Embedded Systems: Safeguard Ethernet Interfaces from Cable Discharges

Timothy Puls, Product Marketing Engineer and Hani Geske, Senior Applications Engineer, Semtech Corporation

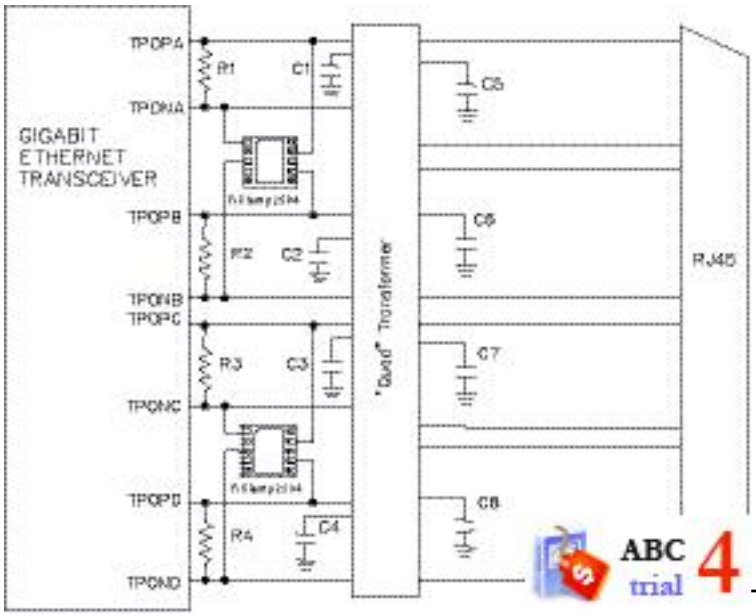
Safeguard Ethernet Interfaces from Cable Discharges

by Timothy Puls, Product Marketing Engineer and Hani Geske, Senior Applications Engineer, Semtech Corporation

Protecting Ethernet interfaces from cable discharges can create a challenge for engineers because good protection must meet two criteria. First, and most important, a protective device must effectively clamp a transient to a safe voltage. Second, the device must present an acceptable capacitive load on high-speed differential transmission lines. Good planning and careful selection of transient voltage-suppression devices can adequately protect Ethernet interfaces from electrostatic discharges (ESDs) and cable discharge events.

Designing a system for both high-speed-communication and transient immunity requirements is nontrivial. Newer Ethernet transceivers run faster, consume less power and use less PCB space. But these advances have contributed to a reduction of on-chip transient-voltage protection levels. Thus, designers need advanced system-level circuit protection to ensure Ethernet systems remain immune to ESD and cable discharge threats.

Engineers might view an Ethernet cable-discharge event (CDE) as a type of electrostatic discharge (ESD), but they should treat CDEs as a separate type of transient event. You can model an Ethernet cable--generally unshielded, twisted-pair Cat-5 or Cat-6--as a capacitive element that can store a significant charge. That cable, which can run as long as 100m, can accumulate charge via triboelectric or induction effects. Simply dragging a cable along a carpet or removing it from a package will lead to a stored charge. Inductive transfer from a user also can charge a cable. Because Cat-5 and Cat-6-twisted pair cables have low-leakage properties, the charge may remain stored on a twisted pair for several hours and it can discharge into an Ethernet port when a user connects it to equipment. The latter type of discharge occurs directly into the communication interface and poses a particularly dangerous threat to Ethernet ports. The high peak voltage and current during a CDE can overstress an Ethernet transceiver and lead to intermittent malfunctions or total failure.



ABC trial 4

The semiconductor industry recognizes the need for a standard method for testing CDE and Working Group 14, ESD Simulators, within the Electrostatic Discharge Association is currently defining a standard method for CDE testing. This work will define a testing method that uses an ESD waveform specified in IEC 61000-4-2, which covers system-level human-body model electrostatic-discharge immunity tests. But the new method will account for energy transfer through a cable rather than through a human body. Unlike a human-body-model ESD, a CDE has an initial current spike followed by a

characteristic plateau and then a ringing signal with rapid polarity changes. A CDE can deliver more damaging energy to CMOS structures than can a human-body-model ESD.

Engineers can somewhat enhance Ethernet-port protection through good PCB layout practices and careful selection of robust components. But Ethernet ports also require the addition of system-level protection circuits. Unfortunately, some protection circuits negatively affect signal integrity and others offer inadequate protection. We recommend engineers consider the following characteristics when they review Ethernet-port protection needs:

* Fast response time
* Low clamping voltage, leakage current and capacitance
* High energy handling capacity
* Easy PCB layout

First, an effective Ethernet-protection device must offer a response time faster than the transient events a system will experience. Thus to safely attenuate a fast discharge during ESDs and CDEs, the protection device must respond within hundreds of picoseconds. The nearby figure shows an example of a protection circuit scheme with a sub-nanosecond response time. Placing the protection devices "behind" the Ethernet transformer further reduces surges.

Second, a well devised protection circuit must provide a low clamping voltage for a transient pulse. A transient voltage suppressor (TVS) such as the RClamp2504N diode array offers a 4V clamping voltage (Vc) for a peak pulse current (Ipp) of 1A. Its Vc increases linearly to about 10V for an Ipp of 25A. This type of low-voltage clamping response provides a large protection margin for an Ethernet transceiver.

Finally, the capacitance of a protection circuit must have minimal effect on Ethernet signal integrity. At Gigabit Ethernet speeds you can no longer treat the interface as a lumped-element system but must consider it as a transmission line in which the effect of capacitive elements on signal performance becomes consequential. Excess capacitive loading can cause signal reflections and an impedance mismatch on the transmission line. Choosing components with minimal line-to-line and line-to-ground capacitance can help to ensure a small and acceptable level of signal distortion.

Timothy Puls has more than eight years of experience in applications and marketing within the semiconductor industry. He holds a BSEE degree from Texas A&M University.

Hani Geske’s has more than 11 years of industry experience. Her last 9 years of experience have been focused on high-speed transient voltage suppression applications engineering. She earned a BSEE degree from the University of Southern California.

Source URL (retrieved on *09/23/2014 - 10:28pm*):

http://www.ecnmag.com/articles/2008/09/embedded-systems-safeguard-ethernet-interfaces-cable-discharges