TECH BRIEF

Secure Military Grade Solid State Drives Overview

- Military packaging
- Built-in encryption and multiple key management modes
- No backdoors
- Military Grade data purging and sanitization
- A family of trusted tools
- SSD building blocks
- Data preservation
- Trusted supply chain and longer lives
- Military Grade SSD options

Introduction

This document introduces the considerations for selecting Solid-State Drives (SSDs) for mission-critical, high-reliability and high-security applications. This overview augments Mercury's white paper, Safeguarding Mission Critical Data with Secure Storage Solutions which offers a more detailed study of the consequences associated with selecting a commercial or enterprise-grade SSD for military or aerospace applications.

Mercury has leading expertise in the rugged, secure storage domain, leveraging twenty years of industry experience designing and building defense grade storage devices. Our proven solutions are found in manned, unmanned, military and commercial mission and data recording applications that require robust built-in security, data protection and purge capabilities. Our most rugged and secure drives form our Military Grade portfolio of SSDs.

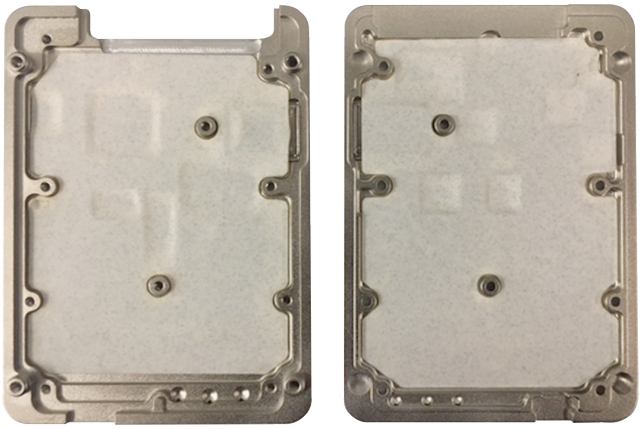


Figure 1. Secure Military Grade SSD rugged packaging

Military packaging

Consumer and enterprise data storage is transitioning from rotary, magnetic media to SSDs comprised of dense, rugged NAND flash memory. With no moving parts, NAND flash-based drives are a requirement for all military and aerospace mission-critical applications. Today, military needs are driving data storage requirements far beyond deployable ruggedness in to the domains of robust data security, purging and sanitization.

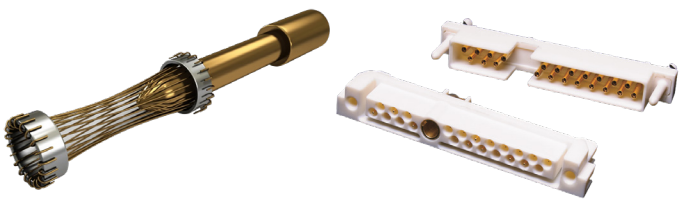
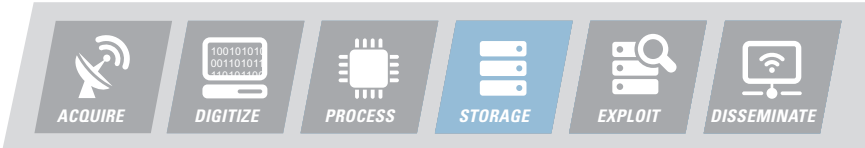


Figure 2. Secure Military Grade SSD rugged interconnects

Mercury Systems is a leading commercial provider of secure sensor and safety-critical processing subsystems. Optimized for customer and mission success, Mercury's solutions power a wide variety of critical defense and intelligence programs.



Built-in encryption and key management

AES-256 (Advanced Encryption Standard) encryption is the industry standard for sensitive data protection using an encryption/decryption key to transform plain text into cipher text and vice versa. XTS (cypher text stealing) block cipher ensures unique cipher text is produced when encrypting identical blocks of data. Mercury was the first SSD provider to attain NIST FIPS 197 certification for our AES-256 XTS encryption algorithm and XTS is built-in to all our Secure Military Grade SSDs.

