Protect Your Fortress from ESD

Jerry Twomey

Published in Electronic Design, August 9, 2012

Jerry Twomey explains how electrostatic discharge (ESD) destroys electrical circuits and how to design circuits that can deal with over-voltage and over-current incidents.

Electrostatic discharges don't have to completely knock out your systems. Smart design strategies can give your devices the stamina they need to withstand ESD strikes.

Introduction

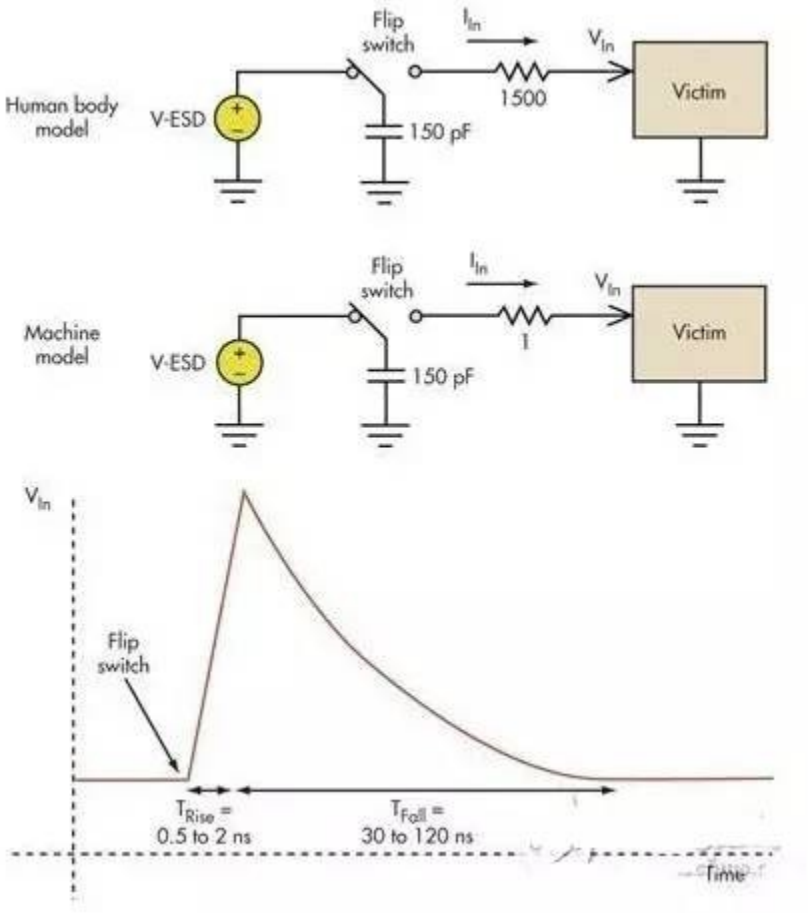
We all have hands on experience with electrostatic discharge (ESD), even if it's just from walking across a carpet and touching something metal, releasing static electricity buildup in one brief moment. Many of us have grumbled about the awkward use of conductive mats, ESD wristbands, and other requirements to meet industry ESD standards in the lab. And, more than a few of us have fried some expensive electronics due to our carelessness with unprotected circuitry.

For some, ESD is a challenge as we handle and assemble unprotected electronics without damaging anything. For others, it's a circuit design challenge to make a system survive an ESD event undamaged, remain functional afterwards, and, better yet, continue functioning through the event without a noticeable failure to the user.

Contrary to popular belief, you can get a system to survive and keep running straight through an ESD event without failure. With that goal in mind, let's get a better understanding of what actually happens in an ESD strike, and from there, figure out how to architect a system to deal with it.

The Simple Model

Figure 1: Board-level ESD typically involves machine models (MM) and human models (HBM).

