2017 Edition

Innodisk's Solutions

Technical White Papers Designed for Engineers

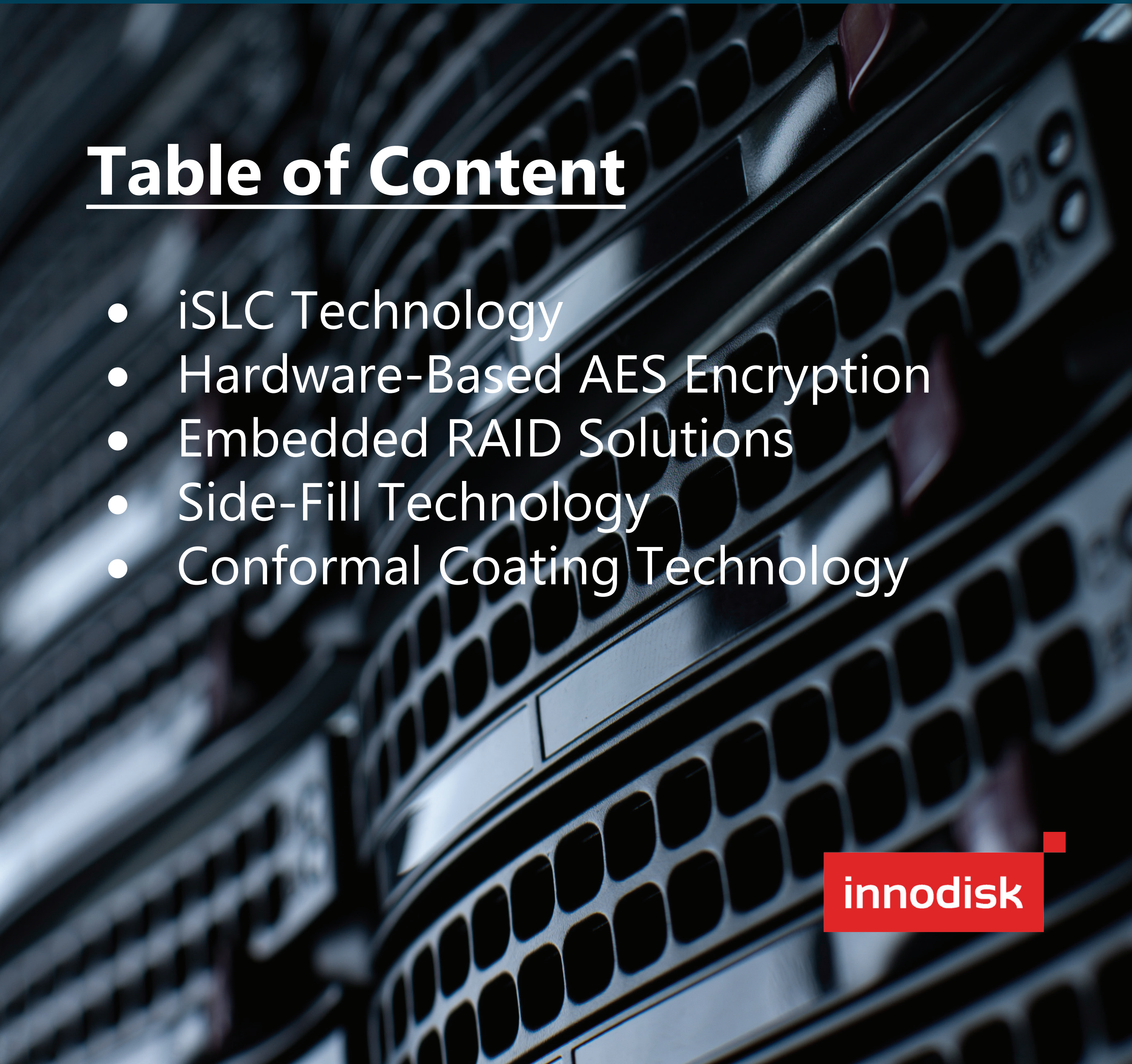


Table of Content

- iSLC Technology
- Hardware-Based AES Encryption
- Embedded RAID Solutions
- Side-Fill Technology
- Conformal Coating Technology

innodisk

White Paper

June 2017

iSLC

A Cost-Effective Superior-MLC Solution With Similar Performance, Endurance and Reliability to SLC

Introduction

This white paper presents Innodisk's iSLC technology as a cost-effective flash solution that increases the performance,reliability, and endurance of MLC NAND flash.

The lower price point that MLC commands over SLC is the trade-off, many users take while sacrificing performance and reliability.

The primary difference between SLC and MLC is the number of bits stored in each NAND cell. SLC stores 1 bit of data per cell, while MLC stores 2 bits per NAND cell. This allows SLC to be more fault-tolerant than MLC, while supporting more write cycles per cell. SLC flash can provide longer endurance and is a perfect choice for high-end applications. More key differences between SLC and MLC include Read,Write and Erase times, Program/Erase (P/E) cycles,and handling of errors bits. See Table 1.

