How to Protect Mobile Devices from 'USB Kill' Threats

WHITE PAPER

TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuses

SMT Gas Discharge Tubes

INTRODUCTION

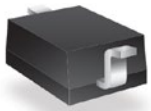
Researchers have long warned about the security risks of inserting other users' USB drives into your PC, even those from whom you trust. If the threat of malware infections isn't cause enough for concern, there have been stories of malicious USB thumb drives that have "fried" laptops. Does this seem like a far-fetched occurrence? Hearing of the threats, *PC World* documented the work of an electronics engineer who set out to create a prototype that could actually kill a mobile device's USB port.

Since its debut (c.1995), the USB port has facilitated the connection between computer peripherals and personal computers, mobile phones, smartphones, tablets, etc. – and its use continues to evolve.

It is always an engineering challenge to consider and evaluate an event "outside the realm of regular expectations" or what is commonly referred to as a "Black Swan" event – especially when you are dealing with industry standards, like the USB standard (USB = USB2.0, USB3.0, Wireless USB, etc.). A Black Swan event is defined as having the following three attributes. First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable.

This white paper presents how USB Kill Drives work, and the damage that can be caused to USB ports by these malicious drives. It also outlines an effective multi-stage protection solution that mobile application designers can implement which goes beyond the minimum standards typically used today.

How to Protect Mobile Devices from 'USB Kill' Threats White Paper



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

What is USB Kill?

The USB Kill or USB Killer 'Black Swan' event – was the engineering challenge to protect a USB port against a 'couple hundred volts' and 'couple hundred amps'.

A USB Kill or USB Killer Drive is a malicious USB flash drive that can first charge via the USB Vbus, and then deliver a power surge of between -220/240 Vdc and >175 A pulses via USB data lines. This extreme power surge is delivered in a repetitive loop with the intention of damaging anything that isn't designed to withstand its surge. This malicious device can cause a wide variety of damage – from a simple damaged port to an uncontrollable thermal event. Because many mobile devices are now used in mission-critical applications or are of a high dollar value, they will need to be protected from USB Kill dangers.

Due to the USB port's broad installed base, the standard/default protection is widely known. A common practice is to protect the USB data lines with an ESD protection device that complies with the IEC 61000-4-2 (ESD) standard. Unfortunately, a USB Kill Drive can exploit this level of protection.

Designed to overpower the most common USB data line protection, the large surge a "USB Kill" or "USB Killer" drive can generate is often too much for the most common ESD protection devices to handle. After the first couple of pulses, the subsequent power surges continue to damage any electronic components in their path, beyond the USB controller – and in some cases, resulting in an uncontrolled thermal event.

Figure 1 shows actual USB Kill waveforms.

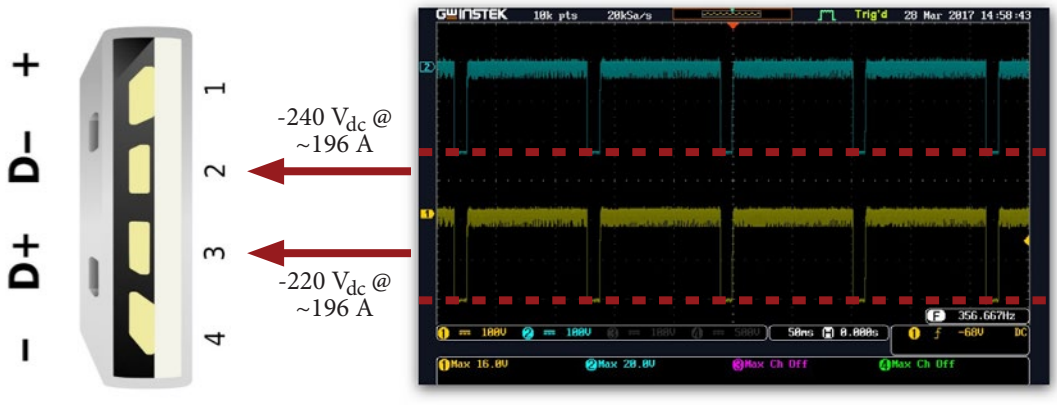
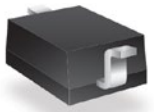


Figure 1. | *Actual USB Kill Waveforms – Voltage & Pulsed Current Levels*



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

An Effective Protection Solution

There are a wide variety of circuit protection technologies available, so it is necessary to find the right robust protection solution for USB Kill Drives. After testing and researching the surge parameters of a USB Kill Drive and how it attacks devices, the engineers at Bourns concluded that a multi-device solution that includes TVS diodes, TBU® High-Speed Protectors (TBU® HSPs) and Gas Discharge Tubes (GDTs) provide the optimum defense against USB Kill threats.

