Write Once, Read Many Drives

White Paper

August 16, 2023

Version 1.0

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

When it comes to storage applications, NAND Flash drives have grown to dominate many industrial and commercial applications. But in certain fields, the nature of the NAND Flash technology can raise some questions. For example, if a drive is submitted as evidence in a trial, how can anyone be sure that the data on that drive has not been altered, revised or modified in some way?

Previously, there was no way to be totally sure. Now, Apacer has developed memory cards and USB drives based around Write Once, Read Many technology, or WORM. These WORM drives can be written to, but they cannot be erased or have written data modified in any way. This technology is not necessary for all drives, but in certain applications and fields, there will be key advantages to using WORM drives.

This write paper will explore those applications and then explain the technology behind WORM drives.

2. Why Do We Need WORM Drives?

As previously mentioned, there are certain applications where the trustworthiness of data stored on NAND Flash drives or memory cards comes into question. 20 or 30 years ago, if someone was shown a video, they would have little cause to dispute its record of reality. However, in the modern world, developments such as Deepfake technology and AI-generated content make it hard for consumers of digital information to trust what they see in front of them. Just because something is recorded as digital video doesn't mean it's true, unfortunately.

This uncertainty can be alleviated in certain applications if WORM drives are installed. For example, consider a police officer wearing a body camera. After receiving a call from a dispatcher, he arrives at a location where a crime is being committed. He activates his body camera, which records the crime in progress. He arrests the perpetrator, takes him into custody, and then deactivates the camera. Later, when the perpetrator is brought to trial, his lawyer questions the validity of the evidence captured on the body camera. "How can the jury be completely sure," he asks, "that the video footage supposedly captured by the officer's body camera has not be altered or modified in some way?" Well, if the body camera was recording onto a memory card with WORM technology, the prosecutors of the case would be able to point out that the data could not be modified once it has been written. The technology that powers the WORM drive makes this literally impossible. Therefore, the judge and jury would have little reason to question the footage recorded by the body camera on that occasion. But without that technology protecting the validity of the data, there's a chance that the judge might decide the evidence is invalid and cannot be submitted for jury consideration.

One can easily imagine other cases where the assurances about data integrity offered by WORM technology would be a major asset. Machines recording votes in an election, for example, might be considered more trustworthy if they recorded those votes onto WORM drives. In certain situations, businesses suspecting internal theft issues might choose to install WORM drives on point-of-sale machines. And in some jurisdictions, WORM technology could ensure the trustworthiness of casino gaming machine data. Customers will have to consider for themselves if their data is valuable enough to require WORM drives, or if the data will be subject to legal or other forms of scrutiny.

3. How WORM Drives Work

The technology that underpins WORM drives is based in the firmware. Apacer has an extremely experienced team of NAND Flash firmware engineers on staff, and their expertise has helped Apacer develop many innovative products over the years. So when development of WORM drives began, the engineers started with the basic functions of 2D MLC NAND Flash technology and the process of how data is written.

In a standard NAND Flash drive, there are commands that the firmware can send to the Flash memory. These commands can include writing data, erasing data, and various other functions. In WORM drives, the firmware is customized to prevent any erase commands from being sent: the firmware is instructed that such commands are illegal. Erasing or modifying data on a WORM drive is therefore impossible.

Once the writing process is complete, the following primary function of the drive will be to preserve the data in a readable state for as long as possible. The “write once” functionality of the drive means that the total P/E cycles consumed will be less than 1 percent. The drive should be stored in conditions where the temperature remains around 40 degrees Celsius. If it is stored under these conditions, the data on the drive should remain readable for up to 100 years.

The entire operational process of a WORM drive is illustrated in Figure 1-1, below.