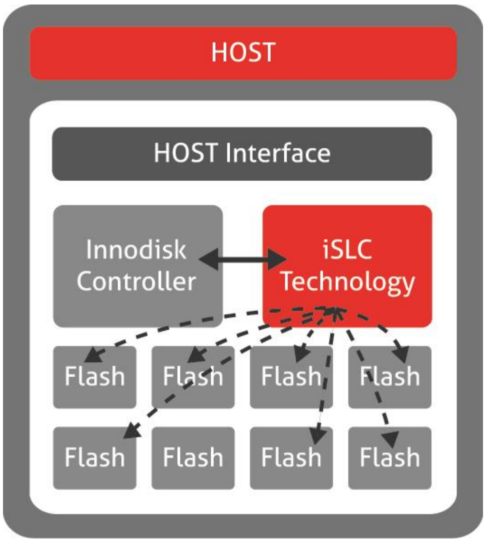


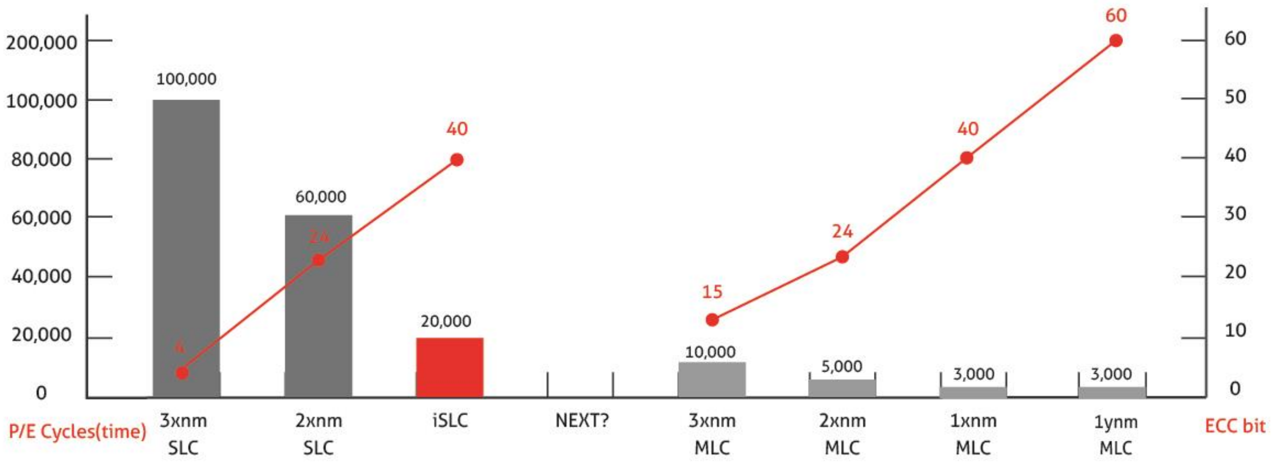
Table 1. Comparing SLC and MLC

	Program Page	Erase Block	P/E Cycle	ECC
SLC (24nm)	400μs	4ms	60K	24 bit/ 1024Bytes
MLC (15nm)	1400μs	5ms	3K	40 bit/ 1024Bytes

Since SLC NAND flash is more reliable and has longer endurance than MLC, so it is the ideal solution for the industrial and enterprise applications. However, due to economic pricing, MLC flash has become a very attractive, although concerns over performance and endurance still remain.

MLC's popularity was driven mainly by price. This has lead MLC NAND manufacturers to create larger capacities at better cost efficiency. The trade-off is a decrease in reliability and endurance seen below.
As NAND flash technology shrinks from 3Xnm to 2Xnm and 1Xnm, manufacturers require higher ECC capabilities to compensate for the decrease in reliability and endurance.

Figure 1 : MLC NAND Flash Trend

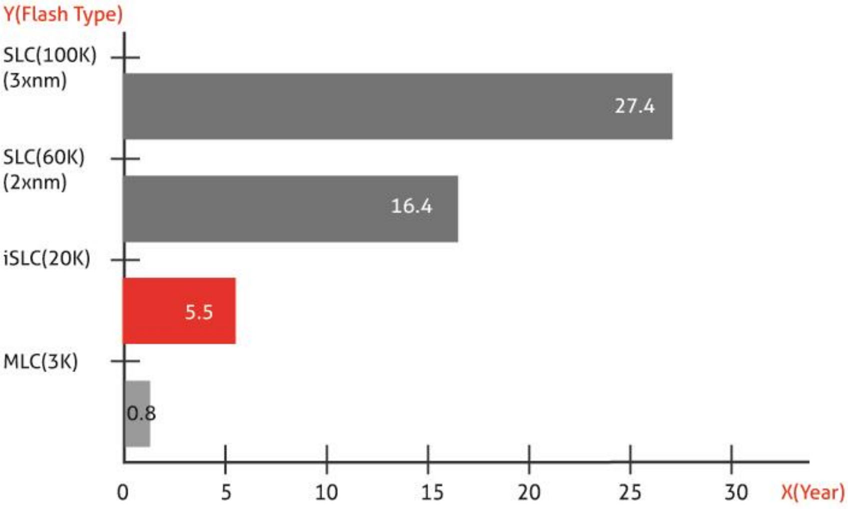


Innodisk has developed iSLC as a hybrid solution for those that require high-performance at a more affordable price point. Innodisk enhances superior MLC through screening and programming by our exclusive firmware. The firmware reprograms two bits per cell into one bit per cell, which increases the sensitivity of data between each level. This practice enables the NAND flash to perform similar to an SLC Flash based solution.

Innodisk's iSLC is designed to overcome this inherent deficiency in MLC NAND flash due to ever increasing demands on performance and endurance. With our iSLC technology, a 32GB capacity drive can write 10 full disk per day throughout a 5.5 year lifespan while the MLC can only last for 0.8 year life. See Figure 2.

iSLC offers an improvement over endurance of MLC to further suit the needs of industrial SSD applications such as Industrial PC, kiosks, Point-of-Sale (POS) systems, embedded systems, and servers.

Figure 2: iSLC increase demands on endurance.

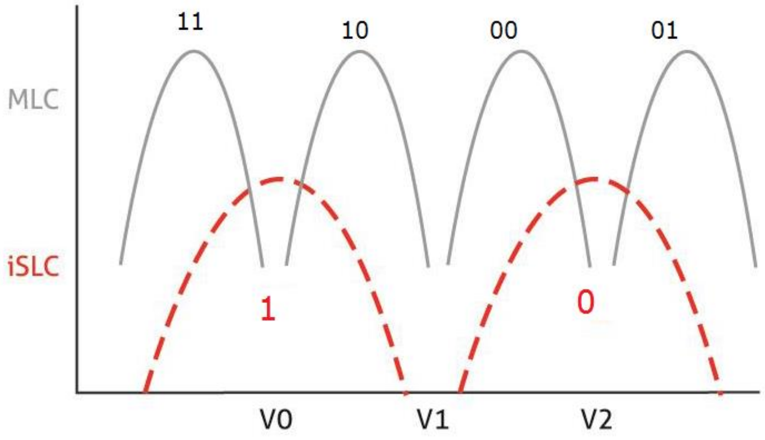


Note: The above diagram is based on a test environment for a 100% sequential write.
Example: Write 32GB x 10 time/day=320GB/day

How iSLC Works

As stated, the purpose of iSLC is to increase the SSD's lifespan, and keep costs down by finding the right balance between Performance, Price, Capacity, Endurance and Reliability – in other words, performing as close as possible to SLC flash, but costing as close as possible to MLC flash. How is this accomplished?

Figure 3: iSLC firmware technology empower MLC



Innodisk uses specially designed, in-house firmware to force to the MLC flash to act as SLC flash. Each SLC cell holds 1 bit – 1 or 0 – while MLC holds 2 bits – 00, 01, 10, 11. iSLC mimics SLC by only holding 1 bit in each NAND cell. See figure 3. This firmware tweak essentially allows the flash to perform close to that of SLC flash. This also increases endurance and data retention levels of the MLC NAND Flash.

Testing Data

The average endurance in iSLC can surpass 20,000 Program/Erase (P/E) cycles, which increases the lifespan of the drive over MLC Flash. Internal tests have been conducted at Innodisk Headquarters for a period of time without any device failure. Table 2 shows a non-stop burn test with measured variables. No errors occurred (data loss, data failure etc).

