ground loop” and can cause significant damage to the equipment, which, in normal operation, uses a small threshold of power to function. While this example shows one facility, ground loops can also develop between multiple facilities.

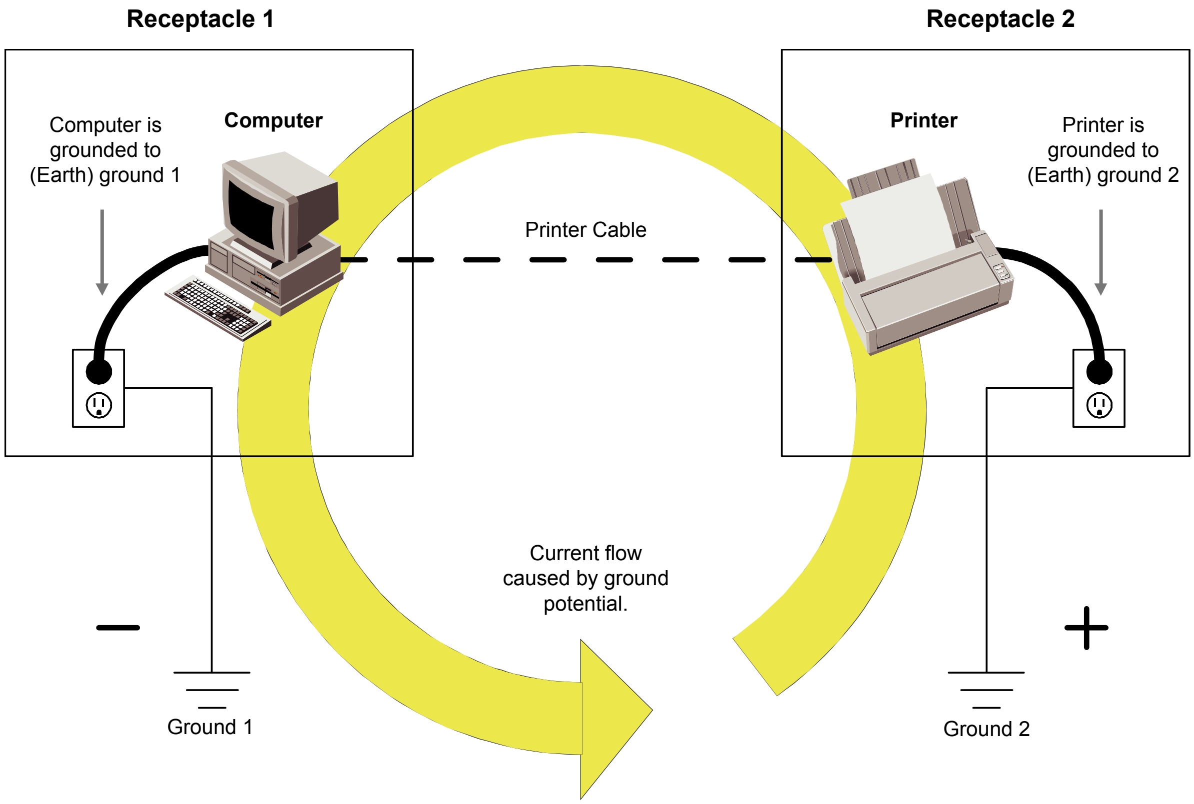



**Figure 5**

*Ground loop*

## A layered approach to transient protection

It is advisable to apply a network of SPDs to provide a layered defense against transients. A first layer would be used to control large incoming surges to a facility, such as transients on the power lines. These may be caused by lightning strikes. Other layers would then be used to control internal power and data line transients. Since the majority of transient voltage surges are generated inside a building, understanding and applying SPDs is imperative for improving the power quality in any facility.

This layered approach is the most effective means for preventing the ill effects of most transient problems. While it is important to isolate power line transient problems in this manner, it is equally important to follow this approach for data lines as well. Most large facilities have some form of first-line defense against large transients on incoming data lines. For example, many homes and facilities use a gas tube or spark gap SPD (often provided by the telephone company) to help reduce large capacity surges to a reasonable level for basic phone equipment (such a stand-alone phone that does not need auxiliary power to function). However, the let-through voltage of these first layer SPDs often do not attenuate the voltage to a safe enough level to prevent it from damaging sensitive electronic equipment such as a computer's DSL or dial-up modem (or even the computer attached to these modems). This also applies to other sensitive electronic equipment attached to coax lines such as audio/video equipment, or broadband cable modem equipment. For this reason additional SPDs should be used to protect individual devices by further attenuating the let-through voltage that is passed from the first layer of SPDs.

## Conclusion

If transient surges are addressed, it is usually in the area of power line disturbances. However, given the percentage of transients created internal to a facility within its data line network it is imperative to evaluate the need for data line surge suppression. Any conductive line is a potential carrier for transients and the sources for inductive coupling within any given facility are numerous. Today's computer equipment is running on lower and lower power thresholds, which means attention to even small amounts of electrical interference is important to prevent damage and data corruption. A layered approach to surge suppression is the ideal method, reducing external and other large surges first and then attenuating them further internally before passing the energy to sensitive electronic equipment. Data line surge suppression is necessary to seal sensitive equipment against data corruption, to prevent damage over low voltage data lines, and to prevent any open paths for transient surges to enter.


## About the author

**Joseph Seymour** is the lead Claim Analyst for the Schneider Electric Claims Department in West Kingston, RI. He evaluates and inspects damages caused by catastrophic transient events, and adjudicates customer claims filed in accordance with the APC Equipment Protection Policy.

## Resources

*Click on icon to link to resource*

**White Paper Library**
whitepapers.apc.com

**TradeOff Tools™**
tools.apc.com

## Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
**DCSC@Schneider-Electric.com**

If you are a customer and have questions specific to your data center project:

Contact your **Schneider Electric** representative

© 2011 Schneider Electric. All rights reserved.