Apacer

Data Defender

White Paper

March 18, 2021

Version 3.0

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

1. Introduction 2

1.1 How Unexpected Power Losses Occur 3

2. Power Failure Management 5

2.1 Layer I – Firmware Protection 5

2.2 Layer II – Mapping Table Protection 6

2.3 Layer III – Last Write Protection 7

3. DataDefender™ – Power Loss Data Protection 8

3.1 What is DataDefender™ and How Does It Work? 8

4. Conclusion 9

1. Introduction

In recent years, solid state drives (SSDs) have been adopted by a wide variety of electronic manufacturers. In addition to higher data transmission speeds and reliability when compared to traditional hard disk drives, SSDs tend to generate less heat during operation. Recent value-adding features have created SSDs that can function in high and low temperatures, or even when subjected to intense shock and vibration. It’s no wonder that they’ve been adapted for use in enterprise, networking, consumer, embedded, industrial and defense applications.

Despite their advantages, SSDs, like other electronic devices, are vulnerable to power failure issues, such as voltage disruptions, power supply fluctuations, or surges. If an SSD’s data is already written to the NAND flash, it’s secure – but data not yet stored can be ‘tangled,’ or corrupted, due to unpredictable power failures during the read-write process. Inconsistent data may not load successfully, which may lead to ECC (Error Correcting Code) errors and data loss. Power instability can also lead to problems related to mapping table damage or page/block data corruption.

As part of an SSD’s standard operation, data must be cached into RAM as illustrated in Figure 1-1.

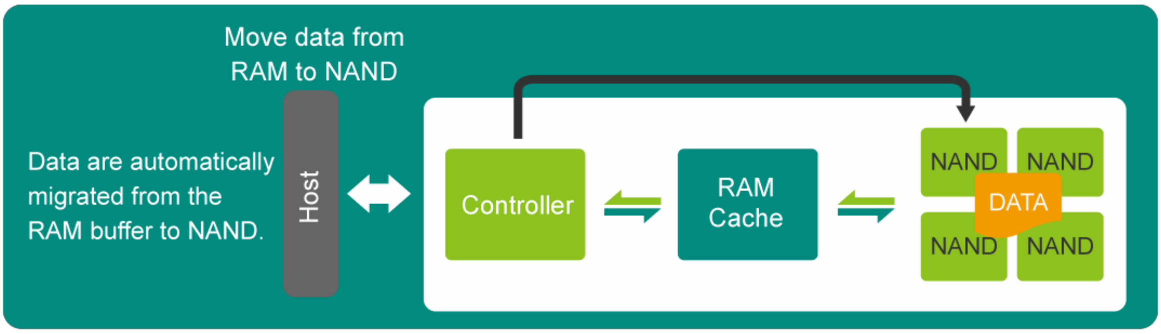

Move data from RAM to NAND
Data are automatically migrated from the RAM buffer to NAND.
Host
Controller
RAM Cache
NAND
NAND
DATA
NAND
NAND

Figure 1-1 Data transmission during stable power supply

When power is unexpectedly lost, data kept in the volatile RAM is at risk, as illustrated in Figure 1-2.

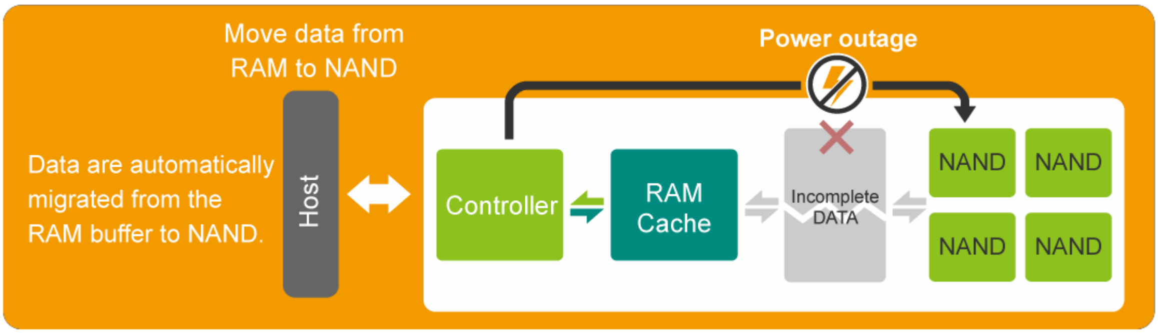


Figure 1-2 Imperfect data transmission during power failure

Therefore, to prevent data loss or drive corruption caused by power failures, it is necessary to equip SSDs with a solid data retention mechanism which enables the drives to check for all uncompleted operations and rectify them if needed.