Table 2: Non-stop burn test of iSLC flash with measured variables

Sample	Capacity	Page Size	Average Erase Count	Error	Total Data Written (GB)	Total Test Time (Hours)
1	16GB	16K	43,001	0	381,002.32	2,389.18
2	32GB	16K	29,021	0	868,884.25	4,298.54

Our tests show the error bits of iSLC are much lower than MLC (see table 3). When Comparing the technology nodes of iSLC and MLC, 1xnm iSLC P/E cycle reached 20,000 times with error bits under 24 bits, while 1xnm MLC P/E cycle reached 3,000 times with error bits up to 40 bits. Table 3 shows ECC bits comparison between iSLC and MLC.

Table 3: ECC bits Comparison between iSLC and MLC

Flash Type	Capacity	Average Erase Count	ECC
iSLC	16GB	34,733	15 bits
MLC	16GB	6,280	40 bits

Write performance for iSLC NAND flash is about 10% slower than SLC NAND Flash while MLC NAND flash is approximately 50% slower than SLC NAND flash. This is a significant jump in performance over typical MLC solutions (see table 4).

Table 4: Comparing the Write performance for SLC, iSLC and MLC on SATA III

Technology	1 CH	2 CH	4 CH
SLC	NA*	110	230
iSLC	50	100	230
MLC	20	40	140

*SLC starts with 2 channels.

Conclusion

iSLC strikes a good balance between affordability and performance. With the increased number of P/E cycles, product lifespan is boosted to seven times that of similar MLC devices; while iSLC performance is closer to SLC levels. These factors all all key in making iSLC the ideal storage solution for applications such as point of sales systems and embedded IPCs, where budget-friendly alternatives are more attractive compared to SLC price ranges.

Innodisk's 3IE4 series includes the following :

- 2.5" SATA SSD
- CFast
- mSATA
- SATA Slim
- ServerDOM
- M.2
- SATADOM

About US

Innodisk is a worldwide leading provider of data storage and memory module solutions for industrial and mission-critical applications. Leveraging in-house engineering and R&D expertise with a keen insight on industry trends, Innodisk's solid-state drive (SSD) technologies provide enhanced, vertically-integrated data storage solutions. Our advanced Flash-based data storage and DRAM memory solutions meet stringent aerospace and defense application requirements, and are also widely used in industrial applications and embedded systems. Innodisk offers customized solutions, from unique form factors to special firmware designs, and our support team of hardware, software and firmware engineers is always ready to tailor the right solution to each customer's needs. Innodisk continually strives for innovation, while providing system integrators and end customers with the best service in the industry.

Innodisk Corporation

5F., NO.237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Phone:+886-2-7703-3000
Fax:+886-2-7703-3555
E-Mail:sales@innodisk.com

innodisk

White Paper

Hardware-based AES Encrypted Storage Solution

The AES hardware-encrypted SSD can reliably encrypt and decrypt data, while TCG OPAL 2.0 compliance offers flexible data access management as well as additional data security.

Introduction

Secure data encryption is essential for a wide variety of mission-critical applications. The protection of confidential information must be applied in situations involving military and civilian security. These scenarios require comprehensive safeguards to protect sensitive data.

Advanced Encryption Standard (AES) hardware-encrypted SSDs offer a proven and efficient method of encrypting data. TCG OPAL 2.0 compliance enables additional security layers and extended user management options.

Because of its complexity, it is not possible to brute-force the AES algorithm using any current or foreseeable technology. There are however other ways to crack the cipher; many of which can be addressed by applying hardware-based encryption as opposed to a software solution.

This paper will expand on this issue and other challenges such a data management, while also giving a more thorough explanation on the different features of AES and the related tools and standards.

Background

The theoretical framework for block ciphers such as AES was proposed in the 1940s, while the first widespread use started in the 1970s with AES's progenitor Data Encryption Standard (DES). DES was abandoned in the beginning of the 2000s as it was seen as unreliable.

The American National Institute of Standards and Technology (NIST) adopted AES, also known as Rijndael after its two inventors, in 2002. It was a specification for electronic data encryption and was chosen for its optimal balance between performance and security. The algorithm was the first of publicly available ciphers to be approved by the US National Security Agency (NSA) to protect classified information.

The hardware encrypted drive utilizes a built-in AES 256-bit encrypted engine located in the controller. The AES engine confirms to the AES algorithm (certificate No. 2474), the Deterministic Random Bit Generator (DRBG) algorithm (certificate No. 337), and the Secure Hash Standard (SHS) algorithm (certificate No. 2093).

Challenges

Challenges pertaining to SSDs and data security can be separated into three categories: secure data encryption, software encryption issues and management.

Secure Data Encryption

The main challenge with data encryption is keeping the encrypted data safe. This means being safe from brute-force attacks and other cracking attempts. The encryption level not only has to handle current threats, but also potential future decryption techniques and the threat that comes along with exponentially growing computational power.

Another aspect to consider is how to render the data unusable if the storage drive is compromised. Because there may be no time limit, there is an increased risk of the encryption being cracked, and as such, the encrypted data must be sanitized quickly.

Limitations of Software Encryption

Software encryption is a reliable method to secure data and is easily implemented, but there are drawbacks:

- Lowers system performance: As all encryption and decryption is handled by the CPU, system performance slows down when data is written or read.
- More vulnerable: Software encryption is only as strong as the system it operates on; a flaw in the OS can easily be used to break the encryption. In addition, it is naturally susceptible to viruses and malware and more prone to human error, such as the user altering or turning off the encryption.
- Unencrypted data: There might be files and data that are hidden and will remain unencrypted.
- OS dependence: The software is dependent on the OS, thus limiting what software can be used.

Management

If several users are accessing the drive, simply encrypting all the data might not be enough as each user has a different level of access, requiring different access ranges.

Solutions

Hardware AES Security

AES Encryption Key

Data encrypted with the 256-bit AES key is protected behind an algorithm that with today's technology is all but impossible to crack. While theoretical attacks have been shown to be possible, they are nowhere near feasible as it would take billions of years to brute force.

