AN004 - End-to-End Data Path Protection

December 2013
# Table of Contents

1. Introduction ................................................................................................................. 3

2. Error Correction and Detection ............................................................................... 4
   2.1 SAS and SATA Link 32-bit CRC ............................................................................................................ 4
   2.2 ECC Detection and Correction ............................................................................................................ 5
   2.3 F.R.A.M.E Technology .............................................................................................................................. 5

3. Summary ...................................................................................................................... 5
1. Introduction

Threats to data integrity in Solid State Drives, as in HDDs, fall into two basic categories: NAND flash memory errors (analogous to media errors in HDDs) and errors that occur to data in-flight either to or from the flash.

Errors in NAND flash consist of both correctable data errors and more catastrophic flash component failures. These correctable errors are analogous to HDD media errors and the SSD deals with them in a similar fashion. However, unlike a HDD where catastrophic failures generally result in total data loss, SanDisk SSDs incorporate additional features to recover from many of the worst NAND failure modes.

Correctable Errors: Bit errors occur fairly frequently throughout the flash array, and increase as the flash ages. These type of errors are detected and corrected on-the-fly by the controller’s Error Correction Code or ECC engine.

Uncorrectable errors: When data bit errors occur in numbers too great for the ECC engine to correct, or when NAND flash pages or blocks fail outright, an SSD’s primary data integrity capability can break down. Without additional protection against these threats, data loss is a real risk.

SanDisk SSDs feature a data fail protection scheme called “F.R.A.M.E.” (“F.R.A.M.E.” is the acronym for “Flexible Redundant Array of Memory Elements”). F.R.A.M.E. correction can recover data in situations where ECC cannot, up to and including the total loss of flash pages (consisting of multiple blocks of user data), and is able to substantially reduce the Uncorrected Bit Error Rate (UBER) risk to better than 1 in 1017bits read, exceeding JEDEC requirements JESD218.

Undetected Errors: While exceedingly rare, single bit errors can escape detection by the ECC engine. Undetected errors in this subcategory will result in incorrect data being returned to the host as good. SanDisk SSDs include additional features to protect against this category of error.

Furthermore, data in transit to/from flash memory is susceptible to soft errors due to radiation induced bit flips. Unless an SSD is also able to detect these errors, in spite of any other error protection subsystems, the integrity of mission-critical data will still be at risk. SanDisk SSD’s 32-bit Data Path CRC error detection provides protection here as well.

While all SSD designs include ECC engines, and some include Data Path CRC, few include protection for catastrophic flash memory failures. An SSD that lacks the capability to recover from an uncorrectable error, such as a page or block failure is unlikely to meet the requirements of high reliability applications. SanDisk SSDs implement protection from all three of these classes of errors, and so are highly suited for the most demanding enterprise applications.
2. Error Correction and Detection

Figure 1 shows a block diagram of the data path protection implementation for the Optimus family of SSDs.

![Figure 1: Optimus Data Path Protection](image)

Figure 2 below shows a block diagram of the data path protection implementation for the CloudSpeed family of SSDs.

![Figure 2: CloudSpeed Data Path Protection](image)

2.1 SAS and SATA Link 32-bit CRC

Data transacted on the host interface is protected by industry-standard link-level CRC. As data is received from the host by the drive, the drive calculates a 32-bit CRC checksum for the data as it is clocked in to the drive’s buffer memory. The CRC is encapsulated with the host’s data when the data is written to the flash. Errors that occur along this internal data path are detectable via both the CRC and the ECC and parity protection implemented in the buffer memory itself.

When a subsequent read of this data is performed by the host, the CRC is checked again prior to returning the data to the host (note, the drive also embeds and protects the Logical Block Address of the data with the CRC, and that LBA is also validated prior to returning data to the host). The round-trip data path CRC protects data from the moment the data is received from the host, through the flash memory (where the CRC is stored with the data), and back out to the host system. This feature adds an additional layer of error detection capability and significantly enhances the drive’s ability to guard against undetected errors arising from normal operating conditions such as ionizing radiation sources, and in extreme cases also affords protection against the limitations of ECC detection capability.
2.2 ECC Detection and Correction

While “ECC” can be (and is) used to detect errors, it also includes information that allows these errors to be corrected (CRC can only detect errors, not correct them). ECC’s ability to correct errors can be significant (meaning, multiple bits in error can be corrected, up to 100s at a time). When the host issues a read of previously written data (or when the SSD reads the data internally as part of its background data management algorithms) the data is automatically validated/corrected with the ECC HW, on the fly. For most errors, this results in the corrected data being returned to the host with no error recovery delays. However, SanDisk SSDs include an additional layer of protection designed to ensure data can be recovered even when the ECC correction span has been exceeded (see section 2.3 for more details). The ECC engine used in the SanDisk SSDs provides uncorrectable bit error rates (UBER) of 1 error per 1017 bits read, which is 10x better than the requirements specified by the JEDEC JESD218 standard, which calls out for a minimal UBER of one in 1016 bits read for Enterprise-class SSDs.

