CTAN005: Write Abort Handling for Cactus Technologies Industrial-Grade Flash-Storage Products

Covered Products: All

1. 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.

2. The Problem

Many industrial computer and embedded systems often experience unexpected power outage, 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.

Many field failures and product returns stemming from write abort are not hardware defects, and can be repaired by re-initializing and re-formatting the device before returning it to the customer. Many of these field failures may be prevented from occurring by the "Make-Before-Break" algorithm and advanced voltage detection hardware implemented on all Cactus Technologies industrial-grade flash-storage products.

3. The Solution

The "Make-Before-Break" algorithm always ensure data in the single-sector buffer is written successfully to the flash before updating the ECC and other on-device data structures.

Even if new data is only partially written to flash before power outage, the on-device housekeeping data structures will remain intact and reflect the last known good state of the device. The completed data writes will remain intact, and the only data loss incurred by the write abort is the data not yet written to the flash when the power is unexpectedly removed from the device.

Also, the ECC engine on-board the intelligent controller will not regard uncorrectable ECC errors as defects (as they can also be caused by write abort) during read operation. This handling has two side effects as relating to write abort issue: the first is, the controller will not mark physical flash blocks written with incomplete or corrupted data during the write abort as bad blocks, therefore a write abort scenario will not cause "damage" to the flash device. The second effect is the controller may pass corrupted data or signal a read error to the host that requires error handling and recovery.

4. SD Card Brownout Detection

In addition to the solutions mentioned in section 3, the Cactus Technologies industrial-grade SD cards also incorporate brownout detection and handling algorithms that designers can take advantage to

prevent possible data loss during write-abort scenarios.

When the supply voltage is 2.7V to 3.3V, then the SD card transfers data normally as the supply voltage falls within SLC NAND and SD card specifications. When the supply voltage drops to a range between 2.5V to 2.7V, the controller will issue a busy signal to the host until the voltage rises above 2.7V. The host should sample the busy signal periodically and stops read/write operations on the card.

During this low voltage range, the SD card controller will attempt writing data in the buffer to the NAND flash pages, but since the NAND flash operates at a voltage level below the minimum operating specification, it is difficult to guarantee data written into NAND flash pages during brownout scenario is valid. Also, if the data is not yet written to the NAND flash pages when brownouts or power loss occurred, the data stored in the buffer is lost. However, data written before the brownout or power loss occurred is safe, and the maximum data that may be lost during a write-abort scenario on the Cactus Technologies industrial-grade SD card is 2Kbyte.

5. Host Design Considerations

Since data losses or corruption may happen during a write abort, we strongly recommend host systems to verify written data (by using MD5 or similar checksum method or by comparing the file against a known good source on the host if possible). 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.

For Cactus Technologies industrial-grade SD cards, designers can take advantage of brownout detection by sampling the busy signal every time before data transfer.

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.

6. Version History

Version	***Date***	***Change***
1.01	October 9, 2006	Initial Version
1.02	December 18, 2006	References to “Cactus” changed to “Cactus Technologies”
1.04	November 22, 2007	Added SD card-specific information
1.05	June 3, 2008	Minor edits