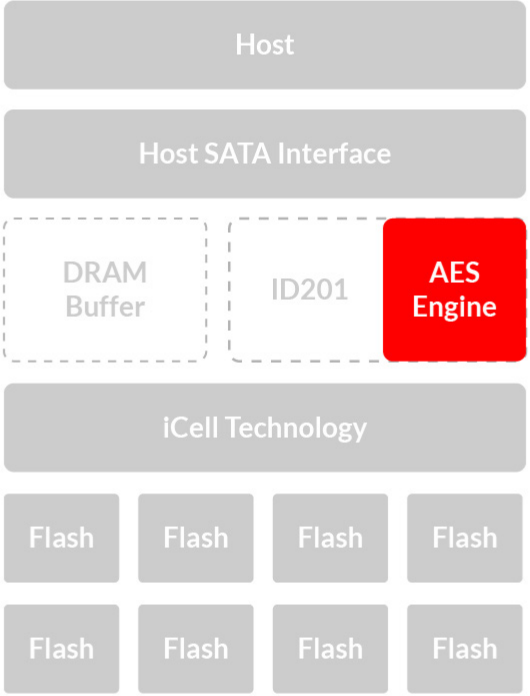


Figure 1: Hardware-based 256-bit AES engine in controller

The AES engine is a hardware design that is built inside the controller (see figure 1), in other words, there is no impact on CPU performance, as the controller will handle all encryption and decryption.
Hardware-encryption also means that the process is fully OS independent, as it does not require compliance with any system or software.

It is not possible to observe the encryption process itself, meaning the user cannot see the encrypted data, as all data that is read will already have been decrypted.

When the SSD controller leaves manufacturing, a series of random numbers will already be generated as the AES key, which is then stored in the NAND flash and is only known by the drive itself. The data will be encrypted and decrypted with this internal AES 256-bit key for all the data written to and read from the device. SSDs with internal AES Encryption Key operate just like normal SSDs.

ATA Security Authorized Key

ATA security features are a set of commands that can help the user manage storage devices, and is accessed through the BIOS (see table 1).

In order to complete the physical security layer of protection, the AES encryption needs to be bundled with the ATA Security command. This is done by enabling an ATA authorized key, which offers an authentication for the drive owner to lock or unlock the SSD for read or write commands. If the authorized key is not set, the SSD will appear to behave like a normal SSD.

Unlike the AES key, the authorized key must be set by the user via BIOS configuration. The ATA Security Password has to be entered with each power cycle and only when correctly entered will the SSD be accessible.

Command	Command Code
SECURITY SET PASSWORD	0XF1
SECURITY UNLOCK	0XF2
SECURITY ERASE PREPARE	0XF3
SECURITY ERASE UNIT	0XF4
SECURITY FREEZE LOCK	0XF5
SECURITY DISABLE PASSWORD	0XF6

Table 1: ATA security command set

AES and ATA Key Combination

With the ATA security authorized key set, not only is the logical data safely encrypted, but the physical drive is protected as well. In other words, if the SSD falls into the wrong hands, the SSD cannot be opened without the password. The information stored inside the NAND flash is safe because all that can be read is randomized, encrypted data.

When the power is switched on, the user is required to enter an ATA security password to get access to the SSD, and the user is only then allowed to send read or write commands with the internal AES Encryption Key for encryption or decryption (see Figure 2).

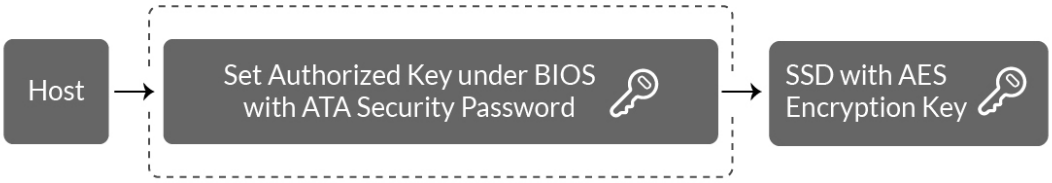

Host
Set Authorized Key under BIOS with ATA Security Password
SSD with AES Encryption Key

Figure 2: AES encryption works along with ATA security password to achieve full protection of the SSD

Sanitizing Drives

Sanitizing means rendering encrypted data useless by changing the AES encryption key. This operation is initiated through the ATA Cryptographic Erase command (see Table 2). After the key has been altered, the data written with the previous key would appear to be random, incomprehensible data. This function also allows the user to verify that the hardware encryption actually works. The purpose of the ATA Cryptographic Erase command is to sanitize all user data and make it unreadable, leaving out time-consuming normal erase procedure that requires many cycles of data overwriting.

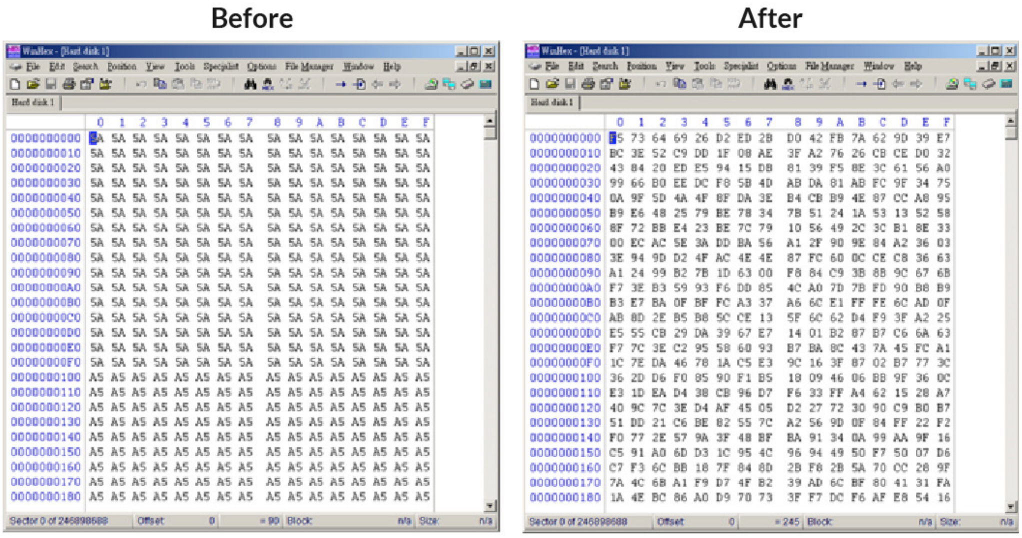
Field	Description	
FEATURE	0011h	
COUNT	Bit	Description
	15:5	Reserved
	4	FAILURE MODE bit
	3.0	Reserved
LDA	Bit	Description
	47:32	Reserved
	31:0	Shall be set to 4372_7970h(DWord)
DEVICE	Bit	Description
	7	Obsolete
	6	N/A
	5	Obsolete
	4	Transport Dependent
	3:0	Reserved
COMMAND	7:0 B4h	

Table 2: ATA Cryptographic Erase command

For example:

1. The user receives a self-encrypted SSD and inputs 'AA55', the user will read the same data pattern as AA55 as the SSD internally encrypts and decrypts the data with Key A which is generated by the firmware before leaving the factory.
2. The A key is then changed to Key B with ATA Cryptographic Erase command. At this time, the user is only able to read data as a random string of alphanumerics (See figure 5).
3. If you write AA55 with Key B again, then of course, the user will get AA55 which had already been decrypted by key B.

