
Security Features for Solid State Drives in Defense Applications



Esther Spanjer
Director of Technical Marketing
Adtron Corporation

Table of Contents

1 EXECUTIVE SUMMARY	3
2 INTRODUCTION	3
3 SECURITY IN SOLID STATE DRIVES VS. HARD DISK DRIVES	4
3.1 Data Remanence in Solid State Drives	4
3.2 Data Remanence in Hard Disk Drives	5
3.3 Flash SSD Data Abstraction Layers	5
4 DATA PROTECTION	6
4.1 Hardware Write Protection	6
4.2 Software Write Protection	6
4.3 Encryption	7
5 DATA ELIMINATION	7
5.1 Security Disposition	8
5.2 IRIG 106-2007, Chapter 10.8	9
5.3 Adtron EraSure Technology	10
6 MEDIA DESTRUCTION	12
6.1 Adtron ZAP Technology	12
7 CHOOSING THE RIGHT SECURITY TECHNOLOGY	13
7.1 Data Recorder in a Helicopter	13
7.2 Data Recorder in a Tank	14
8 CONCLUSION	15
9 REFERENCES	16

1 EXECUTIVE SUMMARY

There are various methods for data protection and elimination in flash solid state drives (SSDs), depending on the security level required within each application. Security techniques can be divided into three categories:

1. Data protection
2. Data elimination
3. Media destruction

Methods of data protection include write protection, password protection and encryption. Encryption is not a technique used today in military applications, due to problems related to key management. Password protection can be used in combination with a biometric key to implement a security scheme that is based on “*what you have, what you know, who you are*”.

Data elimination is handled by Clear and Sanitize procedures. Which method needs to be implemented depends on the security classification level of the organization in which the application resides. Typically, if the device will stay within the same security classification, a Clear procedure will suffice. If it is moved to a higher security classification level, the device needs to be entirely de-classified, and a Sanitize procedure is needed. Moving the device to a lower security classification would require destruction of the drive.

Sanitizing a solid state drive is much faster and requires fewer cycles of the same procedure when compared to hard disk drives, since SSDs experience far lower levels of data remanence.

Complete media destruction can be a solution if a Sanitize procedure is too time consuming and the data needs to be eliminated and destroyed in a matter of seconds. Adtron’s ZAP technology is a unique way of destroying access to data on NAND flash chips within a solid state drive, providing the ability to destroy access on a 64GB drive in less than 5 seconds.

2 INTRODUCTION

In April 2001, a US Navy surveillance plane was intercepted by two Chinese F-8 fighter planes during a “routine” patrol flight over the Chinese South Sea [1]. The US plane was forced to make an emergency landing in China after what officials described as a “minor” mid-air collision with one of the Chinese planes.

The US crew had between 12 and 20 minutes in the air to destroy all classified material on board before making the emergency landing. In the final moments before the plane landed, the crew tried to destroy the hardware with hammers and axes. Just how much the crew was able to destroy is not public knowledge.

Figure 1: US Navy EP-3E ARIES before and after landing in China



This story illustrates the need for high-level security methods in defense systems, and in particular for the storage devices within these systems. This story is at the far end of the security spectrum; there are many systems that require lesser forms of security. For example, Commercial Off-The-Shelf (COTS) electronic

components represent a large part of the deployed military systems, whereby devices such as data recorders and ruggedized laptops that are used in training environments require a lower security implementation. Since these devices stay within the same security classification environment, fast elimination of mission data may be all that is required once a training mission has been completed. On the other hand, if the device is moved to an environment with a higher security classification, a complete Sanitize procedure per the specified Defense department standard will be required. Moving the device to an environment with a lower security classification requires complete destruction of the device.

In general, defense storage system security levels are divided into three categories:

1. Data protection
2. Data elimination
3. Media destruction

The third method would have definitely been preferred in the case of the US surveillance plane, but unfortunately the storage devices on board were not equipped with this feature.

Adtron designs and develops security functionality in accordance with commonly used military specifications. As a result of this focus, Adtron solid state drives find wide acceptance and deployment in defense applications.

This white paper discusses the various solid state drive data security methods that can be applied in defense applications and environments, and discusses Adtron's EraSure[®] technology implemented within its Flashpak[®] solid state drive product line.

3 SECURITY IN SOLID STATE DRIVES VS. HARD DISK DRIVES

Implementing security features that require data elimination or media destruction are far more complex for hard disk drives than solid state drives due to their underlying storage technology. For example, hard disk drives leave behind a much bigger "ghost-image" once data is written to them. This requires more complex and longer data elimination procedures than would be needed for solid state drives.

Media destruction in hard disk drives can only be solved by using large and bulky degaussers, physically destroying the drive, or using chemicals that render the surface of the drive unreadable. Solid state drives, on the other hand, are more suitable for media destruction, due to their underlying silicon technology. Adtron's ZAP technology is one such technique that is able to physically destroy access to the media in a matter of seconds.