1.1 How Unexpected Power Losses Occur

There are two primary drivers that lead to unexpected power losses.

The first is natural causes. This includes natural disasters such as earthquakes, wildfires or landslides. Under such conditions, the power generation in a certain area may be knocked out by the natural disaster, or preemptively taken offline by the administrators. And even if power generation is not affected, the transmission network that delivers power to manufacturers may be disrupted. Power lines may be knocked down, or transmission stations taken offline. In many parts of the world involved in manufacturing, events like these are thankfully rare.

However, the second cause of unexpected power losses remains a very real threat. This is interruptions of power due to human operator decisions. One example of this might be in a casino gambling operation. A system of gaming machines might be connected to a single power source, and the games enjoyed by customers during the normal hours of operation. The gaming machines might be installed and maintained by highly trained engineers. But at the end of the working day, as part of the closing procedure for the casino, a low-level employee might shut down the gaming machines by flipping a switch that disables their single power source. Depending on how the system is configured, this may also cause power surges to some of the connected gaming machines.

Due to a lack of technical knowledge by this employee, the gaming machines could be subject to unnecessary wear and tear as well as data loss or corruption due to this unexpected power loss happening at the end of each working day.

The manufacturer of the gaming machines in this example may find that the SSDs they installed in their machines are riddled with corrupted data, and the cause may not be clear, especially if their testing process before manufacturing only subjected gaming machines to controlled soft shutdowns. Luckily, a solution to this problem has been found. DataDefender™ is designed to prevent data corruption in the case of unexpected power loss, whether the cause of that loss is natural or human.

2. Power Failure Management

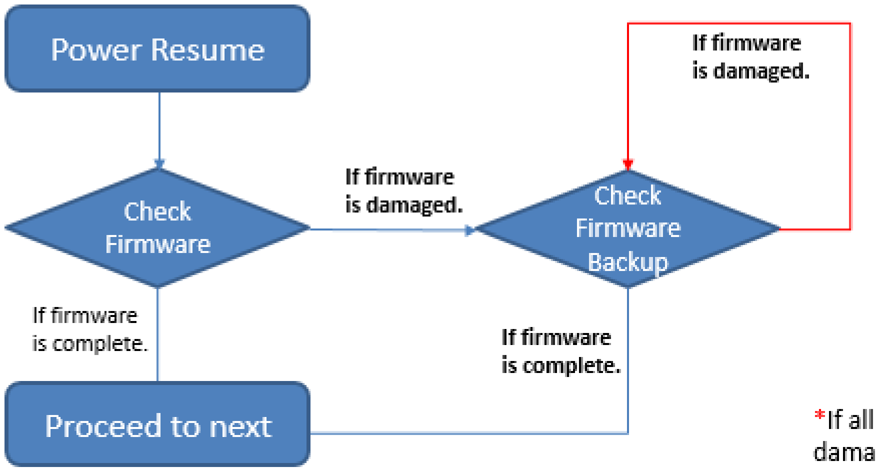
SSDs may be physically robust compared to HDDs, but they are similarly vulnerable to abnormal power failure. If an SSD read or write operation is interrupted due to an unexpected loss of power, there can be inconsistencies in the data; it may not load successfully, and an ECC (Error Correcting Code) failure can occur, leading to data loss.

To secure data integrity on an SSD during a power failure, Apacer has developed a power-loss data protection mechanism which incorporates the following three layers of power failure protection against data loss in the order of technological level:

Security Level	Layer	Description of Power Failure Protection
Less Secured ↓ **More Secured**	I	Multiple firmware backups for firmware protection
	II	Mapping table constantly updated to ensure mapping table protection
	III	Last-minute data written to NAND flash for last write protection