Both Key A and Key B are invisible to the user as they are randomly generated by the SSD firmware.



Before

WinHex - [Hard disk 1]
File Edit Search Position View Tools Specialist Options File Manager Window Help
Hard disk 1

```
              0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0000000000   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000010   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000020   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000030   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000040   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000050   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000060   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000070   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000080   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000090   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000A0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000B0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000C0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000D0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000E0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
00000000F0   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A
0000000100   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000110   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000120   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000130   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000140   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000150   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000160   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000170   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
0000000180   A5 A5 A5 A5 A5 A5 A5 A5  A5 A5 A5 A5 A5 A5 A5 A5
Sector 0 of 246898688   Offset   0   = 90   Block:   n/a   Size:   n/a
```

AA55 written with Key A

After

WinHex - [Hard disk 1]
File Edit Search Position View Tools Specialist Options File Manager Window Help
Hard disk 1

```
              0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0000000000   F5 73 64 69 26 D2 ED 2B  D0 42 FB 7A 62 9D 39 E7
0000000010   BC 3E 52 C9 DD 1F 08 AE  3F A2 76 26 CB CE D0 32
0000000020   43 84 20 ED E5 94 15 DB  81 39 F5 8E 3C 61 56 A0
0000000030   99 66 B0 EE DC F8 5B 4D  AB DA 81 AB FC 9F 34 75
0000000040   0A 9F 5D 4A 4F 8F DA 3E  B4 CB B9 4E 87 CC A8 95
0000000050   B9 E6 48 25 79 BE 78 34  7B 51 24 1A 53 13 52 58
0000000060   8F 72 BB E4 23 BE 7C 79  10 56 49 2C 3C B1 8E 33
0000000070   00 EC AC 5E 3A DD BA 56  A1 2F 90 9E 84 A2 36 03
0000000080   3E 94 9D D2 4F AC 4E 4E  87 FC 60 0C CE C8 36 63
0000000090   A1 24 99 B2 7B 1D 63 00  F8 84 C9 3B 8B 9C 67 6B
00000000A0   F7 3E B3 59 93 F6 DD 85  4C A0 7D 7B FD 90 B8 B9
00000000B0   B3 E7 BA 0F BF FC A3 37  A6 6C E1 FF FE 6C AD 0F
00000000C0   AB 8D 2E B5 B8 5C CE 13  5F 6C 62 D4 F9 3F A2 25
00000000D0   E5 55 CB 29 DA 39 67 E7  14 01 B2 87 B7 C6 6A 63
00000000E0   F7 7C 3E C2 95 58 60 93  B7 BA 8C 43 7A 45 FC A1
00000000F0   1C 7E DA 46 78 1A C5 E3  9C 16 3F 87 02 B7 77 3C
0000000100   36 2D D6 F0 85 90 F1 B5  18 09 46 06 BB 9F 36 0C
0000000110   E3 1D EA D4 38 CB 96 D7  F6 33 FF A4 62 15 28 A7
0000000120   40 9C 7C 3E D4 AF 45 05  D2 27 72 30 90 C9 B0 B7
0000000130   51 DD 21 C6 BE 82 55 7C  A2 56 9D 0F 84 FF 22 F2
0000000140   F0 77 2E 57 9A 3F 48 BF  BA 91 34 0A 99 AA 9F 16
0000000150   C5 91 A0 6D D3 1C 95 4C  96 94 49 50 F7 50 07 D6
0000000160   C7 F3 6C BB 18 7F 84 8D  2B F8 2B 5A 70 CC 28 9F
0000000170   7A 4C 6B A1 F9 D7 4F B2  39 AD 6C BF 80 41 31 FA
0000000180   1A 4E BC 86 A0 D9 70 73  3F F7 DC F6 AF E8 54 16
Sector 0 of 246898688   Offset   0   = 245   Block:   n/a   Size:   n/a
```

Read as random data with Key B

Figure 3: Using the ATA Cryptographic Erase Command to alter the AES encryption key

TCG OPAL 2.0

With TCG OPAL 2.0 a new layer is added on top of the basic setup explained above. It is a set of security protocol specifications defined for industrial data storage devices, and are published by the Trusted Computing Group's Storage Work Group. To take full advantage of TCG OPAL 2.0, the standard involves not only SSD vendors, but also system installation and management. Third party encryption software and utilities are also required to fully implement OPAL functions.

TCG OPAL states that SSDs must be self-encrypted with an AES hardware encryption engine. In-addition, the user is required to pass a boot-up authorization procedure that is triggered after the ATA password has been verified. That is to say, when the system is switched on, a pre-boot shadow image will be shown to safeguard the real Master Boot Record (MBR). Once the authorized password is entered, the real MBR and OS will be loaded for further authority management (see Figure 4).

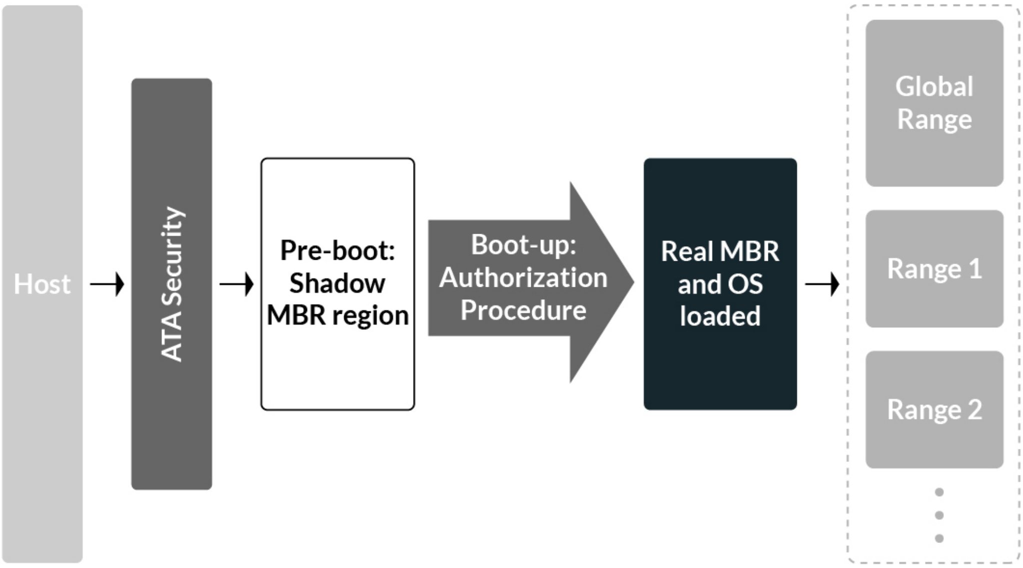


Figure 4: TCG OPAL 2.0 Operation Process

OPAL also allows for the partition of access control to read/write/erase independent LBA ranges for individual users (see Figure 5). "Global Range" is the default settings that encompass the whole user data area. In the figure below, the drive has been altered such that LBA Range 1 and 2 can only be accessed by user 2 and 3 respectively.

