

RELIABLY ERASING DATA FROM AN SSD

Reliably erasing data from storage media (sanitizing the media) is a critical component of secure data management.

Flash-based solid-state drives (SSDs) differ from hard drives in both the technology they use to store data (flash chips vs. magnetic disks) and the algorithms they use to manage and access that data. SSDs maintain a layer of indirection between the logical block addresses that computer systems use to access data and the raw flash addresses that identify physical storage. The layer of indirection enhances SSD performance and reliability by hiding the flash memory's idiosyncratic interface and managing its limited lifetime. However, it can also produce copies of the data that are invisible to the user but recoverable by a sophisticated attacker. For this reason, it is so important to sanitize the media completely.

1. WHOLE-DRIVE SANITIZATION

There are four different techniques for sanitizing an entire SSD: (Figure 1)

- Issuing a built-in sanitize command
- Repeatedly writing over the drive using normal IO operations
- Electrically destroying the drive via a high voltage generator
- Leveraging encryption

1.1 BUILT-IN SANITIZE COMMANDS

Most modern drives have built-in sanitize commands that instruct on-board firmware to run a sanitization protocol on the drive.

Traditionally, the ATA security command set specifies an "ERASE UNIT" command that erases all user-accessible areas on the drive by writing all binary zeros or ones. There is also an enhanced "ERASE UNIT ENH" command that writes a vendor-defined pattern, such as a 1MB binary file with a 0x55 content.

The ACS-2/ACS-3 specification specifies a "BLOCK ERASE" command that is part of its SANITIZE feature set. It instructs a drive to perform a block erase on all memory blocks containing user data, even if they are not user-accessible. SP Industrial SSDs support ACS-2/ACS-3 specifications to provide a 4-way interleave multiple block erase function to sanitize a whole drive effectively. For example, 1TB SSD (SP010TSSD301RW0) or pSLC 512GB SSD (SP512GISSD501RW0) can be triggered by a 5-pin Feature Connector (Table 1) to execute a 4-way Interleave Multiple Block Erase function to complete whole-drive sanitization in around 10 seconds. (Figure 2)

1.2 REPEATEDLY WRITING OVER THE DRIVE

The second sanitization method is to use normal IO commands to overwrite each logical block address on the drive. Repeated software overwrite is at the heart of many disk sanitization standards and tools. All of the standards and tools we have examined use a similar approach; they sequentially overwrite the entire drive with anywhere between 1- and 35-bit patterns. The US Air Force System Instruction 5020 is a good example; it first fills the drive with binary zeros, then binary ones, and finally an arbitrary character. The data is then read back to confirm that only the arbitrary character is present.

The varied bit patterns aim to switch as many of the physical bits on the drive as possible and, therefore, make it more difficult to recover the data via analog means. Bit patterns are potentially important for SSDs as well, but for different reasons. Since some SSDs compress data before storing it, they will write fewer bits to the flash if the data is highly compressible. This suggests that for maximum effectiveness, SSD overwrite procedures should use random data.

The complexity of SSD FTLs means that the usage history before the overwrite passes may impact the effectiveness of the technique. To account for this, we tested SSDs by writing the first pass of data either sequentially or randomly. Then, we performed 20 sequential overwrites. For the random writes, we wrote every LBA exactly once, but in a pseudo-random order.

In most cases, overwriting the entire disk twice was sufficient to sanitize the disk, regardless of the previous state of the drive. However, it takes a lot of time to complete whole-drive sanitization this way.

1.3 ELECTRICALLY DESTROYING THE DRIVE VIA A HIGH VOLTAGE GENERATOR

Degaussing is a fast and effective means of destroying hard drives, since it removes the disk's low-level formatting (along with all of the data) and damages the drive's motor. However, the mechanism that flash memories use to store data is not magnetism-based, so we do not expect the degausser to erase the flash cells directly.

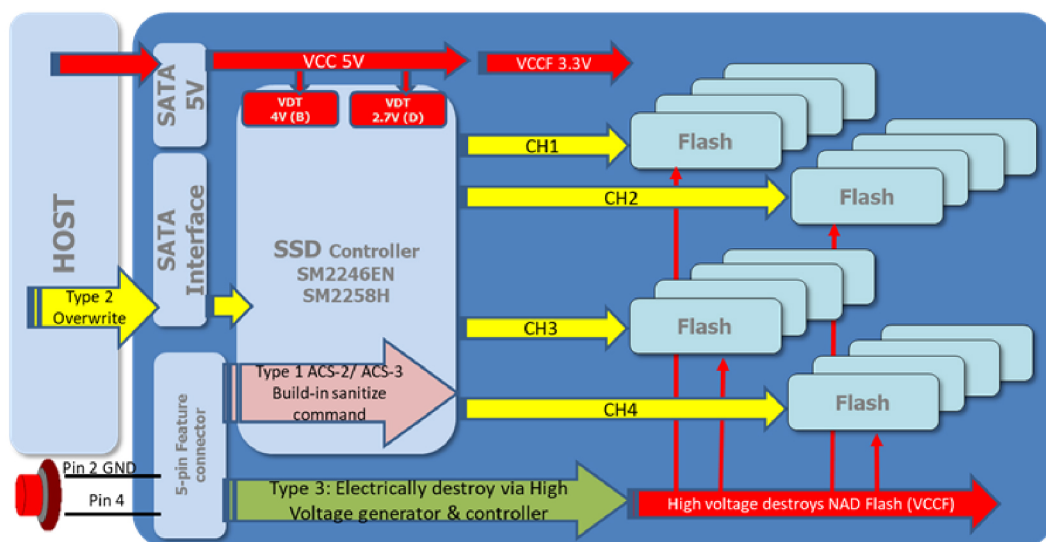
Alternatively, a special design with a high voltage generator and a controller inside the SSD can destroy NAND flash physically. However, this is not a normal design for SSDs. SP Industrial SSDs are equipped with an integrated Industrial-grade Active PMU (Power Management Unit) to provide higher reliability of power compared to traditional discrete circuits. They also feature complete protection with OVP, OCP, Surge Rejection, and In-Out Short Protection to provide a higher level of protection versus traditional fuse design. Therefore, we don't recommend implementing this technique for whole-drive sanitization.