2.3 F.R.A.M.E Technology

User data is written to Flash in groups called “Super Blocks” rather than the way HDDs operate, by writing data a sector/user-block at a time. The SSD controller computes an additional layer of protection which is applied to these Super Blocks in much the same way that a HDD RAID controller does. Called “F.R.A.M.E.”, this additional data provides block-wise redundancy (versus bit-wise for ECC) and can be used to reconstruct data that cannot otherwise be recovered by the previously described features. It is even capable of recovering data in situations where the Flash device cannot return any data at all! The Optimus and CloudSpeed family of SSD’s implement support for errors up to and including full Flash Page failures. Future generation SanDisk SSDs will include the capability to recover an entire flash die!

3 Summary

Solid State Drives must protect data along all data paths and within all storage cells of the NAND flash. This includes protection from flash bit errors, catastrophic flash failures, sub-atomic particle-induced soft errors within internal SRAMs and along control and data paths, and across interfaces including the host interface and the flash memory channels.

SanDisk SSDs provide state-of-the-art error detection and correction, Data Fail Protection and the highest level of integrity for stored firmware, user data, and internal drive meta-data.

Providing overlapping data protection domains, SanDisk SSDs deliver data path protection that exceeds the JEDEC JESD218 specification for Enterprise-class SSDs by an order of magnitude.

Tradeoffs are necessary to achieve a balance between cost, reliability and operating margin. Not all SSD manufacturers have the knowledge and experience to navigate these tradeoffs correctly.
Products, samples and prototypes are subject to update and change for technological and manufacturing purposes.

SanDisk Corporation general policy does not recommend the use of its products in life support applications wherein a failure or malfunction of the product may directly threaten life or injury. Without limitation to the foregoing, SanDisk shall not be liable for any loss, injury or damage caused by its use of its products in any of the following applications:

- Special applications such as military related equipment, nuclear reactor control, and aerospace
- Control devices for automotive vehicles, train, ship and traffic equipment
- Safety system for disaster prevention and crime prevention
- Medical-related equipment including medical measurement device

Accordingly, in any use of SanDisk products in life support systems or other applications where failure could cause damage, injury or loss of life, the products should only be incorporated in systems designed with appropriate redundancy, fault tolerant or back-up features. Per SanDisk Terms and Conditions of Sale, the user of SanDisk products in life support or other such applications assumes all risk of such use and agrees to indemnify, defend and hold harmless SanDisk Corporation and its affiliates against all damages.

Security safeguards, by their nature, are capable of circumvention. SanDisk cannot, and does not, guarantee that data will not be accessed by unauthorized persons, and SanDisk disclaims any warranties to that effect to the fullest extent permitted by law.

This document and related material is for information use only and is subject to change without prior notice. SanDisk Corporation assumes no responsibility for any errors that may appear in this document or related material, nor for any damages or claims resulting from the furnishing, performance or use of this document or related material. SanDisk Corporation explicitly disclaims any express and implied warranties and indemnities of any kind that may or could be associated with this document and related material, and any user of this document or related material agrees to such disclaimer as a precondition to receipt and usage hereof. EACH USER OF THIS DOCUMENT EXPRESSLY WAIVES ALL GUARANTIES AND WARRANTIES OF ANY KIND ASSOCIATED WITH THIS DOCUMENT AND/OR RELATED MATERIALS, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR INFRINGEMENT, TOGETHER WITH ANY LIABILITY OF SANDISK CORPORATION AND ITS AFFILIATES UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR LOSS OF USE, REVENUE, OR PROFIT OR OTHER INCIDENTAL, PUNITIVE, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION PHYSICAL INJURY OR DEATH, PROPERTY DAMAGE, LOST DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrievable manner or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of an officer of SanDisk Corporation.

All parts of the SanDisk documentation are protected by copyright law and all rights are reserved.