The Art of SSD Power Fail Protection
White Paper

WD® SiliconDrive® Technologies Protect Critical Areas of the Drive

Introduction
The embedded systems industry is one of the earliest adopters of solid state storage technology, because solid state drives are better suited than mechanical hard disk drives to environmentally rugged applications. These applications are often subject to extreme temperatures, shock and vibration, and less-than-ideal power conditions. Among these challenges, unplanned power interruptions present perhaps the greatest risk to embedded computing systems. When power is lost during system operation, drives can be corrupted and data ruined, resulting in downtime as drives must be reformatted, operating systems reinstalled, or products returned. This directly impacts overall reliability, dependability, customer goodwill, and total cost of ownership.

Power fail protection is a differentiator for embedded SSDs, and many vendors tout solutions. However, developing effective power fail protection is as much an art as it is a science, and is not a trivial endeavor.

Differences Between Embedded and Client SSDs
What are embedded SSDs and how are they different from the low cost client SSDs that are found in notebooks? In general, the biggest difference is that embedded SSDs are designed with reliability as the top priority, while client SSDs are designed primarily for low cost. This is driven by the primary concerns of the different markets they serve. Embedded systems typically operate 24/7, have long product deployments, and often operate in harsh environments with exposure to extreme temperatures. Client systems such as notebook PCs and tablets target cost-sensitive consumers, and typically become obsolete in 3 years (or less). For the SSD manufacturer, these contrasting requirements determine the type of NAND (SLC vs. MLC) used and features supported.

The type of NAND is the largest factor that affects product cost and service life of an SSD. SLC NAND can have 10-20 times the endurance of MLC, but at roughly 2-4 times the cost. SLC can also safely operate at a wider temperature range than MLC. For that reason, MLC is more applicable for consumer products, while SLC is preferred in mission-critical applications. For more information about NAND endurance, please see WD white paper “NAND Evolution and its Effects on SSD Useable Life.”

Perhaps not so apparent is the additional technology that is needed to produce a high quality and reliable SSD for embedded systems. The strength of error correction, wear leveling, and flash management algorithms are important components and will vary among vendors. However, these algorithms are often proprietary and cannot be compared through product specifications. Often, the best method of comparison is through thorough testing.

Power fail protection technology is undoubtedly one of the most important added features and is a significant differentiator in embedded SSDs. For some SSD vendors, this merely means adding a power hold-up circuit to a client SSD product. This simplistic approach may be sufficient for typical operation in a desktop PC, but it is not in most embedded systems. End users have found that these client SSD products can be easily “bricked” with more aggressive power cycling which uncovers firmware algorithm flaws that cannot be masked by merely adding power hold-up circuitry. Firmware flaws related to wear-leveling or other important NAND management tasks can be exposed when power is lost in the midst of these background operations. Ultimately, many SSD vendors are forced to push out firmware updates (sometimes with multiple iterations) to address these issues, with varying degrees of success.

Truly rugged SSDs must be engineered at the firmware architecture level specifically to withstand aggressive power cycling. Thoughtful consideration on how to protect the critical pieces of the drive firmware as well as the user data must occur at early stages of drive design.
The Art of SSD Power Fail Protection

The Role of Write Caching (Buffering)

Like mechanical hard disk drives, many SSDs use volatile memory as a write cache to improve write performance. When enabled, “write back caching” allows the drive to acknowledge to the host the completion of a write command, although the data may still be “in-flight” within the write buffer and not yet committed to the flash media. If the power fails at this point, the data is lost. Subsequently, when the host tries to access this data, the drive will return incomplete or incorrect “corrupted” data. In SSDs that use a write cache, this would seem to be the greatest vulnerability.

There are two main ways to mitigate the risk from caching:

1. **Power holdup** – Many SSDs include a capacitive holdup circuit or “super-capacitor” as the drive’s power fail protection. With the use of a holdup circuit, the drive controller should have enough time to immediately flush the data in its buffer to the media.

2. **Disable write back caching** – The drive will wait until all data in its buffer is committed to the media before acknowledging write completion to the host.

There are tradeoffs between the two approaches. The cost of including a power holdup circuit can be significant, and may decrease the drive’s long term reliability in high temperature environments. On the other hand, disabling write back caching can significantly reduce the write performance of the drive, depending upon workload.

