Cactus® Technologies

Write Abort Handling for Cactus Technologies Industrial-Grade Flash-Storage Products

White paper CTWP005

Cactus Technologies Limited
Suite C, 15/F, Capital Trade Center
62 Tsun Yip Street, Kwun Tong
Kowloon, Hong Kong
Tel: +852-2797-2277
Email: sales@cactus-tech.com

Cactus USA
3112 Windsor Road
Suite A356
Austin, Texas 78703
Tel: +512-775-0746
Email: americas@cactus-tech.com

Cactus-Tech.com

01 Introduction

Cactus Technologies industrial-grade flash storage products are designed to operate in environments where temperature, shock, vibration and voltage fluctuations occur often and can cause abnormal operations on the device. The special features of the on-board intelligent flash controller for Cactus Technologies flash storage products can help to prevent these extreme conditions from causing drive corruption.

02 The Problem

Many industrial computers and embedded systems often experience unexpected power outages, surges, spikes, sags or brownouts. Sometimes the device is manually removed from the system. These can cause data and disk corruption, and in turn lead to field failures and product returns. When power is unexpectedly removed during idle or read operation, no data loss will occur. Data losses can only occur when power is unexpectedly removed, either by power outage or by manual device removal, during write operations. This is known as Write Abort. If the write operation is "aborted" during flash erase operations, data losses beyond the data pending for write may occur.

03 Failure Symptoms

There are, in general, two types of failure symptoms that the user may come across when the storage device is affected by sudden power failures. These are 1) file system corruptions and 2) internal device data corruption.

File system corruptions are the result of the operating system not being able to completely update the file system records. Some file systems are more vulnerable to corruption issues than others. For example, a journaling EXT3 or EXT4 file system is much more robust against corruption when compared to a FAT file system. Some examples of FAT file system corruption includes corrupted FAT tables or lost clusters.

It should be noted that file system corruptions cannot be prevented by the storage device's firmware or hardware design. This is because the storage device has no knowledge of what file system is being used and does not know where the file system records are located; hence, there is no method for the device to safe guard file system blocks.

Luckily, file system corruptions are generally not fatal. Most operating systems will perform a file system repair operation on the next power up after a sudden power lost event. Alternately, the user can run a command or utility to perform the repair operation.

Internal storage device data corruptions, on the other hand, can make the whole device unusable. This type of error is the result of the device's internal metadata (such as logical to physical mapping

table) getting corrupted during a sudden power loss event. When this happens, either existing data may get corrupted or the drive becomes totally unrecognized by the host. The only way to recover from such a failure is to perform a low level format of the device, thus resulting in a loss of user data.

Since internal data corruption is fatal, it is the focus of the storage device's firmware and hardware design to ensure that internal data corruption does not occur under any circumstance.
In the following sections, we will explain some of the key features in Cactus Technologies Industrial grade flash products that mitigates and/or eliminates Write Abort data corruption problems.

04 Patented Safe Power Loss Protection Algorithm

Cactus Technologies -303, -503 -806 and -900S series products utilize a patented firmware algorithm in order to ensure data integrity when transferring or writing data. Data in these products is written in a way that minimizes the delta between an old and a new state. The data system is coherent at all times. Upon a sudden power fail, the controller is reset and the flash is immediately write-protected. A log of the most recent flash transactions is kept, where entries are made just before any programming to the flash. Should the last entry of the log be corrupted, the controller recovers the last valid entry. This minimizes data loss due to power failures and data corruption at the physical layer is prevented completely. Should power loss happen at the very same time when data is written to the flash, this data in transit might get lost. In no case, however, will the overall data system be corrupted.

Extensive power cycling tests have been performed on -303 and -503 series products to verify that no data loss occurred due to sudden power failures.

05 Minimize Use of External DRAM Cache

Many of our competitor's products utilize extensive DRAM caching to improve performance. Typically, the DRAM cache stores lookup tables and other internal metadata but in many cases, it also stores user data to be written to flash memory. In the event of a sudden power lose, the data stored in these DRAM caches are vulnerable and can cause significant data integrity loss. In the worst case scenario, the device's internal metadata is corrupted and the device will no longer be recognized by the host system and the only way to recover is to do a low level format on the device, causing all previously stored data to be lost.