Common implementations of secure, commercial off-the-shelf (COTS) SSDs require a user to enter a password (ATA password) for drive access. Under this scenario, security is limited to a simple, low-strength, user-defined password. Although effective for some applications, defense solutions require much stronger protection using flexible key management methods. Mercury adds this strength requirement by augmenting ATA password access with:

- Random self-generated keys
- User-defined permanent keys
- Session keys (which are purged if the power is removed)
- BLACK keys with KEK featuring encrypted BLACK and key decrypion key (KEK)
- External keys fill through SSD ports (RS-232 and DS-101)

These additional security implementations ensure that the encryption key is the gating factor that grants access to the stored data.

No backdoors

A fundamental component of any SSD is its controller which is usually an ASIC device designed and produced in volume by foreign manufacturers. When these controllers are integrated into a SSD there is no reliable way to verify that it is free of "backdoors" or encryption bypass capabilities to thwart security features. In contrast, Mercury's in-house developed ARMOR® drive controller is designed and manufactured in the United States. Mercury has 100% authority over our controller's implementation.

Data purge and sanitization

When a drive falls in to the wrong hands, the contents of the drive should be wiped or sanitized quickly.

In the simplest purge scenario, a remote trigger will initiate and complete a cryptographic erase and the encryption key will be purged in less than 30 milliseconds. Although the cipher text remains on the drive, the cipher text cannot be decrypted without the encryption key.

For more sensitive data, additional steps may be necessary to ensure that data is absolutely not accessible. These additional steps may include overwriting of all the data on the drive with non-sensitive data. All storage cells, including spare cells for factory defaults, worn out blocks, wear-leveling and garbage collection should be overwritten. Especially sensitive data may need the assurance of multiple over-write cycles.

No two user scenarios are the same. Defense and aerospace applications may require user-configurable sanitization protocols based on the type of data being stored and the application environment.

A family of trusted tools

Mercury offers multiple user-definable sanitization protocols, including:

- TRRUST-Purge® to wipe the encryption key in less than 30ms.
- Fast clear with encryption key purge and overwriting of all data in 3 to 8 seconds.
- And other common military purge protocols – please contact Mercury for more information.

SSD building blocks

SSDs are built using NAND flash memory of which there is two types, single-level cell (SLC) and multi-level cell (MLC). Each has its advantages and disadvantages.

SLC-based NAND flash offers the highest level of endurance and temperature robustness for the preservation of critical data. SLC NAND is ideally suited to applications that write continually or that run remotely/unattended and where service is difficult at best.

MLC-based NAND flash offers lower levels of read/write endurance by a factor of 10 or more. MLC NAND is ideally suited to large volume storage for a limited time (e.g. flight data recorders).

Mercury's offers both SLC, MLC, and TLC flash memory variants of our Secure Military Grade SSDs.

Data preservation

COTS SSDs are engineered to last at least as long as their warranty and may not provide extended-term data retention. Some COTS SSDs include firmware algorithms to reduce read/write speeds under high utilization conditions to minimize early failures. This may cause critical data to be lost during record. Mercury has full authority over our controller which we optimize for read/write performance, even under sustained and heavy loading.

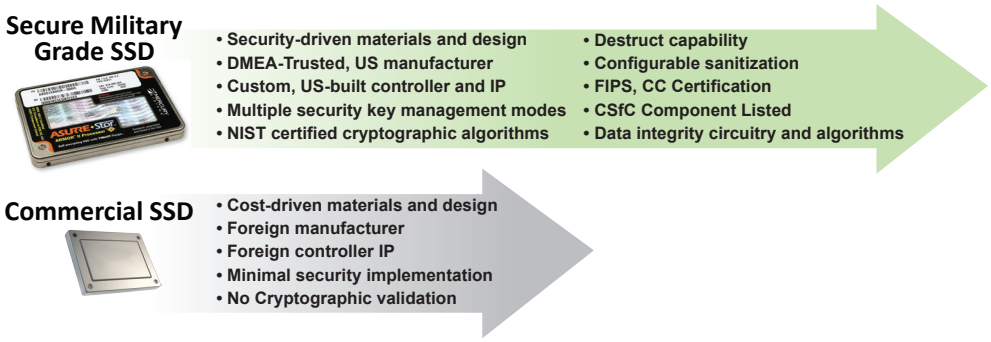


Figure 3. Features of a Secure Military Grade SSD outpace even the best commercial SSD