1.4 LEVERAGING ENCRYPTION

The self-encrypting drive (SED) of SP Industrial SSDs features an AES-256 encryption engine, which provides hardware-based, secure data encryption with no SSD performance loss. This SED follows the TCG/Opal specification for trusted peripherals. The data encryption is always running; however, encryption keys are not managed and the data is not secure until either TCG/Opal or ATA security feature sets are enabled.

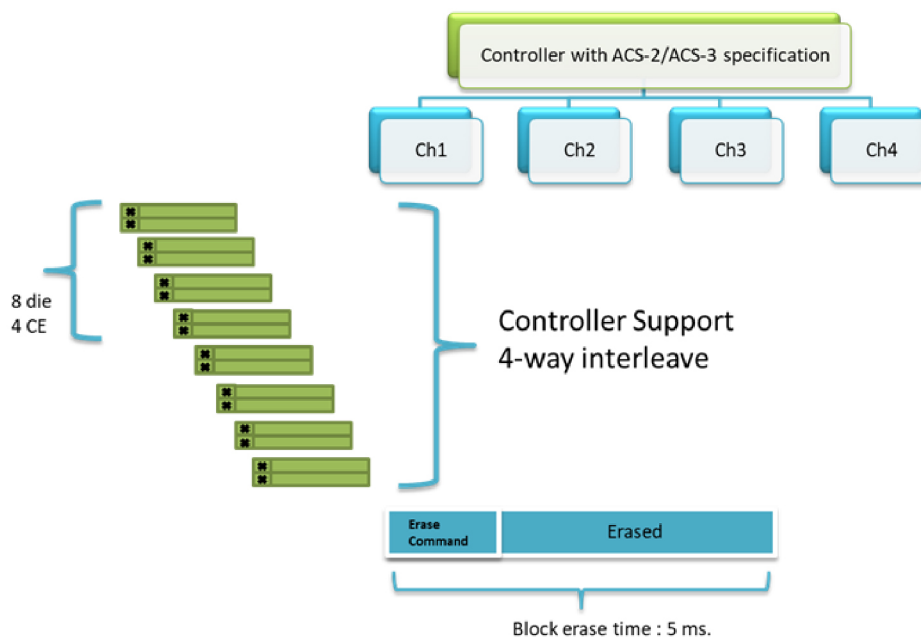
This technique is a quick means to sanitize the drive, since deleting the encryption key will, in theory, render the data on the drive irretrievable.

Figure 1 Different techniques for erasing data from SSDs



- Type 1: Built-in sanitize commands (ACS-2/ACS-3) – Short Pin4 of feature connector to trigger GPIO control pin on SM2246EN/SM2258H SSD controller to execute 4-way Interleave Multiple Block Erase function. Option available for SP Industrial 2.5" SATA III SSDs.
- Type 2: Repeatedly writing over the drive – Sequentially overwrite the whole drive to fill it with binary zeros, then binary ones, and finally an arbitrary character.
- Type 3: Electrically destroying the drive via a high voltage generator – Leverage Short Pin4 of feature connector to activate high voltage generator and controller to destroy NAND flash physically. Option available by OEM design by custom request only.

Figure 2 4-way interleave multiple block erase operation



- SP Industrial SSD 1TB SSD (SP010TSSD301RW0) or pSLC 512GB SSD (SP512GISSD501RW0) configured with 8pcs of Toshiba 15nm 2D MLC T0 BGA NAND Flash TH58TFT0DDLBA8H (8 die/4CE)
- Build-in Sanitize Commands (ACS-2/ACS-3) : Short Pin4 of feature connector to trigger GPIO control pin on SM2246EN/SM2258H SSD controller to execute 4-way Interleave Multiple Block Erase operation to initiate multiple block erase for 4 pcs of NAND flash at the same time. Controller can erase 32 Blocks simultaneous.
- Maximum Blocks per NAND flash is 32,696 blocks. Block erase time is 5 ms. Totally it takes 5.1s (32,696/32x 5ms). Repeat once for another 4pcs of NAND flash to complete whole-drive sanitization. Total Erase time is around 10 seconds

Figure 3 5-pin feature connector

Pin	Function	I/O	Function Description
1	Write Protect	input	short to GND pin to enable write protection
2	GND	n/a	system ground
3	Device activity indicator	output	connect to an LED to indicate device activity
4	Security Erase trigger	input	short to GND pin to trigger security erase function
5	Erase activity indicator	output	connect to an LED to indicate erase function activity