Cactus Technologies recognizes the vulnerability of using external DRAM cache, therefore, we intentionally try to use controllers that do not use DRAM caching. All our -303, -503 and SD products do not use external DRAM caching. Our -602S SATA products also do not use DRAM caching. While our 700S SATA product does use DRAM caching, it is protected by internal power backup circuitry, which we will discuss in the next section.

Cactus Technologies recognizes that the lack of DRAM caching results in lower read/write performance of our products. However, we view the superior robustness against write abort data protection as a higher priority, particularly in industrial applications where high reliability is generally more important than high performance.

06 Internal Power Backup

For high performance SATA II or SATA III products, it is not possible to reach the high data throughput offered by the SATA interface without using external DRAM cache (or large internal DRAM buffers).

As Cactus Technologies recognizes that data stored in DRAM caches is vulnerable to sudden power loss, on products that do use such caching, we also implemented an internal power backup circuitry. A conceptual block diagram of this circuitry is shown below:

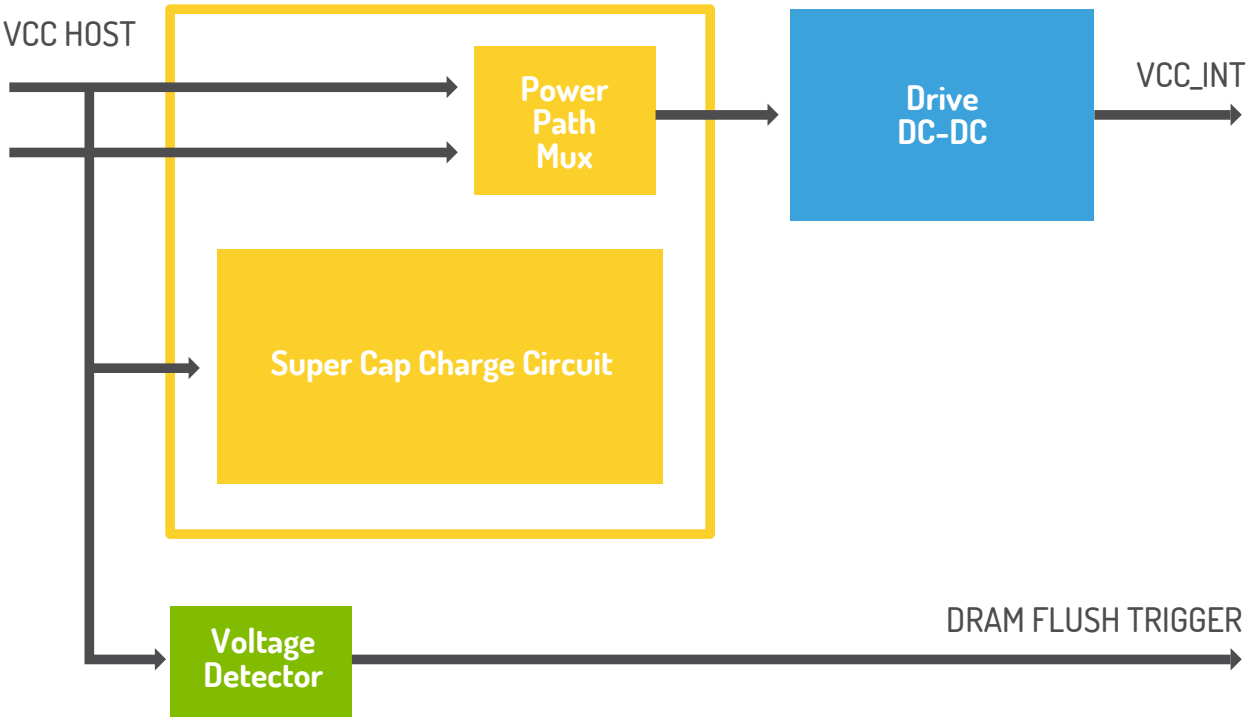
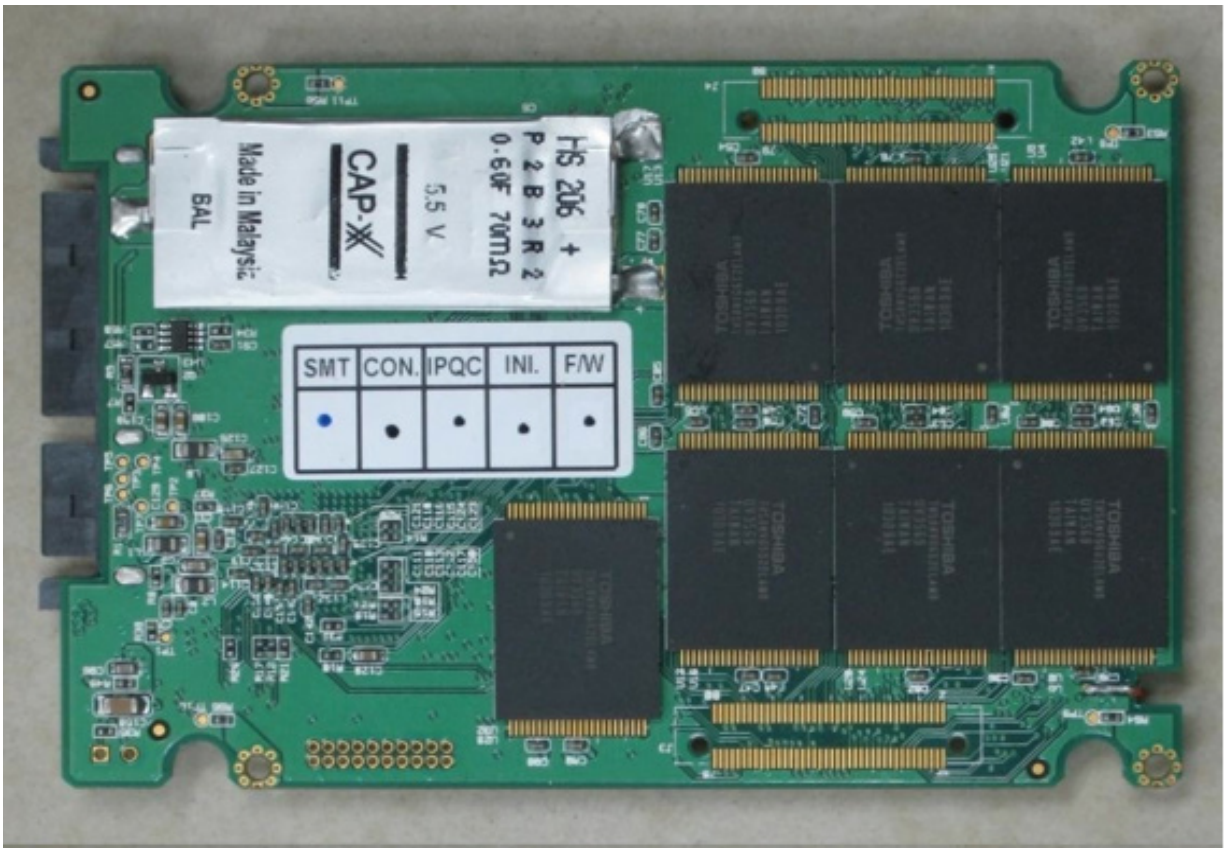