Mapping Table

Losing data in volatile memory (i.e., write buffer) from a power interruption is an obvious area of concern within an SSD, and is what most vendors focus on for power fail protection. However, more important is the internal mapping table of the drive firmware, in which the SSD “maps” logical block addresses accessed by the host OS to different physical pages in the NAND flash. Rebuilding the mapping table is one of the first tasks of an SSD controller upon drive power up, and every write or wear-level operation can result in an update to the mapping table. Therefore, power cycling in the middle of a mapping table update can cause corruption which renders user data incorrect (a miscompare or “silent corruption”), inaccessible, or it can even leave the drive inoperable and unusable by the user.

Client SSDs may take measures such as error correction and partitioning to protect the mapping table, but what is sometimes overlooked is how to recover in more aggressive situations such as if the power fails multiple times during the rebuild of the mapping table from a previous power cycle. This must be thoughtfully architected into the firmware, through various methods such as redundancy and data striping. Then, the drive must be thoroughly tested.

Validation Testing

Any system is only as good as the strength of its testing. Perhaps the most important piece of building a reliable SSD is comprehensive and exhaustive validation testing. The art is in devising tests for the nearly limitless number of failure scenarios that could occur, including obscure and unexpected corner cases. The depth of this knowledge comes only from decades of experience in engineering reliable storage products. Due to time-to-market pressures or lack of resources, this is where many SSD vendors fall short.

The varied applications in the embedded market expose their storage products to many forms of power disruption and interference that can cause voltage spikes, brown outs, and complete loss of system power. Emulating these situations requires testing at both the system level and at the drive level to take into account different powerdown ramp rates. The steeper the ramp, the faster the voltage falls below the NAND’s minimum programming voltage – which results in a greater chance for error.
Effective power cycle testing should also incorporate what WD calls “asynchronous power cycling”, in which power may be interrupted at any time during a write command. These tests should track the last command accepted by the drive before power is lost, so every last sector of data can be verified against the intended write. Combined with methods to verify user data elsewhere on the drive, both critical and “silent corruption” failures can be detected during testing.

WD employs its internal FIT™ (Functional Integrity Test) Lab, with hundreds of systems and thousands of test script combinations including asynchronous power cycling, to wring out as many potential areas of failure as possible. Continuously refined and improved over the years, WD’s FIT testing for embedded SSDs incorporates as many real customer embedded systems as possible.

**WD PowerArmor® Technology**

Since 2005, WD has shipped millions of WD SiliconDrives with WD PowerArmor technology that is field proven in mission-critical application installations around the world – in telecommunication routers, network infrastructure systems, wireless base stations, and industrial computers, where failure is not an option. WD PowerArmor for WD SiliconDrive CF products is described in the groundbreaking WD White Paper “Eliminating Drive Corruption from Power Disturbances.”

WD SiliconDrive A100 SATA solid state drives for embedded applications are available in two tiers of power fail protection, WD PowerArmor and WD PowerProtect™. All WD SiliconDrive U100 eUSB solid state drives are available with WD PowerArmor.

WD PowerArmor is the best protection available, combining voltage detection logic with proprietary firmware algorithms to protect the drive firmware, mapping table, and existing user data. WD SiliconDrive A100 and U100 with WD PowerArmor also protect all in-flight data, up to and including the last accepted write issued by the host. Every WD SiliconDrive with WD PowerArmor product must pass tens of thousands of continuous random power cycles at the drive level as well as system level before it goes into production.

WD SiliconDrive A100 with WD PowerProtect provides excellent protection in the majority of system environments and a moderate write performance improvement over WD PowerArmor. WD PowerProtect uses the same sophisticated firmware algorithms used in WD PowerArmor to protect the critical areas of the drive including firmware, mapping table, and existing user data, but in-flight data may be discarded during a power loss. WD SiliconDrive with WD PowerProtect products are validated through tens of thousands of continuous power cycles at the system level.

WD PowerArmor and WD PowerProtect are validated for all capacities, supply voltages, and form factors in a product family, as each combination may have distinct characteristics.

**Conclusion**

There are a myriad of choices for SATA and USB SSD products today from a multitude of vendors, with many touting some form of power failure protection. However, not all SSDs are created equal, and developing effective power fail protection is as much an art as it is a science. WD pioneered the concept of integrated power down protection in SSDs with patented WD PowerArmor technology in its WD SiliconDrive products, and continues to lead the industry with the most robust embedded SSDs.

For more information, please contact your WD Field Applications Engineer.

For service and literature:
http://support.wd.com
www.wd.com
800.494.4WD (800.275.4902)
800.692.4776
+800.6038.6008
00800.27549538
+31.880052100
North America
Spanish
Asia Pacific
Europe
(toll free where available)