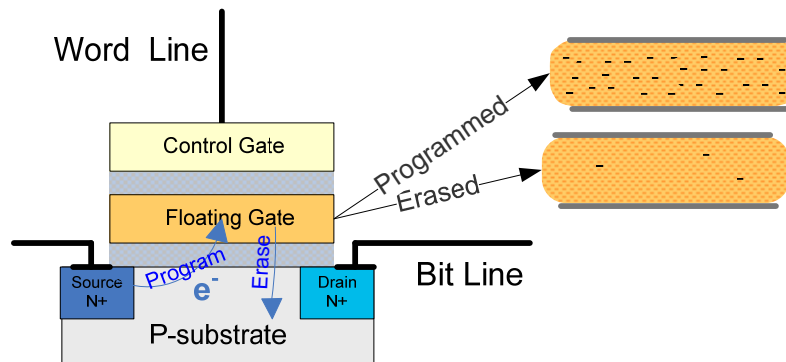
The need for complex data elimination and media destruction techniques stems from the level of data remanence of that particular storage media. Remanence is the magnetization left behind in a medium after an external magnetic field is removed [2]. The smaller the data remanence on the storage media, the more simple data elimination techniques can be implemented. The next sections review data remanence on hard disk drives and solid state drives.

3.1 Data Remanence in Solid State Drives

Solid state drives use NAND flash technology for data storage. Figure 2 below shows the internal structure of a NAND flash cell, which uses a process known as Fowler-Nordheim tunneling to change the charge inside the floating gate [3].

Writing (programming) a "0" into a cell causes the accumulation of negative charges in the floating gate. Writing a "1" into a cell does not change the cell's content. To change the content of a cell from "0" to "1", the cell must be erased in order to release the negative charges in the floating gate.

Figure 2: NAND flash cell



Data remanence in NAND flash is mainly caused by a so-called hot-carrier effect [3], where electrons get trapped in the gate oxide layer and can stay there as excess charge. The amount of trapped charge can be determined by measuring the gate-induced drain leakage current of the cell, or more indirectly by measuring the threshold voltage of the cell. The effect is more apparent in fresh cells, and becomes less noticeable after 10 program/erase cycles.

Erasing the cell will significantly reduce the amount of trapped electrons, making it extremely difficult to recover any data from the device after an erase cycle.

3.2 Data Remanence in Hard Disk Drives

When data is written to a magnetic medium, the write head sets the polarity of most, but not all, of the magnetic substrate. This is partially due to the inability of the write head to write in exactly the same location each time, and partially due to the variations in media sensitivity and field strength among devices over time [4].

When a "1" is written to a disk, the media records a "1". When a "0" is written, the media records a "0". However, the actual effect is closer to obtaining a 0.95 when a "0" is overwritten with a "1" and a 1.05 when a "1" is overwritten with a "1". Deviations of the drive head from the original track may leave significant portions of the previous data along the track edge.

Normal disk circuitry is set up so that both these values are read as "1", but using specialized tools such as a magnetic force microscope, it is possible to read what previous "layers" contained. Using these specialized tools, extracting so-called "ghost-images" becomes fairly easy.

To ensure a complete elimination of a "ghost-image" on a magnetic disk drive, two procedures can be followed:

- Degaussing the media by applying a reverse (coercive) magnetizing force in order to reduce the correlation between previous and present data to a point that there is no known technique for recovery of previous data [2].
- Overwriting the media multiple times with various patterns. A one-time erase of the media will not suffice, and military standards specify up to four Sanitize cycles of erase and pattern-overwrite. However, according to industry recommendations [4], a pattern overwrite of up to 35 times is required to completely clear previously contained data from the media.

3.3 Flash SSD Data Abstraction Layers

An additional complexity to recovering data from a solid state drive (when compared to hard disk drives) arises from the fact that solid state drives contain additional data abstraction layers. In-depth knowledge would be required of the following layers to obtain a valid picture of the extracted data:

- **File system:** Each file system has its own method of mapping files, creating pointers, and storing tables. Knowledge of this would be required for both HDD and solid state drives when data is extracted

- **Logical to physical mapping:** Flash Management Systems map the logical file system sectors to physical locations on the flash. Each solid state drive vendor implements a different flash management algorithm for mapping sectors
- **Solid State Drive architecture:** Each solid state drive vendor has a different architecture, and therefore it is hard to determine where in each flash chip a logical block address ends up
- **Flash cell architecture:** Different flash vendors have different flash cell architectures with different sequences of discrete bits

The additional data abstraction layers in a solid state drive increase the complexity of reverse engineering, making it extremely difficult to extract sensible data.

4 DATA PROTECTION

At the most basic level of data security, hardware and software applications achieve protection from viruses or hackers through write protection and password access protection. These isolate the Operating System (OS), applications, and critical data from corruption or infiltration by external sources. Write and password protecting a drive can be meaningful in applications where the end user is not allowed to tamper with the contents of the data.

4.1 Hardware Write Protection

Write protection prevents data modification on a storage device. It is typically enforced by the hardware through a jumper or switch and implemented through a hardware protection mechanism inside the controller of the SSD. In this case, a protection state machine inside the controller blocks writes to the media.

4.2 Software Write Protection

Software write protection can be implemented through the firmware of the storage device, whereby the host can set/remove the write protection via a host (vendor-unique) command to the drive.