Figure 2 illustrates a traditional USB port protection solution that uses a TVS diode for ESD protection and a PPTC for overcurrent protection and/or reverse polarity protection. Added to a basic USB port protection solution are TBU® HSPs and a GDT that together are necessary for an effective anti-USB Kill solution.

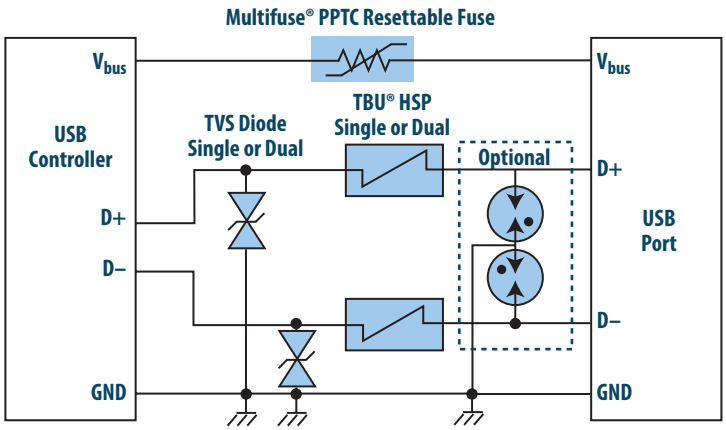
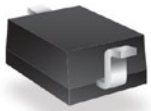


Figure 2. | *Bourns' Suggested Solution*

Bourns designed its TBU® HSPs as electronic current limiters that deliver effective surge protection for lightning, power induction, power cross, Earth Potential Rise (EPR) or other energy surge conditions. Constructed using MOSFET semiconductor technology, TBU® HSPs, when placed in series with a signal line, monitor the current flowing through the line. If the current exceeds a preset level, the TBU® HSP triggers, providing an effective barrier to high voltages and currents. Valuable for a USB Kill application, the TBU® HSP begins protecting in less than 1 millisecond. When in the protected state, the TBU® HSP restricts line current to less than 1 mA typically, and blocks voltages up to the maximum voltage rating of the device. At the end of a surge event, the TBU® HSP will begin the reset process when the voltage across the device drops below the V_{reset} level and will complete the reset process when the signal line returns to its normal operating range.

How to Protect Mobile Devices from 'USB Kill' Threats White Paper



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

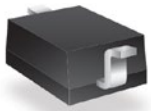
An Effective Protection Solution *(Continued)*

Features that make Bourns® TBU® HSPs highly suitable in an anti-USB Kill application are:

- Series protection device
- Triggers at a specified current
- Can block voltages up to 850 V, enabling easy coordination
- Provides superior protection in less than 1 µs
- Does not add capacitance to the signal line
- Extremely low let-through energy
- Self-resetting (V_{reset} valve)
- Very high bandwidth
- Small size in DFN package

Using a GDT's low capacitance (<1 pf) and fold-back characteristics, this solution performs similar to a "bleeder-resistor." The GDT, with its >2 kA rating and crowbar characteristics, is an optional device to deplete the USB Kill capacitor bank in the first couple of pulses.

GDT surge arrestor devices are designed to operate on the gas-physical principle of the highly effective arc discharge. Essentially a voltage dependent switch, the GDT maintains a high impedance off-state until a voltage exceeds the device's sparkover voltage. At this point, the gas in the GDT becomes fully ionized and conduction takes place within a fraction of microsecond. During arc-over, the GDT exhibits the low impedance of a crowbar device resulting in very low on-state voltage (arc voltage). The crowbar effect of the GDT effectively limits the overvoltage to a low level and shunts the associated flowing current away from downstream components and circuitry. When the surge event subsides and the system voltage returns to normal levels, the GDT will reset into its high impedance (off) state.



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

An Effective Protection Solution

Figure 3 shows a Bourns lab test of only the TVS and TBU® HSP to highlight the reduction in voltage and current from the use of these devices. In this test the voltage has been reduced to the TVS Diode (V_{br}) and the current reduced to a manageable ~68 mA. Please note the repetitive pulses, which will only end when the capacitor blank has been depleted.

