

The need for security:

Embedded form factors leverage advancements in storage protection features

By Steve Gudknecht

As the demand for performance and security in harsh environments escalates, solid-state flash drives are increasingly appearing in embedded military applications. These SSDs provide fast erasure speeds and high reliability while working hand-in-hand with FPGA-based PMC designs.

Place all of your eggs in one proverbial basket and you're looking for trouble. Place them in one basket where there's a good chance they could be lost, stolen, or broken and you've got a potential disaster on your hands. Such is the case with data storage these days. With the cost of mass storage continuing to plummet and capacities per unit area on the rise, larger volumes of information are being stored now more than ever, and the need for security and performance in harsh environments is escalating.

Solid-state flash storage manufacturers are responding to these evolving needs with secure erasure and write protection capability in traditional drive form factors, such as 1.8" and 2.5" (IDE/ATA and SATA) as well as in CompactFlash. Accordingly, solid-state drives are increasingly finding their way into military and secure applications, adding to the need for features such as secure data erasure and write protection.

Many military applications also require hardware-controlled data erasure that operates independently of the operating system. FPGA-based PMC form factor embedded designs are key to this issue as they work hand-in-hand to resolve mass storage challenges.

Erasure speed is another important factor, especially in military applications where emergency situations demand extremely fast erasure as compared to rotating drives. This need becomes more common with the increasing number of military vehicles in harm's way in current and future theaters of battle. Alternately, as a matter of operational efficiency, routine intentional data erasure and write protection allow personnel to quickly declassify vehicles for redeployment.

And finally, the high reliability of solid-state devices, as compared to rotating drives, must also be considered. Data

"With the cost of mass storage continuing to plummet and capacities per unit area on the rise, larger volumes of information are being stored now more than ever, and the need for security and performance in harsh environments is escalating."

storage equipment is now being deployed in field operations where security breaches are simply unacceptable and harsh environments demand the legendary rugged capability of solid-state storage and its resistance to extremes in shock, vibration, and temperature.

Secure erasure and MIL standards

As Table 1 shows, no less than five military standards deal with data erasure methods for solid-state flash devices. While there is some ambiguity in the details between them, all standards are in agreement regarding the intended results of data erasure.

The following differentiation is made between clearing media and sanitizing media: Data on *sanitized* media should be unrecoverable by normal laboratory methods and data on *cleared* media may be recoverable using certain laboratory techniques. The standards go on to state that media that has been *sanitized* can be reused in both secure *and* non-secure areas, whereas media that has been *cleared* of sensitive data can only be reused in nonsecure areas.

All methods stipulate that the ultimate way to ensure that sensitive data is absolutely nonrecoverable is to break out the incinerator, grinder, or the shredder and let the heavy equipment do the work. So what's the difference between clearing and sanitizing media? The DoD 5220.22-M Clearing and Sanitizing Matrix spells out the requirements very clearly, as shown in Table 2.

It boils down to this:

- To clear media – erase once
- To sanitize media – erase more than once
- When in doubt – physically destroy the media

Mil Standard	Clearing	Sanitization	Destruction
DoD 5220 NSA 130-2 Air Force, AFSSI 5020 Army, AR 380-19 Navy, NAVSO 5239	Clearing removes sensitive information from...storage media in a manner that renders it unrecoverable by normal system utilities or nontechnical means.	Sanitizing removes sensitive information from storage media in a manner that gives assurance that the information is unrecoverable by technical means.	Includes incineration, pulverizing, grinding, or shredding.

Table 1

Media	Clear	Sanitize
Memory		
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasable PROM (EEPROM)	i	h or m
Flash EPROM (FEPRM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read Only Memory (ROM)	N/A	m

US Department of Defense 5220.22-M
Clearing and Sanitization Matrix
c. Overwrite all addressable locations with a single character.
g. Remove all power to include battery power.
h. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
i. Perform a full chip erase as per manufacturer's data sheets.
j. Perform i above, then c above, a total of three times.
k. Perform an ultraviolet erase according to manufacturer's recommendation.
l. Perform k above, but increase time by a factor of three.
m. Destroy - Disintegrate, incinerate, pulverize, shred, or melt.

Table 2

One thing remains certain: Unless the media is physically destroyed, there will always be a debate as to whether or not the data it once contained is recoverable and, if so, by which means. This applies regardless of the media type. Solid-state flash suppliers have responded to these requirements with data erasure options that include nondestruct and destruct erasure. Table 3 outlines the differences between these options.

Solid-State Flash Suppliers	Typical Nondestruct Erasure Methods	Typical Destruct Erasure Methods
Silicon Systems, STEC, BitMICRO, Adtron, and so on.	Single-pass erase all data fields, bad and spare data blocks as well as master boot records and file allocation tables. The device can be reformatted and reused.	In addition to non-destruct steps, all management firmware is erased, rendering the device unusable.

Table 3

At first glance, these initial erasure levels meet only the requirements for clearing media. However, solid-state flash developers indicate that data erasure in solid-state media involves multiple writes of arbitrary data or all zeros followed by all ones. (Remember, an erase is actually an overwrite.)

That being the case, a “single” solid-state erase is actually a dual erase process and can, therefore, be considered compliant with the standards. The multiple erasure requirement probably has its roots in residual “ghost” images on magnetic media. (Whether or not residual images of any kind are an issue with solid-state media is a topic for another discussion.) In any event, to ensure compliance with the language of the standards, many solid-state flash developers offer a third level of erasure that carries out the erase process multiple times.