All NAND flash storage devices occasionally corrupt small pieces of data, particularly if the device is heavily utilized. SSDs mitigate this risk through the implementation of error correcting code (ECC) and NAND over-provisioning. Shorter-lived COTS SSDs include limited ECC and over-provisioning to maximize user capacity. Mercury's Secure SSDs feature advanced ECC and NAND over-provisioning that ensures data integrity in harsh military environments.

Mercury implements proven, customizable, multi-layered power-loss protection. Our robust data protection approach, unlike other technologies, is temperature independent. Mercury's Secure Military SSDs feature a deterministic shut-down sequence that guarantees complete read/write operations that are in progress when the power fails.

Trusted supply chain and longer lives

Commercial and enterprise-grade SSDs are optimized for performance and cost. This business model drives design and production to low-cost centers outside of the USA. Defense microelectronics should be manufactured using trusted devices within the United States where trust issues are maintained under the consequence of law. Defense Microelectronics Activity (DMEA) accreditation is the defense industry standard for a trusted supplier of microelectronics solutions. Mercury's portfolio of Military Grade Secure SSDs are all designed, coded, manufactured and supported from a domestic DMEA accredited facility.

Innovation That Matters – Mercury Security and SSD Firsts

Consumer and enterprise product life cycles are shorter than those in change control-sensitive military applications. Mercury maintains ECO control and product availability until components are no longer available, when end of life planning is initiated with our customers.

Secure Military Grade SSD options

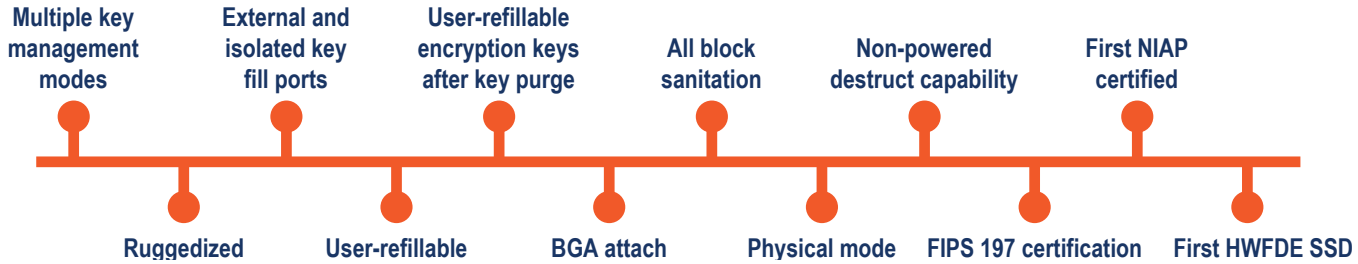
Mercury's Secure Military Grade Secure SSDs are offered as TRRUST-Stor and ASURRE-Stor options.

Figure 4. Rugged, Secure Military Grade SSD with ASURRE-Stor protection

For twenty years prime contractors have trusted Mercury Secure Military Grade SSDs with TRRUST-Stor technologies for their land, air, and sea defense solutions. Our storage solutions range from the de facto 2.5" form-factor, to mSATA, XMC, mobile, VPX, and ultra compact packages. The ultra-compact package has a SWaP-optimized 32 x 22 mm footprint and rugged tin/lead solder ball BGA attach.

ASURRE-Stor SSDs are engineered to the requirements of FIPS 140-2, CC, and CSfC making them ideally suited for the storage of classified, secret, and top secret data when used as a component in a 2-layer CSfC solution registered and approved by the NSA.

TRRUST-Stor™ Mission Pak ultra-portable secure SSD with integrated security and performance-enhancing algorithms is similar in size and function to a commercial USB flash drive, but precision-engineered to withstand the harshest military operating environments while simultaneously protecting the most sensitive data from adversarial attack. The ASURRE-Stor variant of this product, with FIPS 140-2 certification and eligibility for the CSfC program, is planned.