Software password protection is suitable when implementing a security scheme that is based on “what you have, what you know, who you are” [12]. For example, when only authorized personnel are allowed to download mission data from a data recorder, a combined password protection and biometric key would provide a secure identification scheme. In this case, the password would deliver the “what you know,” and a biometric key would cover the “what you have” and “who you are.”

4.2.1 Password Protection in Flashpak Solid State Drives

The password protection feature on Flashpak solid state drives is implemented through the standard ATA command set [5], and supports both a user and master password. When used for data logging purposes, the device can be locked or unlocked at boot time when used as the boot device, or once an application is loaded.

- **Password protection during boot:** When the Flashpak solid state drive is used as the boot device, password protection is implemented in combination with the BIOS of the host system. The BIOS will need to incorporate the ATA commands that enable the usage of the password scheme. During the system boot process, the user must successfully enter a password to the system; otherwise the system will not continue booting.
- **Password protection during operation:** When the Flashpak solid state drive is used for data logging purposes, standard ATA security commands are used for locking and unlocking the device.

After 5 unsuccessful attempts of entering a password, the drive will have to be rebooted before new attempts can be made. These include both user and master password attempts.

4.3 Encryption

Another form of data protection is encryption, whereby the original data, or "plaintext," is converted into a coded equivalent called "cipher text" via an encryption algorithm. The cipher text is decoded (decrypted) at the receiving end and turned back into plaintext.

When using the most common encryption algorithms, such as RSA, AES and 3DES, it is virtually impossible to recover any data from a storage device, providing a high form of security. For example, to break an AES 128-bit encryption, a "brute-force" attack with a system that tries keys at the rate of one billion keys per second will take about 10,000,000,000,000,000,000 years to try all possible keys [6].

The main hurdle that has prevented encryption from being integrated full scale into host applications and storage devices is related to key management. Creating strong and secure keys appears to be surprisingly difficult. The challenge is that most systems are notoriously deterministic, but what is required of a good and strong key is the opposite – unpredictability and randomness. In addition, it is not a trivial matter to provide a secure method of key storage and distribution without running the risk of keys being tampered with or stolen.

In this light, no defense agency has allowed implementation of encryption methods in classified applications. Instead, other methods such as Clear and Sanitize procedures or complete media destruction are accepted forms of securing classified data.

5 DATA ELIMINATION

As the repository for data and programs, flash solid state drives are critical electronic components in a defense computing system. For this reason, all branches of the military have spent significant time and effort developing standards for what has become known as secure erase features in data storage. These standards were originally set in two documents – the Department of Defense (DoD) 5200.28 and the National Security Agency (NSA) CSS 130-2, *Media Declassification and Destruction Manual*. Other branches of the US military have created other data elimination specifications drawn from the DoD and NSA instructions.

Sanitizing or Clearing a solid state drive provides a fast means for data declassification, without the need for degaussing or disk destruction as is the case with mechanical hard disk drives. A particular advantage of these operations in solid state drives is the ability to perform the operations without having physical access to the drive as is the case with degaussing or destruction of a hard disk drive. This makes the declassification procedures quicker, easier and more cost-effective for solid state drives.

A distinction has been made between a Clear operation and a Sanitize (or Purge) operation:

- **Clear:** Clearing is the process of erasing data on the media. In a flash SSD, this is done by executing a block-by-block erase with or without verify. Adtron EraSure technology implements that block-by-block erase on physical block level vs. logical block level.
- **Sanitize** (also known as Purge): Sanitizing is the process of declassifying the drive by executing an unrecoverable removal of all data on the media. In a solid state drive, this initiates a sequence of block-by-block erase, pattern write and pattern verify operations designed to eliminate any traces of the original data. Since data remanence in solid state drives is far less prevalent, a Sanitize procedure with few repeats will not leave a "ghost-image" behind on the drive, making it impossible to recover any data that was present on the drive.

Table 1 below provides an overview of the various military standards that define how data elimination is executed on a disk drive, regardless of the underlying media.

Table 1: Security Erase Military Standards

Procedure	Standard	Action
Clear		All data on the media is erased
Sanitize/Purge	DoD 5220.22-M NISPOM	Erase the media and overwrite with single character, then erase again
Sanitize/Purge	DoD 5220.22-M NISPOM, Sup 1	Erase the media and overwrite with single character, then erase again and overwrite with single character, then erase again and overwrite with random character then erase again
Sanitize/Purge	NSA 130-2	Erase the media and overwrite with random data 2 times, then erase and overwrite with a character
Sanitize/Purge	Air Force AFSSI 5020	Erase the media and overwrite with pattern, repeat 3 times
Sanitize/Purge	USA Army 380-19 ¹	Erase the media and overwrite with random data, erase and overwrite with a character, then erase and overwrite with complement of the character
Sanitize/Purge	Navy NAVSO P-5239-26	Erase the media and overwrite with random data, then erase again
Sanitize/Purge	IRIG 106-07, Ch. 10.8	Erase the media, overwrite with 0x55, erase, overwrite with 0xAA, and then erase again. Then fill the drive with a repeating string of Secure Erase.
Fast Clear		All data on the media is erased simultaneously.