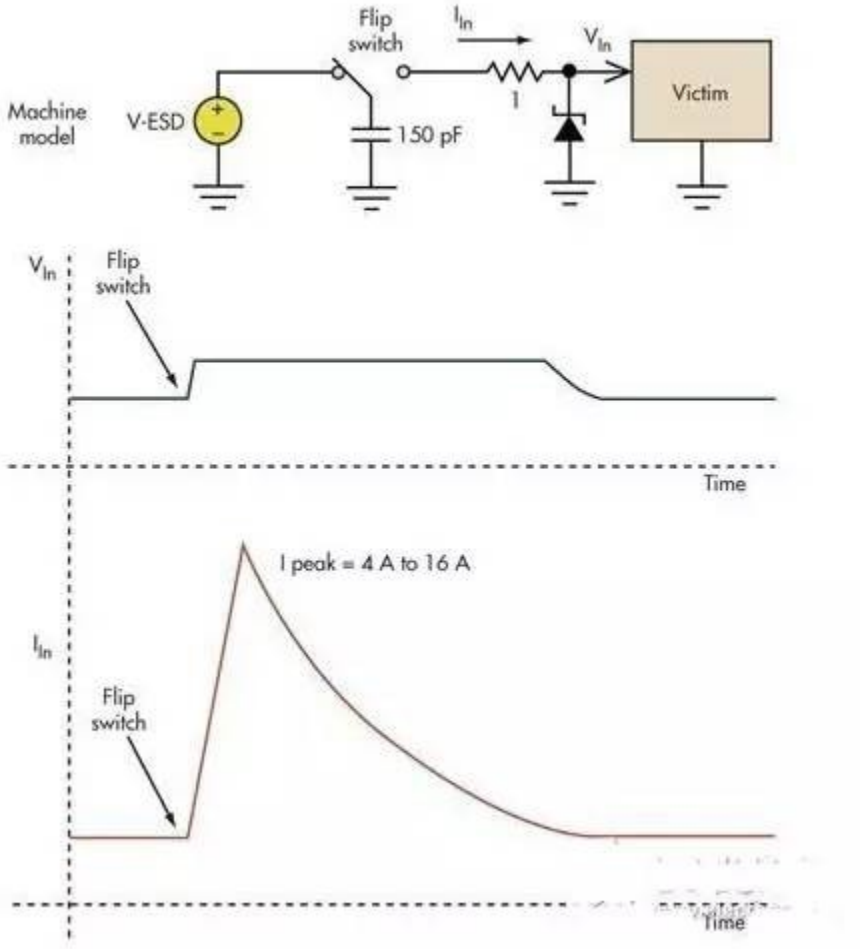


1. Board-level ESD often involves the machine model (MM) and human body model (HBM). Victim circuits are damaged by a high transient voltage that rises in a few nanoseconds and discharges in roughly 100 ns.

Charge a capacitor up to a high voltage. (Voltages of 2 to 8 kV are common.) Then, dump that charge through a closed switch into the “victim” device getting zapped by the ESD event (Fig. 1). The polarity of the charge can be in either direction, so you have to deal with both positive and negative ESD situations.

Depending on the victim circuits, the sensitivity to a positive or negative strike can be quite different, and you need to deal with both. The difference between the two most common models, the human body model (HBM) and the machine model (MM), is nothing more than some series resistance. Human bodies don’t conduct as well as metal.

Figure 2: Basic voltage limiting circuit prevents overvoltage damage

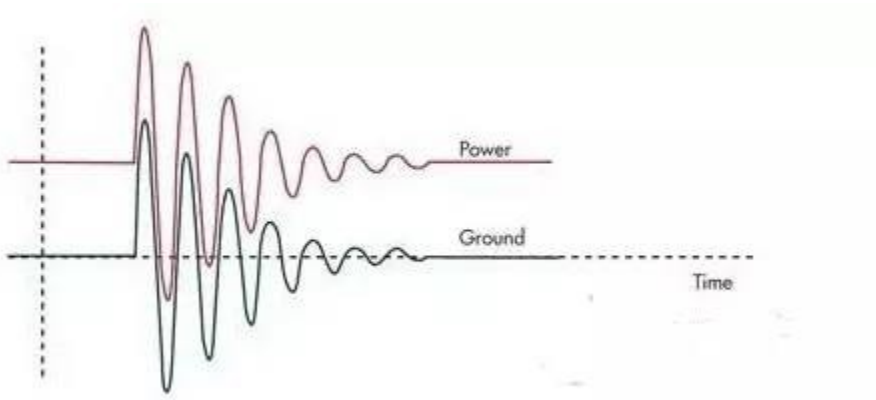


2. A basic voltage-limiting circuit can prevent overvoltage damage. The high transient voltage has been eliminated, but replaced with a multi-amp inrush current that can cause other problems in the system.