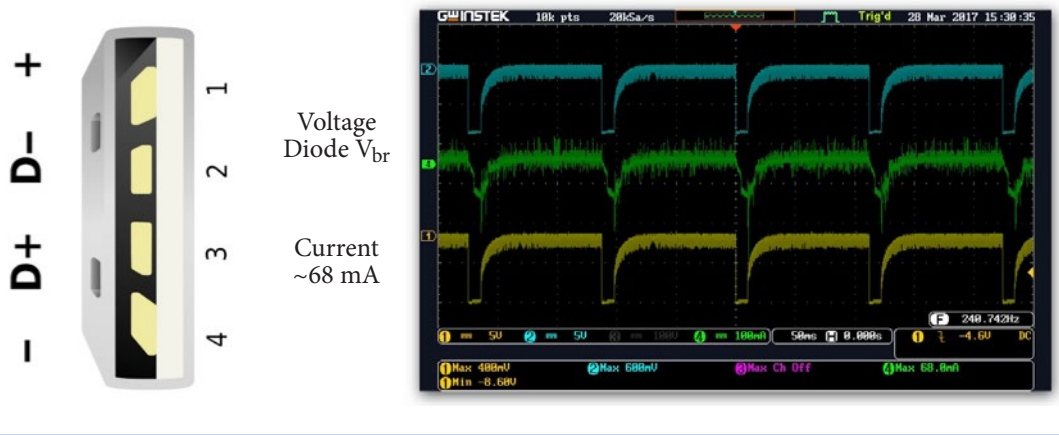
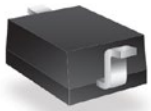


Figure 3. | *Actual Results of Bourns' Suggested Solution Waveforms – Voltage & Pulsed Current Levels*



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

An Effective Protection Solution *(Continued)*

Figure 4 shows Bourns' suggested USB Kill solution that highlights the devices required for evaluation, which can be easily modified per unique customer requirements, single/dual devices, PCB area, etc.

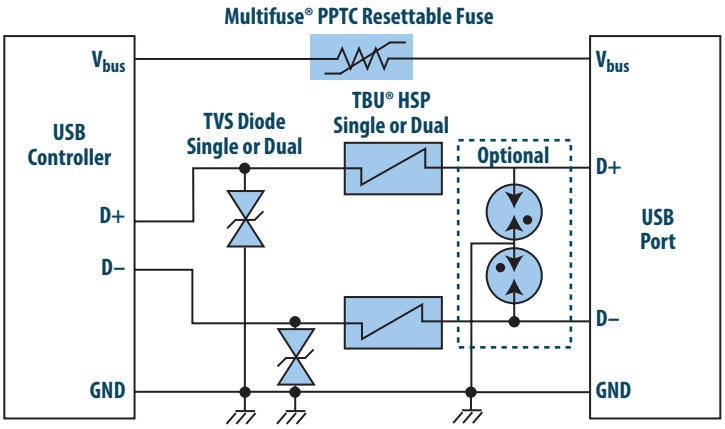


Figure 4. | *Bourns' Suggested Solution & Part Number List (USB 2.0 & USB 2.0 High-Speed)*

Option 1 [MIN] (4 Total Components)

Two TVS Diodes: Bourns® Model CDSOD323-T05LC (1 pF) (1x per data line D+ and D-).
Two TBU® High-Speed Protectors: Bourns® Model TBU-CA040-050-WH (1x per data line D+ and D-).

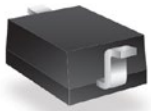
Options 2 [FULL] (7 Total Components)

One Multifuse® PPTC Resettable Fuse: Bourns® Model MF-NSMF075-2 (1x V_{BUS}).
Two TVS Diodes: Bourns® Model CDSOD323-T05LC (1 pF) (1x per data line D+ and D-).
Two TBU® High-Speed Protectors: Bourns® Model TBU-CA065-050-WH (1x per data line D+ and D-).
Two SMT Gas Discharge Tubes: Bourns® Model 2051-09-SM (1x per data line D+ and D-).
(crowbar device) to deplete capacitor bank.

Figure 4 shows two solutions that, depending on PCB space and the desired level of protection, could be selected. The main difference between option 1 and option 2 is the addition of the GDT. If and when a USB Kill is connected, option 1 will cycle until the USB Kill capacitor bank is depleted, which could take some time.

Option 2 uses the GDT's fold-back characteristics as a "bleeder-resistor" to deplete the USB Kill capacitor bank in the first couple of pulses. This multi-stage protection approach gives mobile application designers an effective solution for malicious USB Kill threats using proven components readily available today.

How to Protect Mobile Devices from 'USB Kill' Threats White Paper



TVS Diodes

TBU® High-Speed Protectors

Multifuse® PPTC Resettable Fuse

SMT Gas Discharge Tube

ADDITIONAL RESOURCES

[1] Nassim Nicholas Taleb "The Black Swan: The Impact of the Highly Improbable" (Random House 2007)

For more information and further technical support, visit Bourns online at:

www.bourns.com

BOURNS®

Americas: *Tel* +1-951 781-5500
Email americus@bourns.com

EMEA: *Tel* +36 88 520 390
Email eurocus@bourns.com

Asia-Pacific: *Tel* +886-2 256 241 17
Email asiacus@bourns.com