5.1 Security Disposition

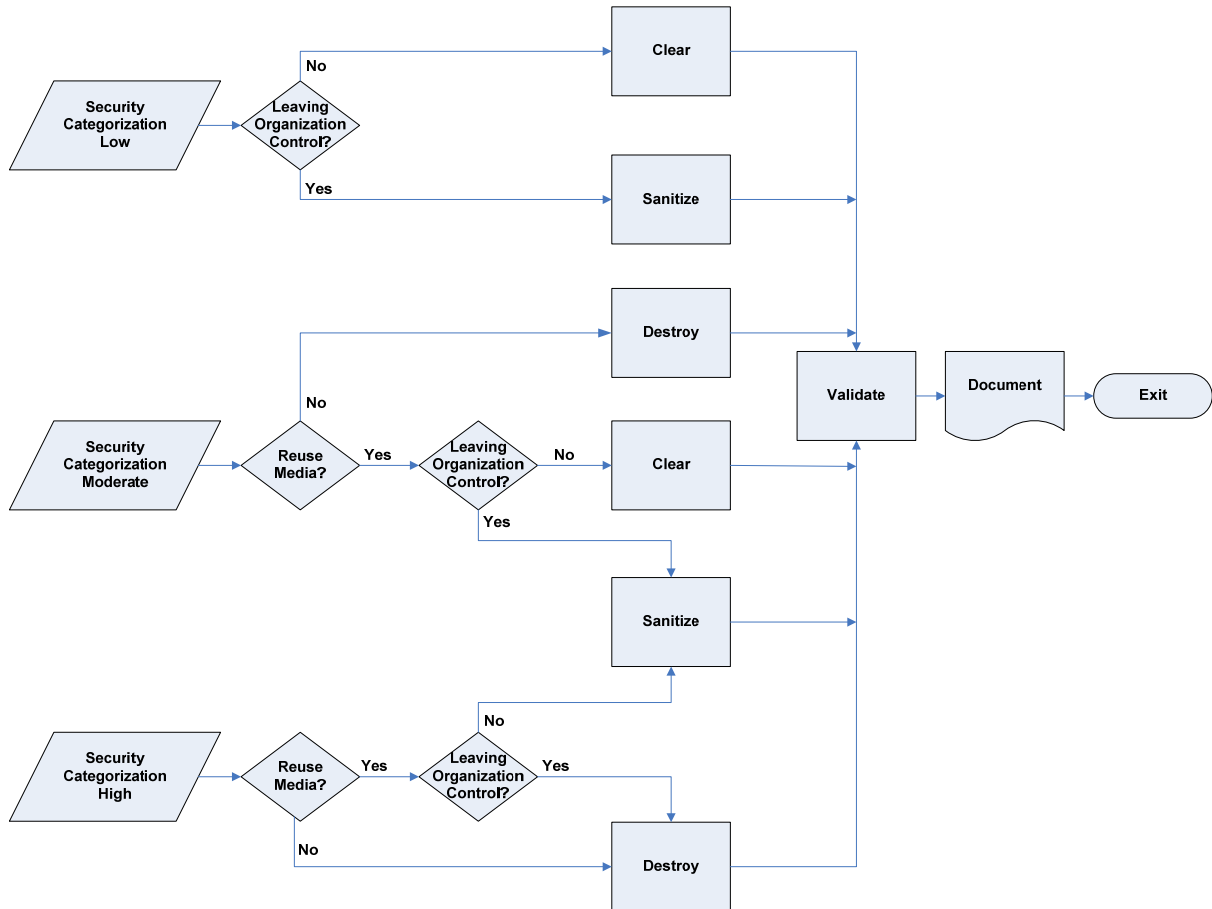
Depending on the security categorization [7] of the organization where the solid state drive is deployed, the chosen procedure of data elimination or destruction can vary, as described below and shown in Figure 3:

- Low Security Disposition:** If the security categorization is defined as *CONFIDENTIAL*, a Clear or Sanitize procedure is required. If the drive will leave the organization, it will be moved to a higher classification level (moving to a lower classification level is not allowed, unless the drive is destroyed) and as such, a full Sanitize procedure is required. If the drive stays within the organization and at the same classification level, a Clear procedure will suffice
- Moderate Security Disposition:** If the security categorization is defined as *SECRET*, complete destruction of the media may be required, depending on whether the media needs to be reused or not. If the media is meant to be used again, a Clear or Sanitize procedure is required. If the drive is leaving the organization and moving to a higher classification level, a full Sanitize procedure is required. If the drive stays within the organization and at the same classification level, a Clear procedure will suffice
- High Security Disposition:** If the security categorization is defined as *TOP SECRET*, complete destruction of the media may be required, depending on whether the media needs to be reused or

¹ USA Army 380-19 was superseded by AR25-2 in 2003. AR25-2 was updated in October 2007, but does not specify a procedure for sanitizing or purging a drive.

not. If the media is meant to be used again, a Clear or Sanitize procedure is required. If the drive is leaving the organization and moving to a higher classification level, a full Sanitize procedure is required. If the drive stays within the organization and at the same classification level, a Clear procedure will suffice

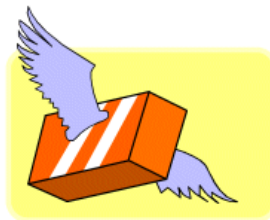
Figure 3: Security disposition flow chart



5.2 IRIG 106-2007, Chapter 10.8

The DoD and NSA defined the security erase standards for storage devices in an era where hard disk drives were the main storage media. Hence, the standards focused on declassification of standard disk and other conventional memory technologies. With the advent of advanced, high-density memory technologies, such as NAND flash, new standards were required.