2.1 Layer I – Firmware Protection

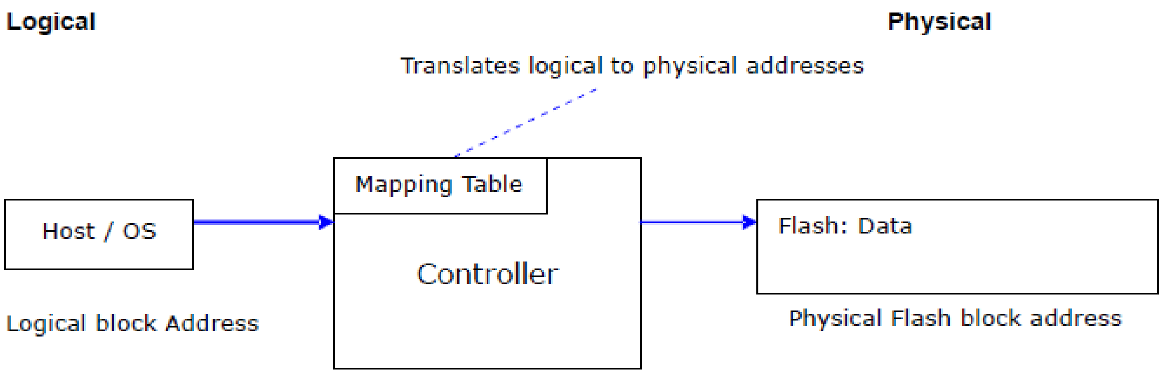
In the event of an unexpected power outage, firmware in SSDs is exposed to the risk of being corrupted, which can cause the drives to enter boot code stage. To prevent firmware from being damaged, Apacer's underlying layer of protection mechanism allows the drive to back up multiple firmware versions. Once the primary firmware is corrupted, other backup version will take over to keep the drive working properly.



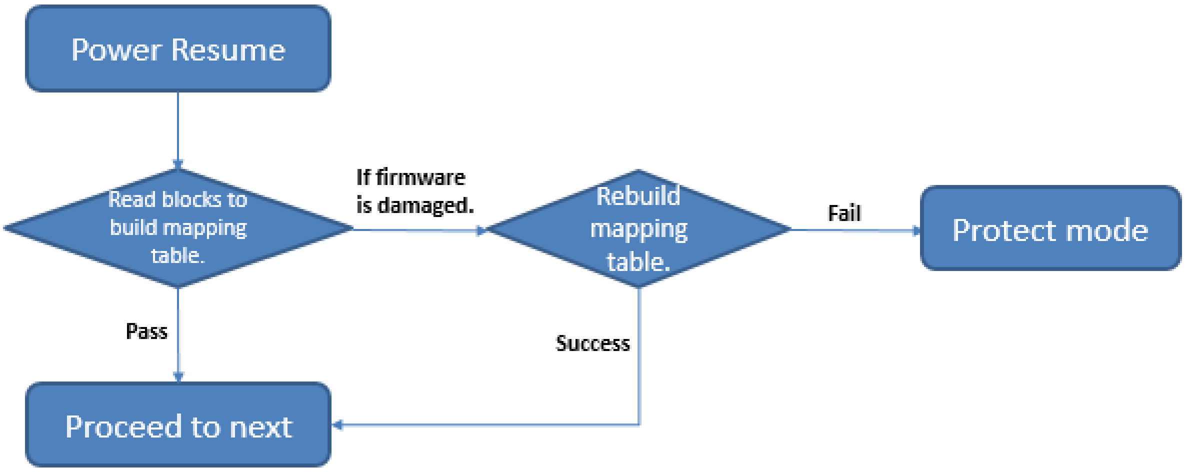
*If all backups are damaged, the drive would enter protected mode

2.2 Layer II – Mapping Table Protection

A mapping table is a built-in block inside the controller that provides logic to physical address translation. While the data is under programming process, the controller is also recording the corresponding logical block address into its mapping table.

