POWER FAILURE PREVENTION, RECOVERY AND TEST

White Paper

January 10, 2010
Version 1.0

This White Paper Describes the Power Failure Protection Technology Integrated in the Fortasa Solid State Drive and Module Products

Please Contact Fortasa Sales for Any Additional Technical Information About Fortasa Products

4151 Middlefield Road
2nd Floor
Palo Alto, CA 94303 USA
888-367-8588
www.fortasa.com

Power Failure Recovery

Overview

Electronic systems are often vulnerable to power disruptions. Voltage spikes, brownouts, surges, blackouts and other power supply fluctuations destabilize system operation with typically unpredictable results. In general, once a power disruption is detected, a system is reset to revert back to an expected and default condition.

The same is not true with the memory systems. Since the memory system could be in the modification process during the power disruption, not only can the user data be changed during the power spike, but more importantly, the reset default condition may be corrupted and destroyed. In such catastrophic event of system file corruption the memory system information could be completely unrecoverable and the whole electronic system would become non-functional.

Therefore it’s of ultimate importance to properly design and thoroughly test the memory system response to the power disruption to prevent user data corruption and more importantly corruption of the default system conditions.

Fortasa Memory Systems products have integrated robust technical features to detect power disruption, prevent damage to the stored data and gracefully recover to a predictable condition after a power failure. Complementing Fortasa’s power recovery technology with the proper host system design techniques would practically eliminate the risk of memory system damage due to power disturbance. And finally, combining the advanced embedded protection technology inside the storage system with additional host system power protection design techniques and verifying reliable operation through extensive system level comprehensive pre-production tests would guaranty the most reliable product operation in the most critical end-applications.

Background

It’s universally accepted that Solid State Drives are an order of magnitude more reliable than conventional Hard Disk Drives. By eliminating all mechanical components, magnetic disks and read heads, solid state drives can withstand significantly higher levels of shock and vibration and work reliably at wider temperature ranges. As an added benefit, the cost for NAND Flash components has been reduced at a rate of almost 50%/year for the last 10 years, making solid state drives not only most reliable but also cost effective storage choice for embedded applications.

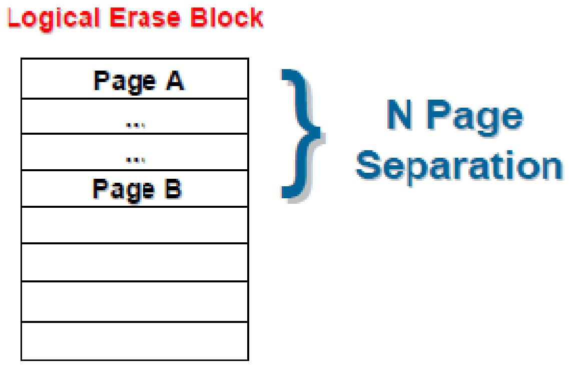
Flash Memory Basics

NAND Flash memory is the base storage medium of the Solid State Drives. A Flash memory cell works on the principle that there is a distinguishable stored charge inside the cell which corresponds to either a programmed or erased condition. A peripheral circuitry can check the status of the cell (read) and determine which state the cell is in. The greater the difference between the erased and programmed condition the easier it's to distinguish the cell state.

During a Flash program operation, the logic circuit pumps electrical charge into the memory cell raising the charge level to a distinguishable condition corresponding to one. During the erase operation, the charge is removed from the memory cell to the level corresponding to zero.

However, if a power disruption occurs during the cell charge or discharge operation, the cell could be left in an opposite or even more dangerously undistinguishable state. What makes this single cell failure truly catastrophic is the fact that NAND Flash memory architecture allows, multiple cells, called page, to be programmed concurrently. While this architectural advancement increases the programming throughput, it creates gross vulnerability for data integrity in case of power disruption.

The issue of power disruption during cell program or erase operation is exacerbated when using Multi Level Cell Flash (MLC) memory. The physical architecture of MLC Flash is that two different pages which could be non-contiguous (separated) share the same memory cell. As an illustration, if a program operation on page A in an MLC device is interrupted another page B could also be affected by the program interruption. The relative location of the paired page B may vary in the same device and also from manufacturer to manufacturer.