Figure 4: IRIG 106 logo



The Inter Range Instrumentation Group (IRIG) is the standards body of the Range Commander Council (RCC). The Telemetry Group of the Range Commander Council specified a new standard, called IRIG 106-2007, chapter 10.8 [8] to define the operation and interfaces for digital flight recorders. It specifically

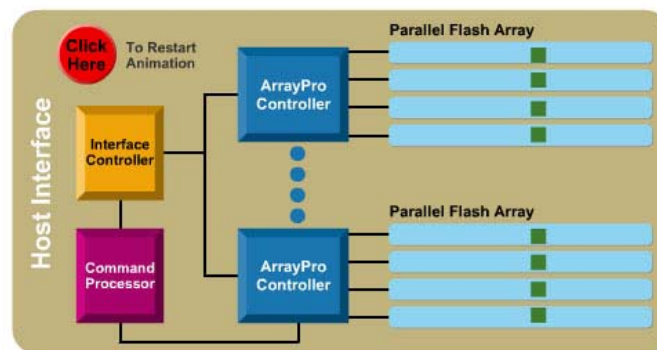
addresses NAND flash architecture and data structures, defines for bad block handling, and allows for reviewing the secure erase results to verify that all classified data has been eliminated. Adtron's EraSure technology, embedded within its Flashpak solid state drives, is fully compliant to the IRIG 106-2007 standard.

5.3 Adtron EraSure Technology

Adtron's EraSure technology is combined with Adtron's ArrayPro™ technology to provide fast Clear and Sanitize options for any capacity solid state drive. Clear and Sanitize provide different levels of data security and performance, and thus provide different levels of protection against compromising sensitive data.

When a Clear or Sanitize command is sent to the Flashpak solid state drive, the ArrayPro controller executes the command in parallel across each of the flash arrays within the solid state drive. Figure 5 below shows a block diagram of the internal architecture of Adtron's ArrayPro technology and how this combines with the EraSure technology.

Figure 5: Adtron EraSure Technology uses ArrayPro Engine



Adtron's EraSure technology operates on a physical block level as opposed to logical block level. This means that all Erase Blocks within the drive, including those that contain data structures, mapping tables or any other blocks used for flash management purposes, are erased during an EraSure operation. To return the Flashpak drive to a state that it can be reused after an EraSure procedure, the drive must undergo an *Initialize Drive* operation. EraSure technology supports the following data elimination procedures:

- **EraSure Fast Clear:** This is the fastest level of data elimination. It performs a single erase of the data from the solid state drive, followed by an automatic *Initialization Drive* procedure. The drive is completely reusable at the end of this procedure.
- **EraSure Clear:** This is the second fastest level of data elimination. It performs a single erase of the data from the solid state drive, after which the drive is completely reusable following an *Initialize Drive* procedure. The initialization procedure is not executed automatically and must be called through a host command.
- **EraSure Sanitize:** Typically, each flash array inside the Flashpak solid state drive is simultaneously cleared of data and then overwritten one or more times, using one of several pre-programmed procedures or a customized Sanitize procedure. After a Sanitize procedure, the solid state drive is reusable following an *Initialize Drive* procedure. Depending on the chosen EraSure procedure, Sanitization of the drive can take minutes to hours.

Adtron's EraSure technology complies with all military standards shown in Table 1, including full support for IRIG 106-2007, chapter 10.8. In addition, EraSure technology supports a custom-defined procedure with up to 30 steps.

An EraSure operation can be triggered by either a software host command or a hardware input. It is possible to connect a pushbutton or other actuator to manually initiate a configured EraSure command.

Once the command is issued, the Flashpak solid state drive indicates progress through a status LED. In addition, it is possible to track the progress (percent of completion) of the secure erase operation through an ATA command.

If an EraSure procedure is interrupted by removing power to the drive (or any other means), the built-in Auto-Resume feature ensures that the EraSure procedure automatically resumes at the same point when power is restored to the drive. This is accomplished by storing various “save points” at key steps in the EraSure procedure. When the Flashpak solid state drive reboots, the controller resumes the EraSure procedure at the last step indicated by the save point.

Note: Please refer to Adtron’s *EraSure Programmer’s Guide* [9] for full details on the EraSure command set and configuration.

5.3.1 EraSure Block Management

An Erase Block of 128KBytes or 256KBytes is the minimum unit of data that can be erased. NAND flash is shipped by flash manufacturers and can contain bad Erase Blocks – areas on the flash that cannot be used for read/write operations. Additional Bad Blocks are accumulated during standard read/write operations. In order to provide complete Sanitize capabilities, solid state drive vendors must effectively manage Bad Blocks that may contain sensitive data.

