Apacer

# End-to-End Data Protection

## White Paper

**Jan. 28, 2019**

**Version 1.2**

**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

The manufacturing of NAND Flash has migrated to smaller geometries in order to lower down the $/GB ratio. This migration has made SSDs more affordable and has opened up room for consumer electronics. However, reliability has been traded off because error rates increase as less cell space is available to contain electrons. Therefore, electrons in the shrunken cell can often be disturbed, resulting in “soft errors”.

Unlike the errors caused by damaged or defective hardware, soft errors, or silent data corruption, are less predictable and locatable. They can potentially occur at any point throughout the process when data travels from the host, through the SSD controller to the NAND storage. Corruption like this is often undetected until the data is read. Serious consequences such as data errors and system downtime may occur if the errors are not found and repaired in time. With smaller NAND Flash geometries, flash memory storage makers rely heavily on ECC mechanisms to reinforce data integrity. However, there is a limit to an ECC’s effectiveness, because it does not exhibit the ability to determine the occurrence of errors throughout the process of data transmission.

As demand for data protection has grown in recent years, ensuring the integrity of data becomes paramount. ECC mechanisms alone are not enough. This is where End-to-End Data Protection comes in. Apacer has therefore launched a series of SSD products featuring this data protection technology to protect against possible corruption in NAND, SRAM, and DRAM memory, and provide two-way error detection and correction covering the whole data path between the host computer system and the internal storage media.

This white paper describes the general concept and mechanism of End-to-End Data Protection and explains the read/write flow in End-to-End Data Protection implemented in Apacer’s SSD products.

# 2. End-to-End Data Protection

End-to-End Data Protection is a feature designed into Apacer's SSD products that extends error control to cover the entire path from the host computer to the drive and back. It ensures data integrity at multiple points by adding protection information to the data in the path to enable reliable data transfers. The data protection information stays with the data from the host, through the SSD Flash controller and then to the NAND Flash media. When read, the same protection information travels the same route back and eventually returns to the host. This measure is implemented to ensure data correctness everywhere in the read/write route.

## 2.1 End-to-End Data Protection Mechanism

End-to-End Data Protection allows SSDs to identify an error occurring anywhere in the process of data transmission. The data integrity technology protects the data in transit through error-checking techniques such as CRC (Cyclic Redundancy Check) and ECC (Error Correction Code) depending on the interface in question to determine if any data mismatch appears during the transfer (see Figure 1-1).

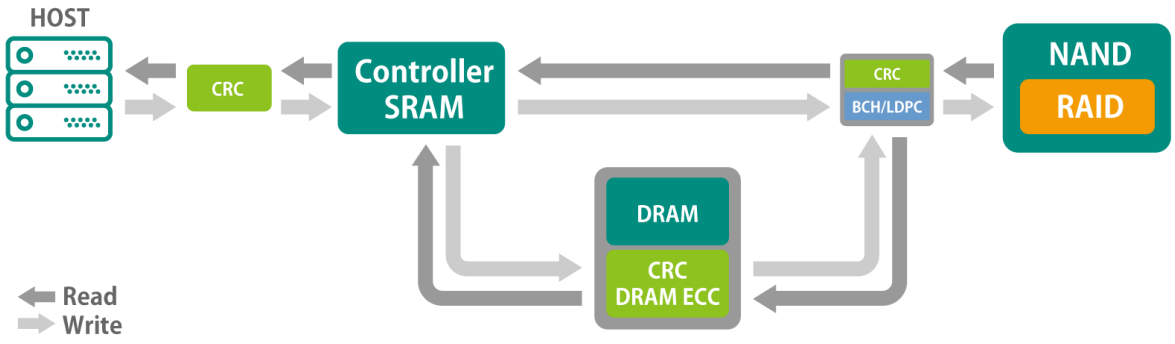


**Figure 1-1** End-to-End Data Protection flow

As a standard feature, each device in the path from computer system to drive can check and report a data error by appending CRC or ECC protection information to the data. Figure 2-1 demonstrates the End-to-End Data Protection flow and data path in which errors can be detected at any point as follows during the read/write route:

1. As data passes through intermediate devices, i.e. SRAM, DRAM, controller
2. Before the data is written to the drive media
3. When the data is read from the media
4. As the data is sent back through intermediate devices, i.e. SRAM, DRAM, controller
5. When the data arrives at the host computer

Through the implementation of error-checking methods including CRC and ECC as illustrated in Figure 2-1 to protect data during transfer, protection information allows each device along the path from the computer system to the drive to check the data is correct. When the data is read later, the same protection information returns with the data to the computer system. The protection information is used to verify the correctness of the data at multiple points in the path. If any error is detected, an immediate attempt will be made to correct it, and any uncorrectable error will be reported to the host. It is two-way security rather than one-way, which offers more comprehensive detection.

## 2.2 Read/Write Flow in End-to-End Data Protection

In addition to appending protection information to data in the computer system, Apacer SSDs employ parity generation and check functions as well as cyclic redundancy checksum (CRC), BCH encoding and checking and low density parity check (LDPC) codes to protect user data as shown below.

### 2.2.1 Write Flow in End-to-End Data Protection

As data passes from the host to the DRAM, CRC parity is generated via a CRC engine and appended to the data in the DRAM. When the data moves from the DRAM to the sector buffer, the parity is checked.