The best protection against overvoltage damage is voltage limiting or clamping with a nonlinear circuit (Fig. 2). Specialty diodes are most commonly used with low impedance when they're forward biased or in their Zener breakdown region. Introducing a voltage limiter quickly causes something else to become evident with a large current surge from the capacitive discharge through the limiter.

Depending on the total impedance of the path followed, that current can be multiple amps. When designing I/O cells for chips, I have often seen 4 to 16 A of surge current go into a device. Dealing with that huge transient current surge becomes the big problem in ESD design. Limiting the voltage is the easy part, but then the resulting current can upset circuitry and grounds elsewhere in the system.

Figure 3: Injecting a large inrush current into the ground through a voltage limiter will cause the PCB ground to bounce as a function of the connection inductance



3. Injecting a large surge current into the ground through the voltage limiter will cause the ground of the PCB to bounce as a function of the connection inductance. If the board maintains a good low impedance ground plane, and the power has good high frequency decoupling, the power should travel with the ground. Proper functionality on the PCB should continue through the ESD event.

The current forced into the ground by the limiter will cause inductive ringing in that node of the system (Fig. 3). The power supply will generally travel with the ground as a function of the power supply decoupling capacitance, so the core of the system remains functional. However, control lines coming onto the board can get corrupted because they have been established relative to a ground that is off the board. The outcome can be an ESD event in one location causing an input elsewhere on the board to be seen as faulty.

A Fortress Mentality

With board-level ESD, you're trying to build a fortress and establish a handful of controlled access points "across the moat." Items connected out beyond the "castle walls" can be loosely classified into a few categories: protocol controlled data, low-bandwidth sense and control lines, and high-speed interfaces. Two of these are easy to deal with, and the third has some challenges. There are several different approaches to keeping the three immune to ESD.

Whatever the final product, some form of protective enclosure will be part of the device. Isolating electronics within that enclosure is a first line of defense that needs to be carefully thought out. In an ideal world, a metal enclosure that connects to the board ground generally works, but modern products are often in non-conductive plastic or other modern materials.

The circuit designer generally doesn’t have much control over what the castle walls are built out of, but bears the responsibility to defend the fortress nonetheless. When defining the enclosure, keep in mind that ESD to any external part of the case can take a multitude of paths into the electronics.

Building a fortress where the PCB can self-protect from ESD starts with a low-impedance grounding approach (see “Simple Grounding Rules Yield Huge Rewards”). Establishing a ground foundation and proper power integrity allows the printed-circuit board (PCB) to maintain signal integrity across the board even when it’s hit with a huge ground current surge.

As a designer, you’re asking everyone to fasten their seatbelts so you can deal with a little turbulence. The plane may go up and down rapidly, but if everybody is strapped in it all stays together and keeps on going. After that, you need to protect the external connections and limit the effects of the ESD event.

Protection circuits should be at placed the entrance to the board and not downstream from the entrance point. You’re dealing with something that has kilovolts of potential for possible arcing problems or a multi-amp inrush current that’s best dealt with at the edge of the board.