FIG. 1

Incoming supply from the host goes to the SuperCap charge circuit to charge up a SuperCap of a value calculated to provide sufficient charge to power the internal drive to guarantee that all the data in the DRAM cache is successfully written to the flash memory. The charge circuit also has a bypass path such that during normal operation, Vcc from the host is supplied directly to the internal circuitry. This is important because it takes some time to fully charge up the SuperCap. The BIOS on some systems may time out before the drive is powered up and thus, not recognize the presence of the drive. The bypass path assures a normal, fast startup of the device.

Separately, the Vcc supply from the host also goes to a voltage detector which is set to generate a trigger signal if the Vcc supply falls below a pre-determined threshold. This trigger signal goes directly to the controller. The controller has specially designed firmware such that when it receives this trigger signal, it immediately makes the SATA interface go busy to prevent further data from being sent to the drive. It then begins the process of flushing all the data in the DRAM cache to flash memory. This process is guaranteed to complete by choosing the correct value for the SuperCap. By using this combination of hardware/firmware design, Cactus Technologies guarantees that even in cases where external DRAM cache is used, there will be no possibility of data corruption occurring in the internal data of the storage device.

It is worth noting that we choose to use SuperCap instead of an array of smaller caps, as is done by some other vendors. The reason for this is because it can take a long time to completely flush the DRAM cache contents to flash memory. This process can take several seconds. The capacitance of small tantalum or ceramic caps is limited, our calculation shows that even with an array of 20 to 30 such capacitors, it does not provide sufficient charge to guarantee the DRAM flush process will complete. SuperCap is the only option.