Page A and Page B share the same physical cells

Flash Controller Basics

To overcome the vulnerability of Flash memory to power glitches, memory system designers have utilized advanced memory management techniques. The most frequently used technique involves usage of Error Correction Code (**ECC)** to detect the failure and correct the data. The ECC algorithm calculates special code based on the user data and programs this code in the overhead space for each programmed page. When the data is read, the ECC algorithm verifies it against the calculated value. In case of discrepancy, the ECC algorithm can correct the read data (within certain statistical limitation) based on the stored special code. Depending on specific product specification, Fortasa Memory Systems solutions offer ECC correction capability substantially greater than is recommended by the Flash memory suppliers. This "safety measure" can correct upto 99% of data corruptions in a typical application.

However, in a small number of cases the number of affected bits within a programming page is so large, that is not able to be corrected by an ECC algorithm. This case is called an uncorrectable failure and if not considered properly during the electronic system design, can have grave consequences.

Corruption Mechanism

During the typical operation, data is accessed by the host through either a read or write command to the memory system. The write command for Flash memory actually consists of two separate actions, an erase and subsequent program. If a power disruption occurs during a read command, then there is no disturbance to the stored information and the host system can return to the same command execution after typical system reset and recovery.

If the power disturbance occurs during an erase command execution, the block being erased might not get erased properly and during the subsequent program of this block would exhibit a program error forcing the host to reissue the same program command to a different address location. Aside from a repeat command execution, a power disturbance during an erase command would not harm the solid state drive.

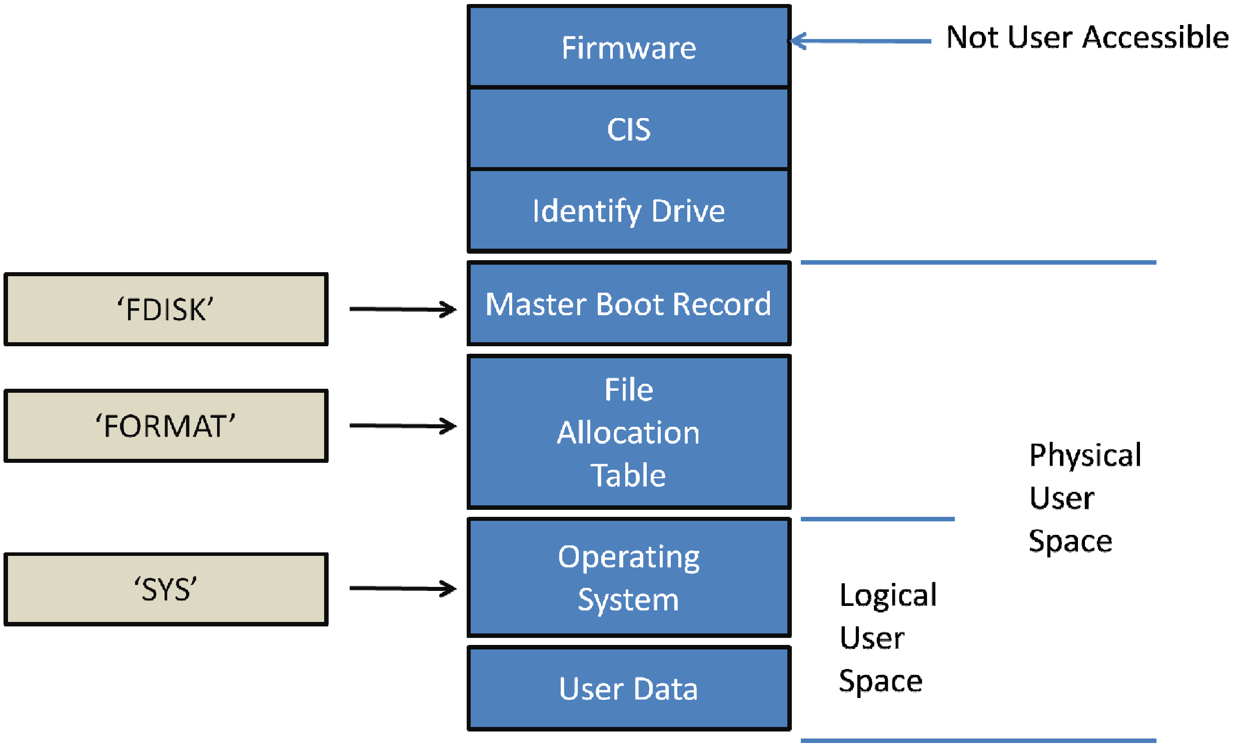
However, if a power glitch occurs during a program command the consequences can be quite severe.