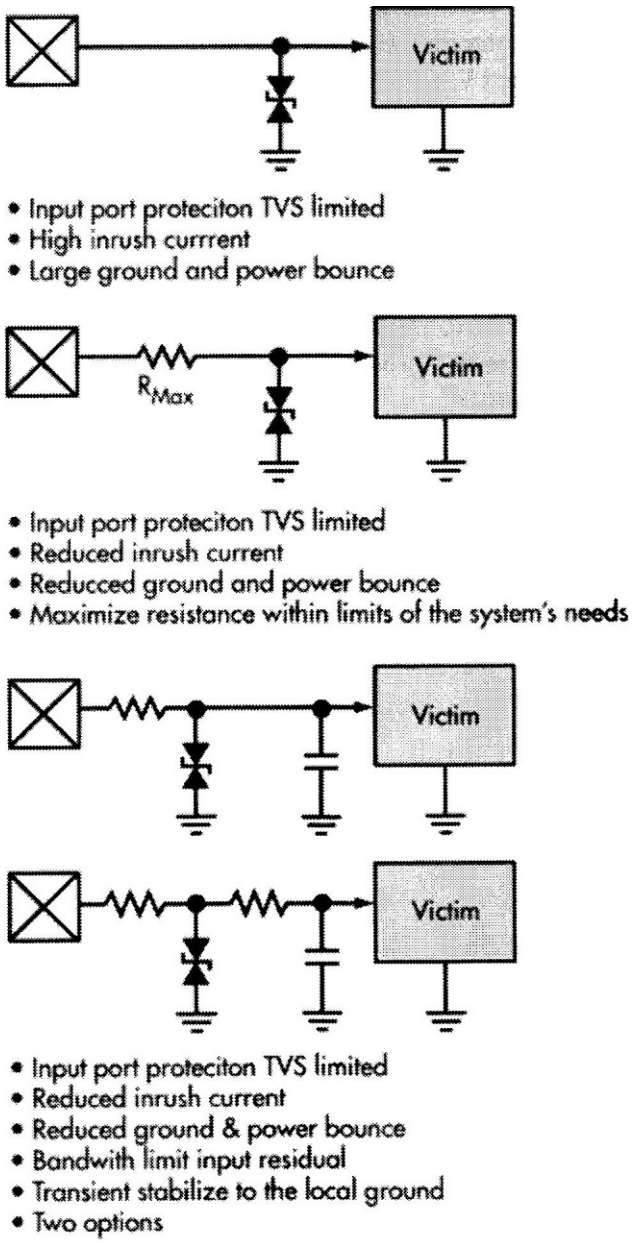
TVS Limiters

Transient voltage suppression (TVS) limiting diodes can serve as voltage limiters. They come in an assortment of voltages optimized to common voltages and logic levels and power supplies. The usual suspects are there: 12 V, 5 V, 3.3 V, 2.5 V, 1.8 V, and 1.2 V.

The numbers should look familiar as the devices were designed specific to the needs associated with many CMOS devices. One size does not fit all, and they should be the appropriate voltage for the device you are trying to protect.

Modern CMOS processes have reduced power supply voltages to protect the limited voltage range of the transistors without a lot of design margin, and that needs to be respected. These devices are generally manufactured using a foundry process that provides a high current device with low resistance characteristics in a small package.

Figure 4: A simple TVS voltage limiter can provide over-voltage protection, but may cause inrush current problems. Inrush current should be limited and the signal needs to remain stable relative to the local ground



4. Simple limiting circuits will provide overvoltage protection but can cause problems with inrush current. The inrush current should be limited, and the signal should be kept stable to the local ground.

Putting a TVS limiter on an input line will protect the input from ESD destructive damage (Fig. 4). But the limiter doesn't deal with corruption of the signal seen at the host process or the upsetting effects due to a huge surge in ground current.

As mentioned before, the performance difference between the HBM and MM can be very significant. In many cases the addition of some series resistance prior to the TVS device will help limit the current surge and reduce ground bounce. Similar to the HBM, the net result is less system stress.

Bandwidth limiting by itself generally won't deal with ESD. The attenuation of a low pass filter on a small ESD even would require 60 to 140 dB of attenuation to get rid of the transient, which isn't easily done in a simple passive filter. The TVS limiter gets the signal down between the power rails.

Then, a first-order RC section can be used to maintain digital signal integrity (Fig. 4). The capacitor also stabilizes the input relative to the local ground. This method works well to protect the large number of low-bandwidth inputs, which includes "set and forget" control lines, sensor inputs, and similar things.

Although we talk largely about protecting the input ports to the PCB, output port protection is similar. TVS limiters and additive resistance are appropriate here as well. Limiting the voltage will help prevent semiconductor damage and other parts that have voltage restrictions.