Next, the data remains accompanied by the CRC in the sector buffer. The parity is checked when the data exits the sector buffer.

After the data passes through the ECC engine, BCH or LDPC (depending on whether memory cells are stacked vertically or scaling) error correction codes are generated and stored with CRC parity in the NAND flash with the data, and then it is checked when exiting. This is shown in Figure 1-2.

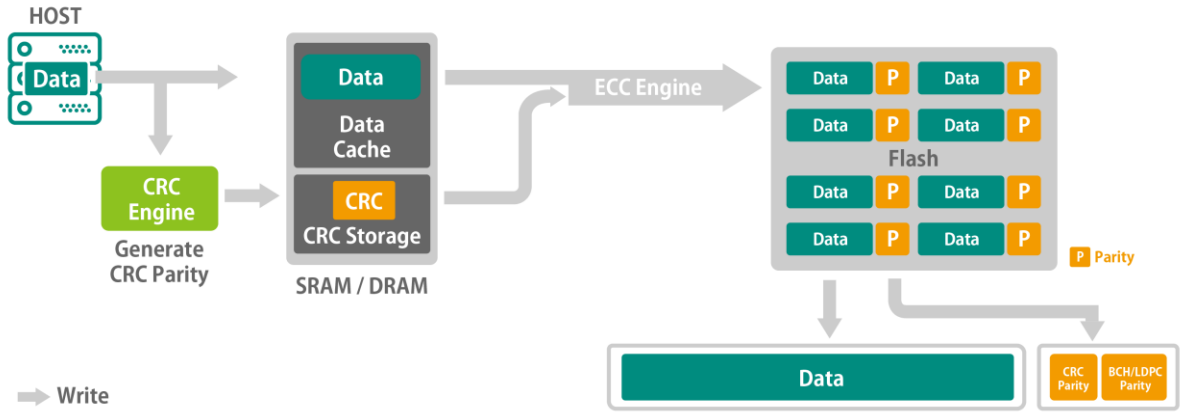


**Figure 1-2** Write flow in End-to-End Data Protection

### 2.2.2 Read Flow in End-to-End Data Protection

When data is read from the NAND, the process occurs in reverse order: BCH or LDPC (depending on whether memory cells are stacked vertically or scaling) error correction codes are attached to the data along with CRC parity as the data moves from the NAND through the ECC engine to the DRAM and are checked on exit; the CRC and BCH codes generated on write are read and verified; and finally parity is generated before the data enters the host and is checked upon exit. This is shown in Figure 1-3.

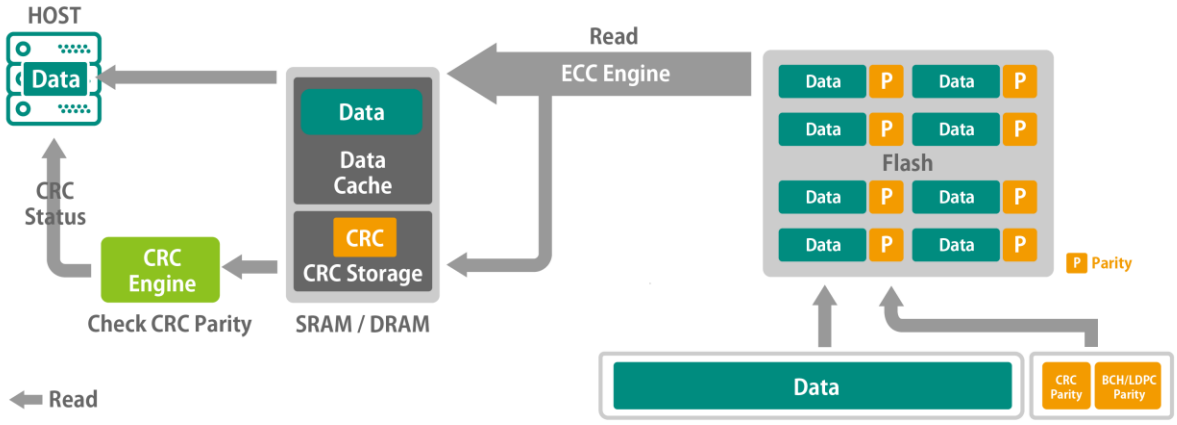


**Figure 1-3** Read flow in End-to-End Data Protection

# 3. Conclusion

Data reading, writing, and transmission from a host computer system to storage media – involving as it does a number of components, physical channels and complex software processing – may result in errors if data becomes corrupted.

To safeguard data center applications with multiple secure checkpoints providing protection from data loss and corruption and meet the rigorous demands of the SSD market for data protection, Apacer offers a robust, optimized data integrity mechanism with data protection information to detect errors along with all data that is written by establishing a highly secure connection between multiple end points. The data correction capability enables data protection for the entire system from the host computer to the drive media. Data protection for the entire system can improve system stability by protecting the system from damaged or inconsistent data to minimize downtime. This error-checking mechanism therefore enhances protection as well as the trustworthiness and reliability of the SSD.

# Revision History

| Revision | Description | Date |
|---|---|---|
| 1.0 | Official release | 5/10/2018 |
| 1.1 | Added 2.2 Read/Write Flow in End-to-End Data Protection | 9/27/2018 |
| 1.2 | Minor grammatical revisions and changes to Figure 2-1, 2-2 and 2-3. | 1/28/2019 |

# 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