FPGA technology and the software problem

At the component level, solid-state flash drives can support both software and hardware initiation of secure erase as well as write protection. Solutions that rely solely on software are, of course,

subject to the stability of the application software, OS, and CPU. System lockups can occur even under the best conditions and are more likely to occur when the system comes under strain. Therefore, a key requirement for many secure military and commercial applications is that initiation of both the erase and write protect functions must be accomplished via hardware, without OS intervention.

Externally mounted switches or push buttons allow hardware actuation that requires only applied power and no software intervention whatsoever. The switch type and location are selected according to the needs of the application.

Utilizing FPGA technology in new PMC products solves the software reliance problem and allows hardware initiation of all three features – nondestruct and destruct erase as well as write protect – in embedded form factor products. The Secure PMCStor by ACT/Technico (Figure 1) provides hardware-enabled data security features at the board level using FPGA technology in a conduction-cooled PMC product.

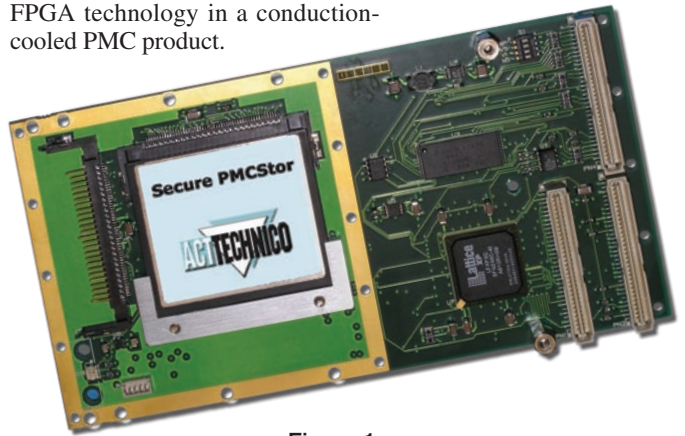


Figure 1

A custom FPGA IP core can recognize the particular CompactFlash vendor/model. Upon operator initiation, it performs signal conditioning adapted to the vendor requirements for the desired command. Available IP cores providing PCI-to-ATA controller capabilities reside alongside the custom signal conditioning cores to provide both functions inside a single chip. PMC form factor products bring these much-needed security functions to applications requiring up to 16 GB of storage capacity per PMC slot.

The need for speed

Another consideration in securely erasing sensitive data is speed. The 2001 collision and forced landing of an EP-3 spy plane in China highlighted the need to develop a reliable method to destroy large blocks of data as quickly as possible. Storage units used in combat operations at all levels from aircraft and ground-based equipment to wearable computers gather and share sensitive information that may need to be erased at a moment's notice.

Accordingly, erasure speed is a major concern. There are wide-ranging claims about the speed of data erasure in rotating media; however, even the most aggressive figures pale in comparison to solid-state erasure capabilities. Consider a one-hour erase cycle for a 20 GB disk drive volume compared to a 15-second erase cycle for a 16 GB volume in CompactFlash as some manufacturers claim.

Reliability and security

Intentional security breaches constitute one way to lose control of crucial data. But, if the data is no longer available due to storage device failure, that constitutes a real problem as well.

Redundancy schemes have evolved to the point where embedded systems with small footprints can address system availability and uptime requirements. The best redundant systems, however, add cost by their very nature, using as little as 50 percent of deployed capacity in RAID 1. Redundant systems consume valuable cabinet space, generate more heat, require more power, and in general require additional support infrastructure, especially in cases where elaborate temperature, shock, and vibration mitigation schemes are introduced.

In spite of the aforementioned, rotating storage remains the weakest link in most systems. A recently completed study involving large populations of rotating hard drives in benign enterprise systems showed that hard drives accounted for nearly 50 percent of all hardware failures in the systems observed. Temperature extremes are the number one killer of hard drives. Some studies suggest up to a 50 percent drop in service life and MTBF for every 10 °C increase in operating temperature beyond an optimal 35 °C to 40 °C.

On the other hand, solid-state hard drives start out with MTBF ratings three to four times higher than their hard disk cousins and can operate at -40 °C to +85 °C with little or no degradation in lifespan or any other performance measure. Likewise, they are almost impervious to excessive shock and vibration as they easily meet most MIL-STD-810 and 901D requirements.

Worried about read/write endurance? Solid-state storage technology has increased the write/erase endurance number to 2 million

cycles. Advanced wear-leveling techniques coupled with predictive algorithms that track bad block statistics and write/erase cycles can accurately predict failure and warn the user to take preemptive action.

Solid-state flash dismounts data protection issues

Hardware-based secure erase and write protect features are rapidly becoming requirements in a wide range of rugged applications where data protection is paramount. Solid-state flash manufacturers are providing products that meet those needs with options to rapidly erase or write protect data using reliable hardware-driven commands. Embedded equipment manufacturers are implementing these new products in FPGA-based PMC form factors for use in applications requiring moderate storage capacities in harsh environments. **CS**



Steve Gudknecht is a product manager at ACT/Technico. He has held positions in field applications and marketing in high-technology industries for more than 28 years. Steve's responsibilities include product development, product marketing, training, and sales support. He can be reached at steveng@acttechnico.com.

ACT/Technico

215-956-1200

www.acttechnico.com