Mercury's new TRRUST-Stor VPX RT radiation-tolerant SSD featuring BuiltSECURE™ technology is the first commercial SSD precision-engineered for the harshest possible operating environments leveraging OpenVPX™ standards. Although designed for commercial satellite applications, the new device can also be adapted for other applications where radiation exposure may occur, including high-altitude aircraft, airborne weapons, and mission-critical ground computing systems. TRRUST-Stor VPX RT SSD includes advanced BuiltSECURE error correction algorithms paired with large geometry industrial-grade Single-Level Cell (SLC) NAND flash memory. Designed for fault-tolerance with up to six failed NAND devices, the new device offers long-term data integrity for applications where device repair or replacement is cost-prohibitive. Recognizing that no two mission requirements are identical, customers can tailor power consumption against performance requirements for each unique mission. Mercury's new storage product is designed for seamless integration with the OpenVPX ecosystem of processing boards and chassis.

For more information, including modified-COTS secure storage options please contact Mercury Systems at secure.ssd@mrcy.com or (602) 437-1520.

Figure 5. Comparison of commercial and Secure Military Grade SSDs

	Feature	COTS solution	TRRUST-Stor®	ASURRE-Stor®	Benefit
Security	Self-encryption	AES-128 AES-256	AES-256 XTS Other algorithms supported	AES-256 XTS Other algorithms supported	Flexibility and security
	Key management	ATA password only	Multiple key management modes	Multiple key management modes	Customizable security implementation
	Backdoors	Possible	No	No	US design and 3rd party validation eliminated back door security threat
	Sanitization	No	User configurable	User configurable	Flexibility and security
Data integrity	Warranty throttling	Common	No	No	Consistent read/write performance
	ECC	1E-14 UBER	Better than 1E-18 UBER	Better than 1E-18 UBER	Data integrity
	Data protection upon power loss	Common	Yes	Yes	Data integrity
Physical robustness	Shock and vibration	Limited tolerance	Very high tolerance	Very high tolerance	Suitable for the harshest military and aerospace environments
	Temperature throttling	Typical	No	No	
	Operating temperature	Optimized for office environments	Optimized for wide temp swings	Optimized for wide temp swings	
	Form Factor	2.5", M.2, BGA	2.5", mSATA, BGA, Mobile, VPX, M.2*	2.5", Mobile*, BGA*, M.2*	Flexibility
	Space Application Variants	No	Yes	No	Suitable for high radiation environments
Supply Chain	Country of origin	Typically foreign	Built in US (DMEA-trusted)	Built in US (DMEA-trusted)	Trusted manufacturer
	Controller origin	Typically foreign	ARMOR™ controller designed in the US	ARMOR controller designed in the US	Security customization and pedigree
	Commercial availability	1-2 years	Very long-term	Very long-term	Long-term supply continuity
Independent validation	3rd party certifications	FIPS 197[1]	FIPS 197	FIPS 197 CC (#CCEVS-VR-VID10783-2017)[2] FIPS 140-2[3] (#2884) CSfC HWFDE component listed[4]	Validated security
	Validated for sensitive data storage	No	No	Yes	Trusted component for 2-layer encryption implementation, such as CSfC

*Planned, but not launched.

[1] For more information on FIPS 197, please refer to http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] For more information CC (Common Criteria for Information Technology Security Evaluation), please refer to https://www.commoncriteriaportal.org/

[3] For more information on FIPS 140-2, please refer to http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[4] For more information on CSfC, Certified Solutions for Classified Program, please refer to https://www.nsa.gov/resources/everyone/csfc/

3309.04E-0418-TB-SSD-military

www.mrcy.com

mercury systems™

Innovation That Matters™

Corporate Headquarters
50 Minuteman Road • Andover, MA • 01810 USA
(978) 967-1401 • (866) 627-6951
Fax (978) 256-3599
www.mrcy.com

MADE IN AMERICA