Western Digital.

WHITE PAPER

Flash Health Monitor and Host Lock

Utilizing advanced features for your automotive and surveillance applications

Western Digital Technologies, Inc. or its affiliates' (collectively "Western Digital") general policy does not recommend the use of its products in life support applications where in a failure or malfunction of the product may directly threaten life or injury. Per Western Digital Terms and Conditions of Sale, the user of Western Digital products in life support applications assumes all risk of such use and indemnifies Western Digital against all damages.

This document is for information use only and is subject to change without prior notice. Western Digital assumes no responsibility for any errors that may appear in this document, nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

Absent a written agreement signed by Western Digital or its authorized representative to the contrary, Western Digital 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 or any product referred to herein expressly waives all guaranties and warranties of any kind associated with this document any related materials or such product, whether expressed or implied, including without limitation, any implied warranty of merchantability or fitness for a particular purpose or non-infringement. Each user of this document or any product referred to herein also expressly agrees Western Digital shall not be liable for any incidental, punitive, indirect, special, or consequential damages, including without limitation physical injury or death, property damage, lost data, loss of profits or costs of procurement of substitute goods, technology, or services, arising out of or related to this document, any related materials or any product referred to herein, regardless of whether such damages are based on tort, warranty, contract, or any other legal theory, even if advised of the possibility of such damages.

This document and its contents, including diagrams, schematics, methodology, work product, and intellectual property rights described in, associated with, or implied by this document, are the sole and exclusive property of Western Digital. No intellectual property license, express or implied, is granted by Western Digital associated with the document recipient's receipt, access and/or use of this document or the products referred to herein; Western Digital retains all rights hereto.

This document and Western Digital communications to the user associated therewith, shall be treated as Western Digital Corporation's proprietary and confidential information, protected by the recipient as such, and used by the recipient only for the purpose authorized in writing by Western Digital Corporation. This document shall be covered as Western Digital Corporation's confidential information under all applicable nondisclosure agreements between the recipient and Western Digital Corporation.

Table of Contents

1.0 Overview

NAND flash storage offers many compelling advantages for OEMs in the automobile and surveillance sectors. NAND flash is small, fast, and resilient; it performs predictably and reliably in a wide range of environmental conditions for which an increasing number of OEMs are designing solutions. With the advance of the Internet of Things (IoT), the challenges facing manufacturers go beyond choosing a storage solution by capacity alone. How do you minimize service costs associated with in-field replacement of storage systems that are at end of-life? How do you prevent the inappropriate use of data on a storage device?

Two new technologies were recently added to the Western Digital product targeting Automotive, industrial and surveillance applications:

- Health Monitor
- Host Lock

This white paper describes these two technologies, the benefits, and the best use cases for the implementation in products and environments where the health and controlling access to data is critical. You will learn how Health Monitor can reduce both the incidence of in-field storage component failure and the cost of meeting customer expectations and service levels. You will also gain a better understanding of how Host Lock can help protect your intellectual property—and your customer's personal data—from unauthorized use and duplication.

2.0 The Strengths of Flash Storage

For manufacturers in the rapidly evolving and expanding automotive and IoT industries, the advantages of NAND flash as a data storage solution are distinct. Flash comes in a variety of form factors, from embedded flash devices (EFD) in a tiny package of 11.5x13x0.8mm[1] to microSD™ and SD™ cards, USB devices and SSDs. The capacities range from 8GB to 4TB[2].

Industrial-grade flash solutions from Western Digital® are designed for use in wide range of conditions (with temperatures ranges as broad as –40°C to +105°C and high humidity). Furthermore, because flash-based products are solid-state devices with no moving parts, the performance and reliability are not compromised by most jolts, bumps and vibration. This makes flash an ideal solution for on- and off-road vehicles, and aerial and remote surveillance systems that require the utmost reliability under harsh conditions.

The process of writing data to a flash memory cell is finite. The physics involved are such that every write operation will cause a slight degradation of the flash cell itself. Consequently, data cannot be written to a flash storage cell indefinitely. One by one, individual storage cells in a flash device eventually wear out and will no longer reliably retain data.

This is a well-known and documented phenomenon. To prolong the life of the flash device, a manufacturer employs a good wear-leveling algorithm, uses a strong error correction and detection mechanism, and builds the product with enough spare blocks to allow some of the blocks to wear out over time.

When one block can no longer hold data reliably, the flash controller logically removes the block from its pool of available storage cells and swaps in one of the spare blocks to replace the worn one.

Manufacturers test their architectures for flash cell wear, and characterize the durability of a device in terms of terabytes-written (TBW). The OEM uses the TBW statistics to determine how much data can ideally be written to the device over its lifetime.

---

[1] Package size differs based on capacity.