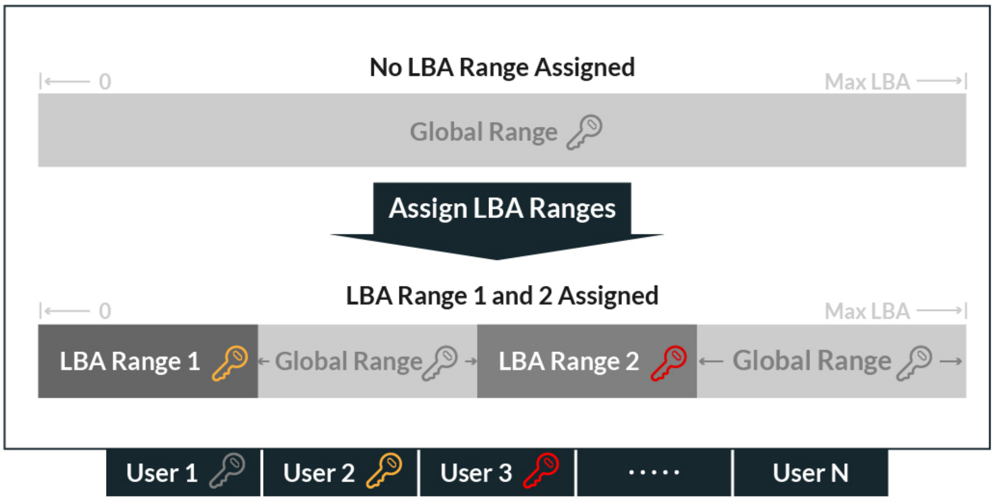


Figure 5: LBA Range Operation

SSD compliant with TCG OPAL 2.0 enables the use of both Manufacturer Secure ID (MSID) and Physical Secure ID (PSID):

- MSID: MSID works as a master ID that must be input to access the real MBR. After accessing it for the first time, the user can then set up passwords for individual LBA ranges and create a multiple-user system.
- PSID: PSID is a command that can be input to revert the SSD back to default factory settings. This means that the AES Encryption Key will be permanently changed and user data will be randomized, affectively sanitizing the drive. At the same time, the main password will revert to MSID.

Conclusion

TCG OPAL 2.0 certified AES hardware encryption offers strong, multilayered protection for confidential data.

By keeping the encryption/ decryption process in the SSD controller, the user avoids the risks and drawbacks associated with software encryption such as OS weaknesses to cracking, OS dependence and reliance on system CPU.

If the data you are storing is critical, a hardware-based AES solution will always be the more secure choice.

The Innodisk Solution

Innodisk AES Product Family: 3MG2-P

Various Form Factors With AES Function	Hardware-based 256 Bit AES Key	Data Destroy	TCG OPAL 2.0	IEEE 1667
- 2.5" SSD - mSATA - SATA Slim - M.2	3MG2-P AES provides a hardware-based mechanism for data encryption/ decryption	By altering the AES Key, data is destroyed in less than a second	Independent access to read/ write/ erase specific data areas (LBA ranges)	Compliant with TCG OPAL for IEEE 1667

Innodisk Corporation

5F., NO. 237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com

White Paper

Embedded RAID 1 Solution

It is difficult for embedded system integrators to find viable solutions to their storage expansion projects. This is where Redundant Array of Independent Disks (RAID), specifically RAID level 1, comes in as a simple and proven method to keep data safe in case of disk failure. Innodisk offers compact, cost efficient hardware RAID solutions that are designed for the embedded market.

Introduction

As opposed to traditional enterprise applications, there are several unique challenges facing the embedded system integrator when deciding on a RAID solution: limited space, system constraints, data integrity issues, harsh operating conditions. These conditions render standard RAID rather impractical for most embedded applications.

With embedded systems there is no one-size-fits-all solution, so the system integrator has to find a customized solution while at the same time keeping costs low. And if failure were to occur, it is imperative that the operator is notified and that the system can be fixed without compromising data integrity.

This paper aims to take a closer look at what constitutes the above mentioned difficulties, and then present the reader with a viable and cost effective solution.

Background

The embedded industry is diverse and encompasses widely different areas. Yet, there are certain common themes that are shared across the industries. With the ubiquity of IoT (Internet of Things) there is an ever growing demand for increased connectivity and modernization. Whether it is defense, automation, aerospace or in-vehicle, every operator faces similar difficulties when it comes to storage expansion. Space onboard the vehicle or platform is already fully utilized, and there is little to no room for new systems. Any expansion or upgrade might thus turn into a very costly affair.

However, every operator still faces unique challenges, whether it is robustness, data security, accessibility et cetera. As such there is a need for customization that might not be offered by the larger embedded vendors.

With a tailor-made solution, the operator can ensure there is only negligible interference with already onboard systems, the data is safe and the environmental footprint is small; all the while having a low impact on the bottom line.

Challenges

Data Integrity

Data Integrity is essential in the embedded industry as a sudden failure can mean costly down time and even pose a risk to operation and personnel. In the event of disk failure, there has to be a system of notification as well as easy accessibility for disk replacement.

Size Constraints

A standard enterprise RAID setup would normally include high capacity storage in a more expensive and bulky package. For embedded system integrators capacity requirements often come secondary to space-limitation concerns.

Software RAID vs Hardware RAID

Standard RAID is also normally built through software, which means that the RAID building process is handled by the CPU. However, in embedded systems CPUs are primarily chosen for their energy efficiency and small footprint – RAID building can as such severely impact processing speeds.

Harsh Environments

Industrial systems see operation in remote and inhospitable environments. To ensure data integrity, the components need to withstand large temperature variations, electromagnetic interference, and shock and vibration.

Solutions

RAID 1

One of the embedded market's main concerns is data integrity. To address this, RAID 1 works by simply mirroring two SSDs, so in the event of one disk failing (degraded mode), all data is still intact and accessible (see figure 1). While writing speed remains the same as a single disk setup, RAID1 increases reading speed by having the same set of data available on both disks.