Flash management algorithms assign Erase Blocks for different purposes and containing different types of data, as described in Table 2 below.

Table 2: Block Definition

Block	Usage	Content
User Data	Write and read areas for the user. Equals the available capacity on the Flashpak solid state drive	Contains user data
Failed	Retired User Data block. Also known as accumulated Bad Block	Can contain old user data
Spare	Unused until placed into service to replace Failed blocks	Erased with no user data
Factory Defect	Marked by flash chip manufacturer as non-functional. Also known as Bad Block	Never used by Flashpak solid state drive, and does not contain data
Buffer	Erased blocks that accept new user data. The content is later merged with User Data block and is not part of the Flashpak solid state drive capacity	Contains new user data
Reserved	Holds control and configuration information for each flash controller	Contains firmware and control structures, but no user data

Adtron’s EraSure procedure erases and overwrites all of the above mentioned block types, and keeps track of the erase status of each block through an Erase Block database. If an Erase Block fails to erase or write during a Sanitize process, it will be processed outside of the standard flow.

5.3.2 Implementing and Verifying EraSure

As mentioned in section 5.3, EraSure procedures can be triggered via a software host command or a hardware input. Regardless of the trigger method, the OEM host computer requires a device driver to support the following functionality:

1. Program the selection for the desired EraSure procedure. May be done real time or prior to a mission
2. Trigger the pre-selected EraSure procedure by software command or hardware trigger
3. Issue commands to verify the execution of the EraSure procedure
4. Issue a command that reinitializes the drive after an EraSure procedure

Note: Please refer to Adtron's *EraSure Programmer's Guide* for full details on the command set.

To verify the validation of an EraSure procedure during design stage, the following steps are recommended:

1. Interrupt the power during the EraSure procedure to validate the recovery and continuation of the process (EraSure will resume the procedure when power is restored)
2. Validate the non-stop progress by attempting to interrupt and stop the procedure
3. Verify the absence of all known data within all the Erase Blocks, as defined in Table 2. This can be done through the host computer interface (EraSure command) or by removing the flash chips to independently verify the data content.

6 MEDIA DESTRUCTION

Different military specifications call for different media destruction procedures. The NSA 130-2 specification [2] requires the use of degaussers for magnetic disk drives, after which the drives can be disposed of through shredding or burning. It does not specify anything for solid state drives and refers to Clear and Sanitize procedures to ensure complete data elimination.

A more stringent specification is the NAVSO P-5239-26 standard [10], which calls for a variety of hard disk drives destruction techniques, ranging from degaussing to sand blasting or chemically destroying the disk. Besides the common Sanitize techniques, no specification is provided for media destruction of solid state drives.

In certain cases, standard sanitization techniques are not adequate for the application due to timing constraints. If the data must be eliminated in a matter of seconds, other methods, such as physical destruction of the media, may be applied. Today, there are not a lot of techniques available on the market that will physically destroy the flash media. One such technique is Adtron's ZAP technology, which is able to physically destroy the access to the flash media in a matter of seconds, making it impossible to retrieve any data from the NAND flash components.

6.1 Adtron ZAP Technology

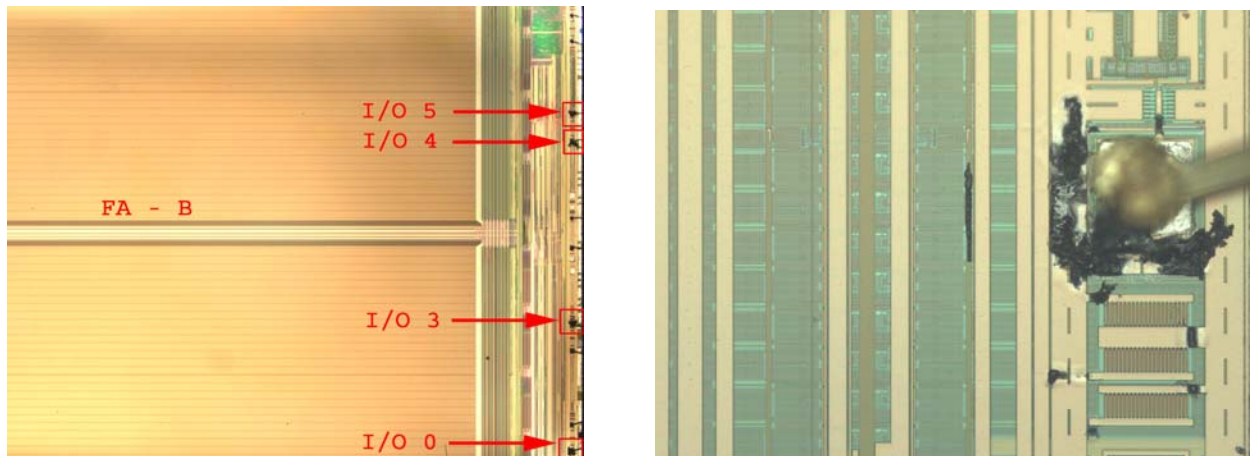
Adtron developed a destructive technology, named ZAP, which destroys the ability to access the flash chips in a 64 GB Flashpak solid state drive in less than 5 seconds. Triggered by either a software command or a hardware input (push button or similar), a high energy impulse destroys the I/O transistors and static protection logic within each flash chip on the drive.