Some series resistance will help with ground stability too. Also, keeping the ESD surge current away from a digital chip's I/O cells will prevent ground bounce internal to the chip, allowing the processor to remain functional when the external limiter takes the brunt of the current surge.

ESD Inside A Chip

For multiple reasons, ESD protection inside of an IC is a bit of a compromise. Silicon and metal have been optimized to the core functions of the IC, not for high current circuitry. Specialty TVS devices use silicon optimized for high current circuitry and perform better than PN junctions in generic CMOS.

In addition, I/O cells with high-amperage ESD protection can take up a good amount of space, pushing the cost of the IC up. Further, high-frequency pins on the IC often can't have large-geometry ESD protection attached due to the capacitive load it creates.

As a general rule, ESD protection within a chip suffices to get the IC fabricated and soldered onto a PCB, but falls short of the robust protection an applications environment often needs. If a connection goes off the PCB, generally it needs further protection from external abuse.

Data Communication Ports

Properly designed communication ports use a robust protocol that includes testing data integrity by use of a cyclical redundancy check (CRC) code. Ethernet, USB, and the CAN bus develop a CRC code and transmit it with the data. The receiver is designed to check to see if the CRC code fits the data sent. If it doesn't match, either the data or the CRC code was corrupted, and a request to resend the data goes out.

Since an ESD event lasts under 100 ns, the CRC check, verify, and resend process will usually deal with ESD invisibly. The end user typically is never aware that corrupt information was corrected. Some other protocols don't have safeguards in their structure.

I2C, the serial peripheral interface (SPI), and system management bus (SMBus) communication were designed to stay on a PCB and can't verify and correct data. If you're going off the board with something, make sure that you have a way of verifying data validity.

Most modern communication paths are differential, using some form of low-voltage differential signaling (LVDS). Each LVDS connection needs to be TVS protected just like all the other signals. Magnetic isolation (common with Ethernet) and common-mode chokes will help deal with common-mode variance that happens due to ground bounce in an ESD event as well. Optical isolators or magnetic isolation should be used in situations with signals coming in that don't share a ground with the PCB.

A high-speed data stream that requires perfect data integrity but includes no error checking is particularly difficult to safeguard from ESD. Considering how devices are readily available with serial data rates above 1 Gbyte/s and full communication protocol protection, this can be avoided.

Analog Signals & Digital Intelligence

Any analog signal going on or off the board needs basic TVS protection. The bandwidth of what is attached needs to be considered to determine what other steps should be taken. Most analog control signals, motion control systems, audio, and indicator lights won't need more due to the slow response time of the device. RF front ends are the physical layer of a communication channel with error checking as part of the protocol providing self-correction.

Hardware can provide only so much protection. If there is some processor at the center of the system listening and controlling things, some options are needed there as well. The techniques described here should give you a processor that doesn't get lost or need to go through a reset cycle. What's underneath the control of that host is another consideration, though.

Generally, you need to write some intelligence into the code of the processor so it can recognize bad information and deal with it. Slow speed sense and control lines are easily addressed through time spaced polling of the port. Since ESD events are brief, if the data at the port remains stable for multiple samples over several milliseconds, your system will get beyond the ESD event without mishap.

In addition, outputs can be refreshed as part of a recurring process. This isn't needed if the processor is the memory element. But if the data is latched remotely, a refresh routine will manage corruption.

Conclusions

Empirical testing with both positive and negative ESD needs to be performed on all of your device's externally exposed surfaces. The IEC-61000-4-2 and ISO-10605 specifications outline testing methods and should be consulted to avoid redesign efforts after the fact. It's better to cover these issues as part of the design process. The ESD Association offers a number of useful standards and procedures for testing and compliance.

These procedures should take care of most of your ESD issues. Due to the single-event nature of ESD events, some special tools will be needed to do laboratory evaluations. You need an ESD gun capable of creating single and repetitive ESD events and a fast storage oscilloscope with good single event capture capability.

Also, a front-end attenuator with 10,000:1 attenuation and good high-frequency grounding will keep you from destroying the input amplifier of the scope while allowing you to see what's going on. But then, we hope the scope designer included good ESD protection in the front end!

Jerry Twomey
jerry@effectiveelectrons.com

###