Cactus Technologies has implemented SuperCap backup design in our 700S series SATA SSDs.

This product has been tested by numerous customers and is proven to provide superior immunity against sudden power loss data corruption.

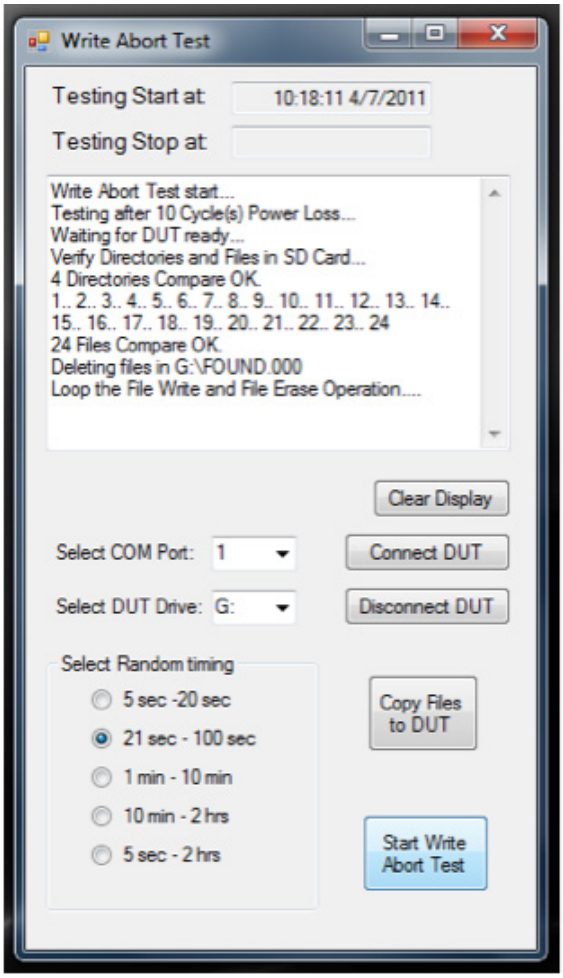
07 Rigorous Testing

In addition to the firmware and hardware design features discussed above, Cactus Technologies has built test fixtures and conducted extensive power cycling tests to verify that our products are robust against data corruption in a sudden power fail scenario. The pictures below show our test fixtures for testing SD Cards, CF cards and SATA SSDs and CFast cards:

The test fixture has a DC-DC controller and a bus isolation circuit, and is controlled via a serial port connected to a PC. Special test code written by Cactus Technologies randomly shuts off power and isolates the interface bus from the DUT. This ensures that the DUT is not powered via interface bus signals.

A typical test sequence is as follows:	
1	Pre-copy some directories and static data to the DUT.
2	Verify directories and data in DUT.
3	If some corrupted files in directory "\FOUND.000", delete them, as these are results of file system repair (as discussed in Section 3.
4	Start a random timer to disconnect the DUT.
5	Write a large file (File A) to DUT.
6	Delete "File A" in DUT
7	Write another large file (File B) to DUT
8	Delete "File B" in DUT
9	GOTO step 5. Repeat loop until the random timer activated.
10	The random timer disconnect the DUT, Wait 3 sec and re-connect the DUT.
12	Scan and repair corrupted files. This is standard OS file system process.
13	GOTO steps 2 and repeat loop.

The following picture is a screen capture showing a typical test run:



Cactus Technologies performs ongoing testing of new controllers and firmware to ensure data protection against sudden power fail is not compromised.

08 Host Design Considerations

Since data losses or corruption may happen during a write abort event, we strongly recommend host systems to have some sort of data verification scheme, such as using MD5 or similar checksum method or by comparing the file against a known good source on the host. This will make sure that correct data is written to the device. If the verification fails, the host can re-write the data to the device or perform other error-recovery steps to ensure data integrity.

If the system design allows, adding redundant power supply and designing the system to avoid manual device removal can also prevent write abort from occurring in the first place.

09 Support Information

If you would like any additional information regarding data contained in this white paper feel free to contact a Cactus representative:

Asia/Pac RIM	info@cactus-tech.com
Americas	americas@cactus-tech.com
EMEA	info@cactus-tech.com