The damage to the flash die is visible to the naked eye. Before executing a ZAP cycle, the internal logic tests the destruct signal path to ensure maximum damage. The energy impulse is applied repeatedly to ensure total destruction of the flash media. For additional protection, a Clear command can precede the ZAP procedure.

An external lab validated the functionality of Adtron's ZAP technology by verifying the destruction on the flash chips. The analysis included external package inspection, X-ray inspection, micro probing, and parallel-lapping, as well as die encapsulation and inspection. According to the lab report [11], the "*optical die inspection revealed visible evidence of typical Electrical Over-Stress (EOS) damage on all the I/O pins reported on all dies*" and "*micro probing confirmed shorts for all the I/O pins with respect to Vss on all four dies.*"

Figure 6 below shows the visual results of the damage done after the ZAP technology was applied to the flash chips.

Figure 6: Visual damage on flash chips with Adtron ZAP technology



Although the ZAP technology does not destroy the flash media in a literal sense, it destroys the I/O blocks that are required to perform read or write operation from/to the flash. The only method to obtain data would be to probe the flash area, which would prove to be an extremely difficult task, considering the fact that the Flashpak solid state drive uses QDP (Quad Die Pack) NAND flash chips in its design.

An 8GB flash chip contains over 8 billion transistors; a QDP version would equal more than 32 billion transistors within one flash chip. Reaching the data that is stored in the flash die layers that are more deeply embedded into the device would require peeling off each flash die separately. An excerpt of the lab report reveals the following on the complexity of such a task:

“Individual die extraction will be difficult, if not impossible. The major issue faced in singulation of each of the flash dies is preventing the die from cracking while chemically and/or mechanically separating them from each other. In order to maintain as much of the die circuitry to enable visual inspection during this analysis, it was necessary to sequentially expose each die, destroying die#1 and 3 by mechanically grinding away”.

Even if probing the separate flash die layers would result in recovery of the data, the data abstraction layers within a solid state drive, as described in section 3.3, would create additional complexity to make sense of the data that was obtained.

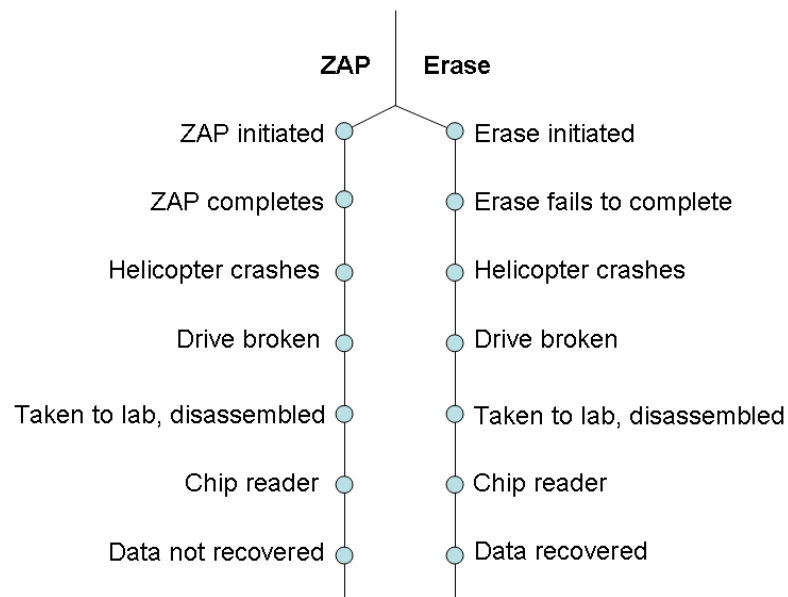
7 CHOOSING THE RIGHT SECURITY TECHNOLOGY

Choosing the correct EraSure procedure depends on many factors. Two illustrative examples are presented below.

7.1 Data Recorder in a Helicopter

The solid state drive inside the data recorder of a helicopter stores tactical maps and functions as a data logging device for data captured during a flight. To ensure data security, the drive can be either provisioned with a Sanitize procedure, or Adtron’s ZAP technology. In case of an emergency, when the helicopter is about to crash, the system triggers the selected security procedure. Depending on the implemented technology, two scenarios can be followed, as shown in Figure 4 below.

Figure 4: Data recovery in ZAP vs. Erase



- **ZAP:** Since the ZAP procedure is finished in a matter of seconds, it is most likely that the entire media is declassified before the helicopter hits the ground. Once the drive is recovered, however, no data can be obtained afterwards in a lab
- **EraSure Sanitize:** Depending on the implemented EraSure procedure, sanitizing the drive will take minutes, if not hours. It is therefore unlikely that the media will be completely declassified before the helicopter hits the ground. Once the drive is recovered, analysis in a lab will most likely be able to recover the remaining data

As can be seen from the two different outcomes on data recovery, it is important that the right choice of data security technology is made.