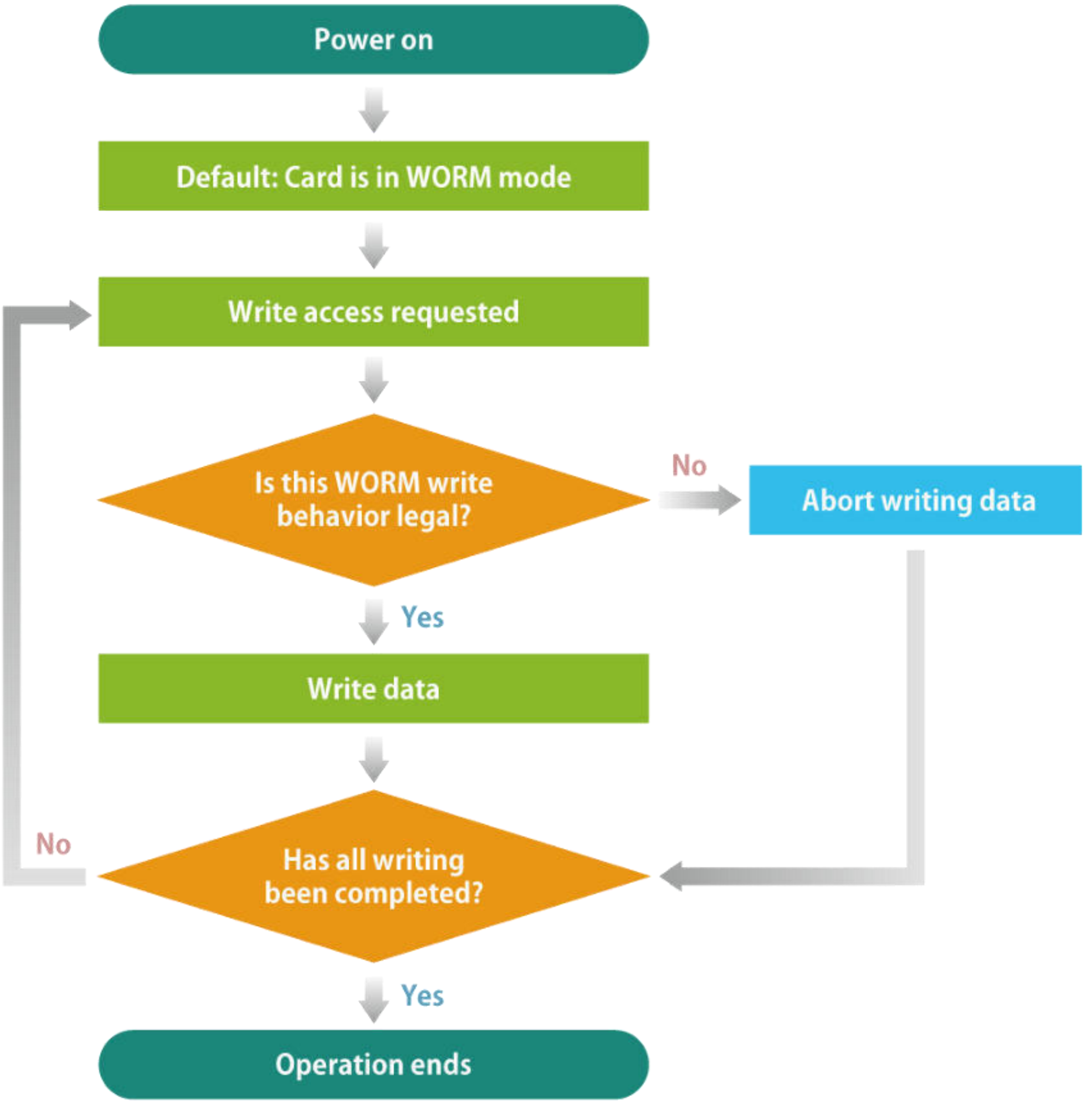
Power on
Default: Card is in WORM mode
Write access requested
Is this WORM write behavior legal?
No
Abort writing data
Yes
Write data
Has all writing been completed?
No
Yes
Operation ends

Figure 1-1: Operational Behavior of WORM Drive

4. Conclusion

When it comes to modern computing applications, trust is often in short supply. Apacer wanted to do what it could to increase the trustworthiness of data recorded on NAND Flash drives, especially those expected to be subjected to legal or governmental scrutiny. So the Write Once, Read Many technology was developed, and is now available in a variety of form factors, including both memory cards and USB drives.

It's up to the consumer to decide if their application will benefit from WORM technology. But if they choose to adopt it, WORM drives will reliably write and preserve their data, storing it carefully for whenever it may be examined for integrity.

Revision History

Revision	Description	Date
1.0	Official release	8/16/2023