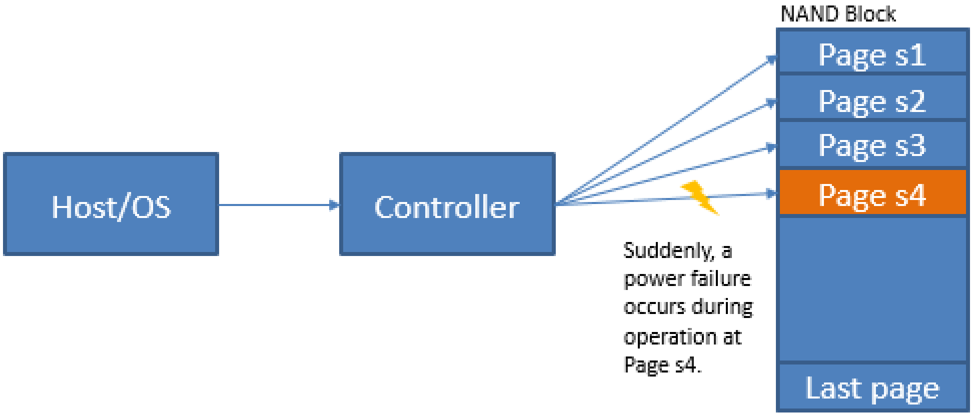


In an unexpected power outage, mapping information processed by a mapping table is at great risk. It is because mapping information of the mapping table is temporarily cached in the controller and becomes “solid” or “hardened” information once moved to flash memory. In other words, mapping information can be lost if a power failure occurs before it is flushed into the physical blocks. When power is down, the controller will read every NAND flash block in sequence and retrieve the logical address mapping to rebuild the mapping table as soon as the power supply is resumed. If the mapping table is not successfully rebuilt in the initial reading, the controller will keep reading block address information until the mapping table is recovered.



2.3 Layer III – Last Write Protection

NAND flash programming is usually divided into multiple write operations and each is written to a page of a block. As illustrated below, the write operation is carried out one page at a time in most NAND flash devices. If a sudden power failure occurs during the programming, the page with programming-in-progress data will be found invalid and with error. For instance, in the following illustration, the host is performing write operations to a NAND block. Suddenly, power goes off while page s4 is being programmed. Data written by the previous program operations on page s1, s2, and s3 can be retained because the data has already been written into the flash chips during programming operation. However, data in page s4 is invalid with error when the power resumes. The ECC in firmware will detect and correct the error in page s4 to ensure data integrity of the entire block.



3. DataDefender™ – Power Loss Data Protection

3.1 What is DataDefender™ and How Does It Work?

The DataDefender™ technology incorporates simultaneous approaches to data protection. The key element is a low voltage detector. This is paired with firmware protection, which includes mapping table reconstruction.

When an unexpected power failure occurs, the low voltage detector will be triggered. When this happens, the SSD's protection mechanism is activated and cuts off data transmission from the host. Once power supply is resumed, the firmware protection mechanism will ensure the integrity of the firmware as well as the data already written into the NAND flash media, as described in section 2. The low voltage detector and the firmware protection mechanism, working together, can protect written data and the firmware itself.

DataDefender™ represents a deeper level of protection than Power Failure Management technology can offer on its own.

4. Conclusion

Power loss protection is a critical element in data integrity. This is especially true for SSDs designed with a volatile RAM cache, because data can be lost if a power outage occurs before the cached data is moved into the non-volatile NAND flash. Since SSDs are often deployed in demanding environments, power disruptions may occur unexpectedly and potentially cause catastrophic damage to the data on the drive. When power fails during SSD operation, drives can be corrupted and data ruined, resulting in downtime as drives must be reformatted and operating systems reinstalled.

To ensure data integrity and the stability of data transmission in the event of power outage, Apacer developed the DataDefender™ technology, based around a low voltage detector. Apacer is dedicated to protecting data stored in SSDs — even in the event of an unexpected power loss. DataDefender™ gives our storage devices significant robustness, even in the presence of uncertain power environments. Especially for fields where data integrity is essential – such as the healthcare, defense and transportation industries – DataDefender™ is the most reliable solution.

Revision History

Revision	Description	Date
1.0	Official release	9/27/2018
2.0	- Changed technology name to DataDefender™ - Changed DRAM cache in figure 1-1 and 1-2 to RAM cache - Updated Section 2.1 by including the implementation of power detector - Changed the title of Section 2.2 to Firmware Solution - Changed the title of Section 2.2.2 to Group Page Reprogram Mechanism and updated the content - Updated Figure 2-5	10/8/2018
2.1	- Grammatical revisions and figure updates	11/8/2018
2.2	- Revised Figure 2-6 slightly.	7/1/2019
3.0	- Overhauled all content.	3/18/2021

Global Presence

Taiwan (Headquarters)

Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.

Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan

Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe

Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China

Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India

Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com