[2] 1GB =1,000,000,000 bytes and 1TB = 1,000GB for storage capacity. Accessible user capacity less due to formatting or other factors. Capacity differs based on form factor.

3.0 Monitoring Flash Wear with Health Monitor

The integrated Health Monitor feature of Western Digital's industrial-grade flash solutions provides a method of determining the health of a flash storage device—in real time—in the field.

As previously mentioned, TBW is a good reference for a synthetic workload analysis and can be used to assign the right product to the right use case; however, there are factors that are beyond the designer's control. The most critical variable is the system overhead and how many writes are occurring for OS and applications housekeeping activities rather than storing actual data. It is of special concern in IoT environments, where the metadata can be larger than the data itself; the metadata undergoes rapid changes during system deployment. This problem is amplified due to modifications made to the implementation options. In an open system where a user or an administrator can add future software features, it can result in an additional workload on the flash that will lead to unplanned wear.

Knowing the expected endurance of a given flash device is not the same as knowing how healthy that device is at any given moment. An OEM can calculate that a device with a particular endurance rating, subjected to a predicted number of programmatic writes and erasures, should meet the needs of a particular use case for a predictable period. However, such models can prove unreliable under real-world conditions. Because of the way flash writes data to the cells, small random writes (as opposed to large-block sequential writes) can amplify the effect of cell wear and accelerate overall device wear. Different system designs and different applications will access the flash and different patterns. This real-world variability has a direct effect on the long-term health of the device, and unless you can determine the health of that device while it is in use, you cannot know for certain if the device will actually perform as expected for as long as expected.

The integrated Health Monitor feature could, at the very least, prevent the failure of a flash storage card at an inconvenient time. For example, a storage management application in a vehicle could check the health of the storage card on a routine basis. When the health report from the card reaches a certain threshold, the storage management system could prompt the "maintenance required" message to display–and proactively alert–the driver to schedule the car for maintenance at the dealership; the technician can replace the worn card before it reaches end-of-life.

In smart video and surveillance systems, the system can poll the card and receive a report on the health status, which in turn can be used to prompt for a maintenance event, thereby ensuring that there is no sudden loss of operation due to unplanned maintenance, as well as minimize the cost of maintenance activities by planning the maintenance well in advance.

In each scenario, easy access to accurate, timely information about the health of an individual storage component makes it possible for a service technician to replace a declining flash storage component before it fails. It can be replaced as part of a routine maintenance call rather an emergency operation after the device has unexpectedly failed. With better awareness of flash health in real time, you can lower maintenance costs, improve service reliability, and increase customer satisfaction.

4.0 Preventing Unauthorized Reuse of Flash-based Data

While one of the advantages of flash-based storage, particularly when delivered in an SD or microSD form factor, is the ease with which it can be removed and replaced, that ease also creates a potential point of vulnerability. The data on a removable card can be pulled from one device and inserted in another. Any data stored on the device could be copied and reused in unintended and costly ways. If you were an OEM delivering facial recognition surveillance systems, any hotel using your system to identify VIP guests as they approach the front door would not want video information copied from a microSD card and leaked. If you are an OEM designing proprietary maps for an automobile navigation system, you do not want those maps copied by unscrupulous competitors and reused without compensation.

The Host Lock feature on Western Digital's industrial flash offerings is designed to combat this kind of vulnerability. Host Lock enables a manufacturer to lock a flash storage device with both a Card Ownership Password (COP) as well as a Card Lock Password (CLP), which work together to protect a card's content. When a Western Digital flash storage device is COP- and CLP-protected, these features help prevent a host without the passwords from reading from, writing to, or erasing the device and an unauthorized user from copying data and reusing it for an illegal purpose.

5.0 Summary

The size, capacity, performance, endurance and reliability of flash storage make it an ideal solution for the storage needs of the automotive and surveillance industries. With Western Digital Health Monitoring, your customers can enjoy an uninterrupted experience of your products, because the underlying health of the storage system can be monitored in real time and managed in a way that avoids unannounced end-of-life events. Similarly, the protections afforded by Western Digital's Host Lock feature helps prevent the portability and flexibility of a flash-based storage solution from becoming costly points of vulnerability.

6.0 Contact Information

Western Digital Technologies, Inc.
951 SanDisk Drive, Milpitas, CA 95035-7933
Phone: +1-408-801-1000
Fax: +1-408-801-8657
Email: oemproducts@wdc.com

Western Digital®

Western Digital
5601 Great Oaks Parkway
San Jose, CA 95119
U.S.A.

For service and literature:
support.wdc.com
www.wdc.com
800.ASK.4WDC North America
+800.6008.6008 Asia Pacific
00800.ASK.4WDEU Europe (toll free where available)
+31.88.0062100 Europe/Middle East/Africa

August 2018