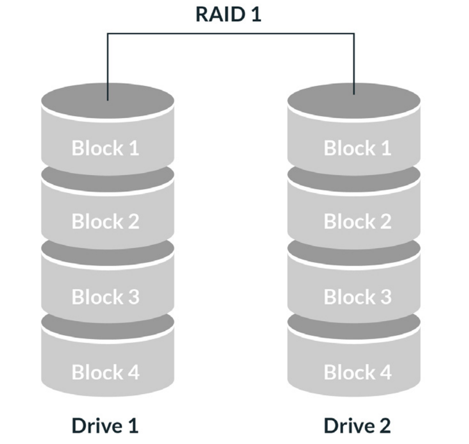


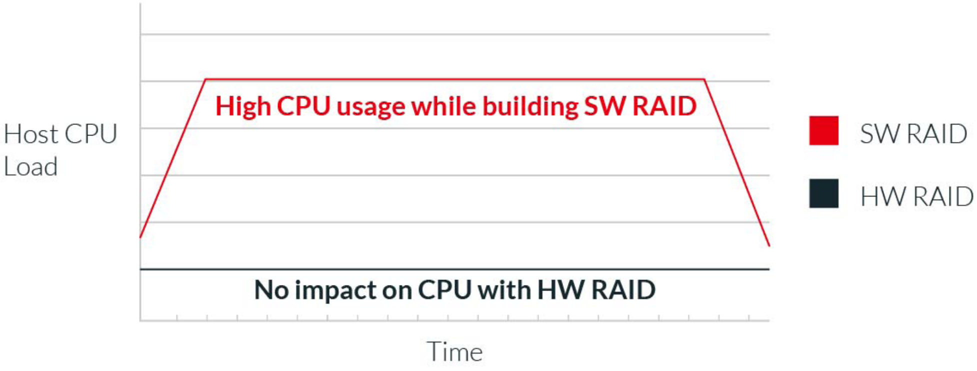
Figure 1:RAID 1 mirrored disks

Compactness

Space limitations are easiest solved by utilizing compact form factors. The smallest RAID setup simply requires an array module with two attached SSDs – allowing for a much easier integration.

Hardware RAID

Innodisk offers hardware RAID where RAID is built by an integrated controller on the module. This means that disk mirroring happens without relying on the host CPU – ensuring that there is no interference with ongoing CPU operations (see graph 1). The process is fully automated and will kick in as soon as a new SSD module is installed.



Graph 1: Difference in CPU usage for hardware and software RAID

Monitoring Software

With an efficient monitoring system, the user can access SSD SMART info at any time. A notification system will alert the user if anything out of the ordinary were to occur – which in turn allows the user to fix the problem before data is lost.

Innodisk's iRAID software offers these features, while also allowing for separate control of up to five array modules.

Robustness

For operation in extreme environments, Innodisk modules are tested and proven for use in industrial temperatures ranges from -40°C to 85°C, and in vibrations up to 5G@7~2000Hz and shock up to 50G@0.5ms.

Conclusion

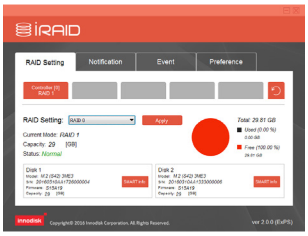
Every embedded application is unique and requires a unique solution, yet there are certain challenges that are commonly shared such as limited space, system restraints and harsh conditions. With a compact embedded RAID 1 setup, these challenges can largely be mitigated. Hardware RAID ensures little to no impact on system performance; monitoring software will alert users and keep them up to date; and industrial robustness ensures reliability.

Innodisk's RAID 1 Solution

Innodisk provides flexible form factor and interface alternatives:

Form Factor	mPCIe/mSATA	M.2	2.5”	Standard PCIe x 4
Input Interface	PCI Express 2.0 SATA III	SATA III	SATA III	PCI Express 2.0
Output Interface	SATA III	SATA III	SATA III	SATA III
Output Connector	7 Pin SATA	7 Pin SATA	M.2 2242/2260/2280 mSATA	M.2 2242/2260/ 2280/22110

iRAID is Innodisk's in-house designed RAID and SSD monitoring software.



RAID Setting: RAID 0

Current Mode: RAID 1

Capacity: 29 [GB]

Status: Normal

Total: 29.81 GB

Used (0.00 %) 0.00 GB

Free (100.00 %) 29.81 GB

Disk 1
Model: M.2 (S42) 3ME3
S/N: 20160510AA1726000004
Firmware: S15A19
Capacity: 29 [GB]

Disk 2
Model: M.2 (S42) 3ME3
S/N: 20160310AA1333000006
Firmware: S15A19
Capacity: 29 [GB]

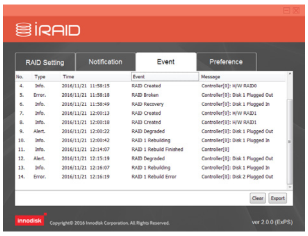
Copyright© 2016 Innodisk Corporation. All Rights Reserved. ver 2.0.0 (ExPS)

Monitor

Allows you to quickly asses the status of your RAID setup

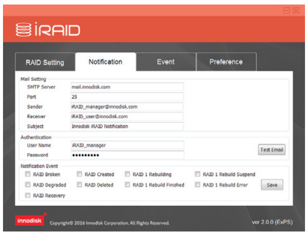
Records

Access detailed records of your devices



No.	Type	Time	Event	Message
4.	Info.	2016/11/21 11:58:15	RAID Created	Controller[0]: H/W RAID0
5.	Error.	2016/11/21 11:58:18	RAID Broken	Controller[0]: Disk 1 Plugged Out
6.	Info.	2016/11/21 11:58:49	RAID Recovery	Controller[0]: Disk 1 Plugged In
7.	Info.	2016/11/21 12:00:13	RAID Created	Controller[0]: H/W RAID1
8.	Info.	2016/11/21 12:00:18	RAID Created	Controller[0]: H/W RAID1
9.	Alert.	2016/11/21 12:00:22	RAID Degraded	Controller[0]: Disk 1 Plugged Out
10.	Info.	2016/11/21 12:00:42	RAID 1 Rebuilding	Controller[0]: Disk 1 Plugged In
11.	Info.	2016/11/21 12:14:07	RAID 1 Rebuild Finished	Controller[0]
12.	Alert.	2016/11/21 12:15:19	RAID Degraded	Controller[0]: Disk 1 Plugged Out
13.	Info.	2016/11/21 12:16:07	RAID 1 Rebuilding	Controller[0]: Disk 1 Plugged In
14.	Error.	2016/11/21 12:16:19	RAID 1 Rebuild Error	Controller[0]: Disk 2 Plugged Out

Copyright© 2016 Innodisk Corporation. All Rights Reserved. ver 2.0.0 (ExPS)



Mail Setting
SMTP Server: mail.innodisk.com
Port: 25
Sender: iRAID_manager@innodisk.com
Receiver: iRAID_user@innodisk.com
Subject: Innodisk iRAID Notification