7.2 Data Recorder in a Tank

The solid state drive inside the data recorder of a tank captures data during training sessions at a military base inside neutral territory. Once the training session is over, the tank commander takes the drive out of its enclosure inside the tank and returns it to a secure place on the base.

The data that is captured during the session needs to be declassified, although the highest security level is not required as the drive remains inside the premises of the base. Since the tank commander does not want to wait hours for the drive to be declassified, a fast EraSure Clear procedure, where the data on the drive is erased and the drive is reformatted in a matter of seconds, will suffice.

The situation would change if the drive were to be transferred to another program or military base, and would have to undergo a more stringent declassification procedure. In that case, an EraSure Sanitize procedure, according to IRIG 106-07, would be more appropriate. Since this procedure takes a few hours, it should only be implemented only for occasions like this.

As can be seen from the above example, the drive would have to support two different EraSure commands in order to support two different usage scenarios.

Figure 5: Tank commander

8 CONCLUSION

Various methods exist for data protection and elimination depending on the security level required within an organization. Many defense applications require the functionality provided by Adtron's EraSure technology.

Securing confidential data in emergency situations is essential. The damage that may result if confidential information falls into the wrong hands can be devastating. Sanitizing mechanical hard disks is an arduous process, requiring special degaussers, stable power conditions during the process, and ample time, all of which may be lacking during an emergency. Solid-state flash drives are better suited for this task, and can be erased in seconds using Clear procedures. When the drive is used in a medium-to-high security categorization, a Sanitize procedure may be required. Depending on the military specification that is implemented, declassifying a solid state drive in a Sanitize procedure can take minutes to hours.

The Clear and Sanitize commands implemented within Adtron Flashpak solid state drives provide the performance and erase levels required by all U.S.A. defense organizations.

The fastest way to eliminate data on a drive is by destroying the media itself. Not many such techniques are available on the market today. Adtron's ZAP technology is a unique way of destroying access to the NAND flash within Flashpak solid state drives. Within 5 seconds, a 64GB drive can be destroyed, leaving it virtually impossible to access or retrieve any data from the NAND flash components.

9 REFERENCES

- [1] www.cnn.com, *U.S. surveillance plane lands in China after collision with fighter*, April 1, 2001.
- [2] NSA/CCS Manual 130-2, *Media Declassification and Destruction Manual*.
- [3] Peter Gutmann. *Data remanence in Semiconductor Devices*, proceedings of USENIX Security Symposium, Washington DC, August 2001
- [4] Peter Gutmann. *Secure Deletion of Data from Magnetic and Solid-State Memory*, proceedings of USENIX Security Symposium, San Jose, CA, July 1996
- [5] ATA/ATAPI-7, 1410D Volume 2, Revision 0, 5 November 2001, section 2.7
- [6] *About AES – Advanced Encryption Standard, A short introduction*, August 2007, Svante Seleborg, Axantum Software AB
- [7] <http://www.taonline.com/securityclearances/>, *Types of Security Clearance*.
- [8] RCC Document 106-07, *Telemetry Standard*, Chapter 10.8, *Digital Recording Standard*, September 2007
- [9] Adtron EraSure Data Security, *Secure Erase Programmer's Guide*, November 2007
- [10] NAVSO P-5239-26, *Information Systems Security (INFOSEC) Program Guidelines*, Naval Information Systems Management Center, http://www.fas.org/irp/doddir/navy/5239_26.htm
- [11] Failure Analysis Report H09154, MEFAS Lab, Lake Forest, CA
- [12] www.computer.org, *Biometric Authentication*, Alfred C. Weaver, University of Virginia, Feb 2006.

About the Author

Esther Spanjer is Director of Technical Marketing at Adtron Corporation. With more than 10 years of experience with flash-based solutions, Ms. Spanjer has gained valuable insight into the use of this rapidly evolving technology in a wide range of embedded applications in the military, aerospace, communications and industrial markets. She joined Adtron to help evangelize the use of flash technology for new types of applications in both the traditional markets and the emerging enterprise market. As users become more familiar with the full range of benefits of flash technology, she believes that flash-based storage will be adopted in a broader range of what have typically be thought of as hard-disk applications.

Ms. Spanjer received a B.Sc. degree in Electronic Engineering from the Technical University Amsterdam (Netherlands) in 1991. She can be reached at espanjer@adtron.com.

About Adtron

Founded in 1985, Adtron is the leading designer and global supplier of high performance and high capacity solid state drives. Adtron Flashpak solid state drives integrate seamlessly into defense/ aerospace, industrial automation, medical, transportation, telecom and enterprise applications. Based on Adtron's advanced ArrayPro™ performance engine, Adtron solid state drives deliver superior sustained read and write rates and are designed to reliably meet stringent environmental requirements. The Adtron Quality Management System is ISO 9001:2000 certified. Adtron is headquartered in Phoenix, Arizona with channels in all global markets.

Learn more about Adtron at <http://www.adtron.com>

Flashpak and EraSure are registered trademarks of Adtron Corporation.
ArrayPro is a trademark of Adtron Corporation.

© Adtron Corporation 2008

Security-R1-031408