Holistic Approach to Data Storage

Now that we had discussed in detail the effect that power glitches have on the storage media, it's worthwhile to look at the total storage solution from the Operating System point of view.

File System Basics

To understand the vulnerability of the storage system to the power disruptions it's important to understand the typical system file structure:



The Address space of the storage system consists of the following:

Category	Description
1. Drive Firmware	Internal Code for the Flash Controller internal operation
2. Identify Drive	Read Only Drive Specific configuration information to be read by the host to recognize the features and capabilities of the drive
3. Master Boot Record (MBR)	Drive specific record that contains partition and boot information that the system reads and interprets to address the drive
4. File Allocation Table (FAT)	A table that links discrete address locations into sequential file structure. Due to drive efficiency or fragmentation, pages can be scattered across the whole drive address space and FAT table keeps track of the sequential data locations to recreate the stored file.
5. Operating System	Critical files to enable host system operation and execution of required programs
6. User Data	Files that are most frequently updated, erased or modified.

The program command is used to either program or modify a data sector or update a FAT table that links the updated sector to the rest of the file.

Power Disruption during FAT table update

When a power disturbance occurs during the FAT table update, the information that was being programmed could become distorted and incorrect data could be stored in the programmed sector. The result of the wrong information stored in the FAT table would show up at least as a file corruption or in the worst case as a whole drive file structure being lost and unrecoverable. To prevent this catastrophic failure, Fortasa products have implemented a redundant FAT table structure which keeps a copy of the original FAT sector until an updated FAT sector is safely programmed. Only once the updated sector is verified to be correct does Fortasa’s Flash controller mark the back-up FAT sector to be erased and made available for future program. This algorithm practically eliminates any chance of FAT table corruption.

Power Disruption during Operating System or User Data Files

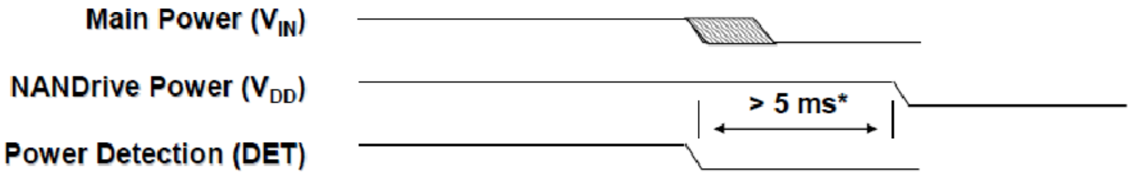
If a power glitch happens during user or system file update, it's usually difficult to detect such occurrence. Certainly, the inherent robust capabilities of the ECC algorithm dramatically reduce the risk of catastrophic or unrecoverable error, but a proper system design that considers power interruption prevention and recovery is an additional measure to prevent failure.

System Level Considerations to Avoid Program Failures due to Power Interruptions

There are multiple methods that the systems designer can utilize to dramatically reduce the risk of power interrupt caused failures.

Hardware Methods

1) *Consider to use a Super Capacitor as a Reserve source of power to complete the last program command*
Fortasa Products typically require ~5ms of reserve power to the drive to complete the NAND max program time, control signal propagation delay and queuing.



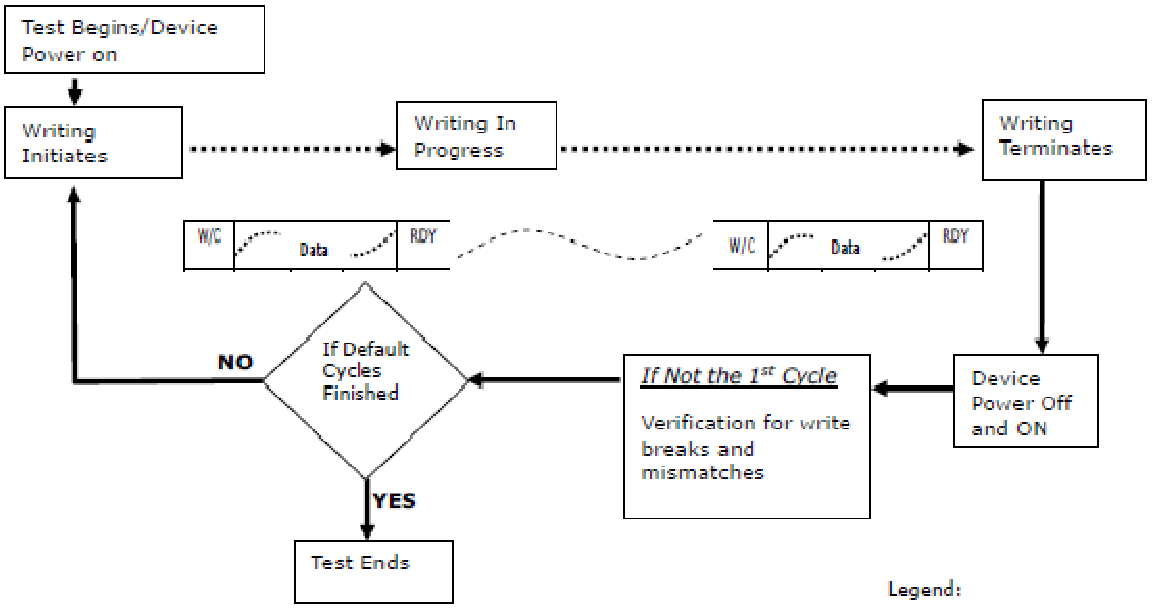
The additional energy of the Super Capacitor will allow the current program operation to be completed and verified. This will guaranty that a power glitch didn't disturb the cell and cause unrecoverable condition.

Software Methods:

1) *Follow ATA Spec and wait for command completion before starting the next command*
Frequently, designers issue multiple sequential ATA commands into the queue to gain additional performance improvement. In this situation, a power fluctuation would erase the queue form non volatile cache rendering the system incapable of knowing at which command the failure occurred and what command needs to be repeated. Issuing a single ATA command at a time, would enable the host to track the executed command sequence and be able to repeat the last command in case of failure.

Power Cycle Verification Test

To ensure that there are no hidden background program operations that could jeopardize written data, Fortasa has included a detailed and comprehensive testing procedure as part of product production release. This test verifies all Fortasa's Solid State Storage products for post write completion and data integrity..



Flow Chart of Power Cycle Test

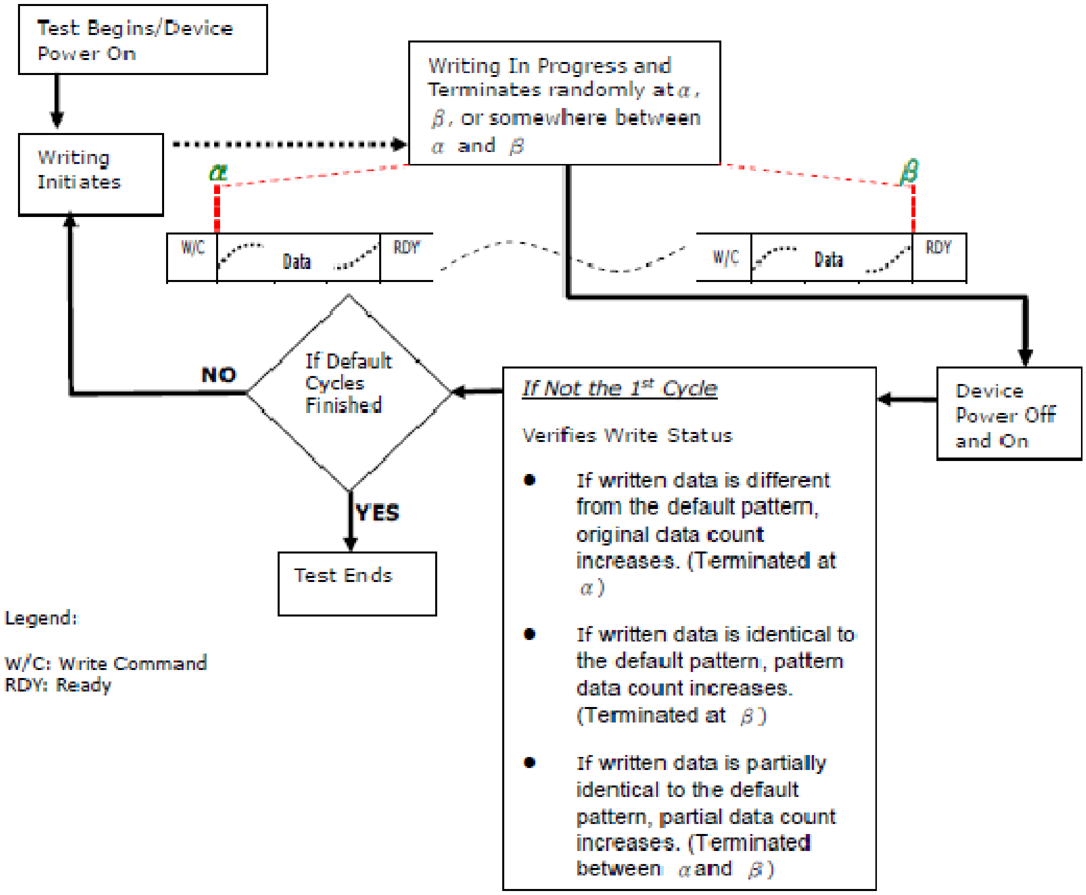
Legend:

W/C: Write Command
RDY: Ready

This test ensures that there is no additional background writes to the system once the write operation is completed and the full data cache has been properly flushed.

Power Interruption Failure Test

To ensure resiliency for all Fortasa to Power Supply Interruptions, Fortasa has included additional detailed and comprehensive testing procedure for Power Cycling as part of product production release. This test verifies all Fortasa's Solid State Storage products on their abilities to recover information when power is cycled and interrupted under specific and random conditions.


Test Begins/Device Power On
Writing Initiates
Writing In Progress and Terminates randomly at α, β, or somewhere between α and β
α
β
W/C
Data
RDY
W/C
Data
RDY
If Default Cycles Finished
NO
YES
Test Ends
Device Power Off and On
If Not the 1st Cycle
Verifies Write Status
If written data is different from the default pattern, original data count increases. (Terminated at α)
If written data is identical to the default pattern, pattern data count increases. (Terminated at β)
If written data is partially identical to the default pattern, partial data count increases. (Terminated between α and β)
Legend:
W/C: Write Command
RDY: Ready

Flow Chart of Power Failure Test

In this test the power interruption can randomly occur during either the data or file structure program cycle. This test makes sure that the system and data structure can be recovered under any Power Cycling condition. .

Conclusion

Fortasa Memory System Products contain the most advanced Power Interruption protection technology making sure that most critical data such as Master Boot Record and FAT Table remain uncorrupted regardless of the condition and duration of the Power Interruption event. As part of our product release procedure, we exercise all our new designs under a comprehensive power interruption stress test. This test is performed under the full temperature range and all operating voltage corners to guaranty superior handling of power interruptions. In addition, by following the described best practices design techniques by the host designer would practically eliminate any potential issue relating to a power supply glitch.

Revision History

Revision	Date	Description	Comments
1.0	01/10/2009	Initial Release	