Authentication
User Name: iRAID_manager
Password: ●●●●●●●●●●

Notification Event
□ RAID Broken □ RAID Created □ RAID 1 Rebuilding □ RAID 1 Rebuild Suspend
□ RAID Degraded □ RAID Deleted □ RAID 1 Rebuild Finished □ RAID 1 Rebuild Error
□ RAID Recovery

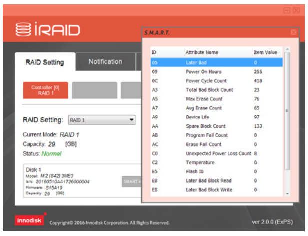
Copyright© 2016 Innodisk Corporation. All Rights Reserved. ver 2.0.0 (ExPS)

Notifications

Tweak settings to notify operator when certain parameters are met

SMART

Easily access the SMART information of your storage devices



RAID Setting: RAID 1

Current Mode: RAID 1

Capacity: 29 [GB]

Status: Normal

Disk 1
Model: M.2 (S42) 3ME3
S/N: 20160510AA1726000004
Firmware: S15A19
Capacity: 29 [GB]

ID	Attribute Name	Item Value
05	Later Bad	0
09	Power On Hours	255
0C	Power Cycle Count	418
A3	Total Bad Block Count	23
A5	Max Erase Count	76
A7	Avg Erase Count	65
A9	Device Life	97
AA	Spare Block Count	133
AB	Program Fail Count	0
AC	Erase Fail Count	0
C0	Unexpected Power Loss Count	8
C2	Temperature	0
E5	Flash ID	0
EB	Later Bad Block Read	0
EB	Later Bad Block Write	0

Copyright© 2016 Innodisk Corporation. All Rights Reserved. ver 2.0.0 (ExPS)

Innodisk Corporation

5F., NO.237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com

White Paper

Side Fill Technology

Harsh environmental conditions can fracture and damage ball grid arrays (BGA) and solders by inducing thermal and mechanical stress. Innodisk's side fill technology is a simple, well-tested and cost efficient solution whereby applying resin to three sides of the DRAM integrated circuits (IC) the allover robustness of the module is strengthened.

Introduction

With the continuous demand for smaller DRAM modules, the size of BGAs has similarly decreased. What this means is that the BGA solder has become smaller and consequently less robust. At the same time DRAM modules see operation in increasingly inhospitable environments, where mechanical stress from shock, vibration and severe thermal variations are part of daily operation.

There are measures that can be taken to mitigate these challenges, among them are side fill and underfill. Due to the ambiguity surrounding these two terms, this paper defines the technologies as such :

- Side fill: a resin is applied to 3 of the DRAM IC sides to strengthen the connection between the printed circuit board (PCB) and the BGA
- Underfill: using a resin to completely fill the space between the PCB and the BGA

This paper aims to explain the challenges facing the embedded industry in harsh environments and why side fill is the optimal solution.

Background

Side fill as a concept was first proposed in the 1960, and although technology has taken great strides since then, the basic concept of side filling remains the same. The technology did not see wide usage at the time, as PCBs of the era was generally robust enough. However, computers are now commonplace in even the most challenging environments – making requirements for robustness higher than ever.

Challenges

What smaller PCBs consequently lead to is a decrease in size of BGA balls and pitch. This translates into an overall reduced robustness of the link between the PCB and the BGA.

Many embedded applications see rough thermal cycling, such as satellites moving from sunlight to the cold dark side of the earth in cycles just over an hour. These temperature changes lead to a constant cycle of expansion and contraction that can eventually cause damage to the onboard modules - and with only a short distance between the PCB and BGA, there is not much leeway. This is especially true for modules with thermal mismatching where the material in the PCB and the BGA have different expansion/ contraction rates.

Many systems undergo shock and sustained vibration, e.g. in vehicles operating in rough terrain or airplanes in turbulence etc. This can cause solder points to gradually weaken until they eventually fail, and can also lead to fractures in the PCB.

Solution

Side fill

Side fill is a proven and cost efficient method to increase PCB to BGA connection robustness. Tension tests show that with side fill applied, modules tolerate up to 2 times the force before finally coming loose.
The resin will also function as a thermal expansion absorber; in other words when the module is undergoing expansion/contraction, the resin allows for more movement while maintaining BGA connection integrity. The resin also functions as a heat sink by increasing heat dissipation, thus raising the threshold for thermal variations.

With the resin applied, mechanical and thermal stress is more evenly distributed, causing less stress on each individual solder point and increasing overall endurance.

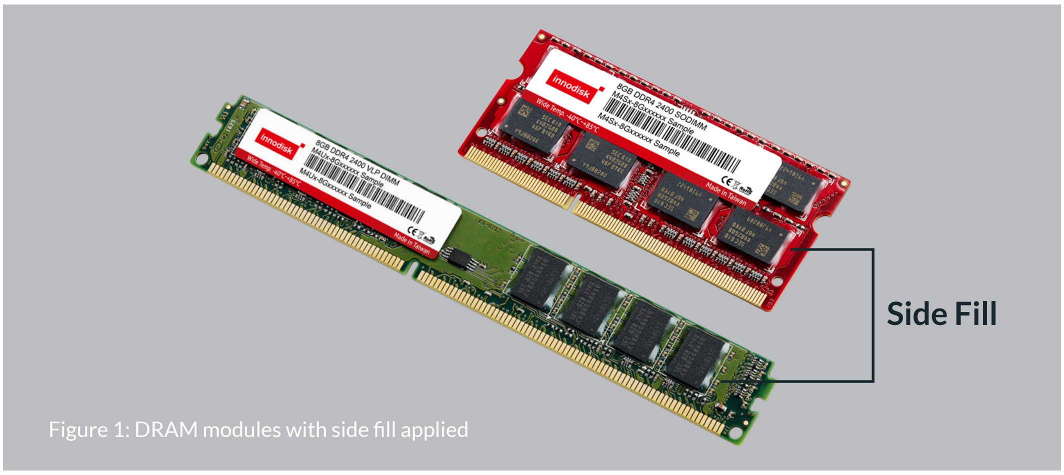


Figure 1: DRAM modules with side fill applied

The advantages of side fill vs underfill

While underfill in theory offers the same benefits as side fill, there are certain advantages that make the latter the stronger candidate.

- More cost efficient: side fill uses less resin and application time is faster, thus lowering costs
- Easier to repair: compared to underfill, the resin is easier to remove when it is only applied to the sides of the IC & PCB. This also lowers the risk of damage to the PCB when the module undergoes repair
- Lighter weight: Minimizing the burden on weight-sensitive devices
- Air pockets: By filling the entirety of the space between the BGA and the PCB, there is an increased risk for trapped air pockets. By only adding resin to three sides, this problem is effectively mitigated

Conclusion

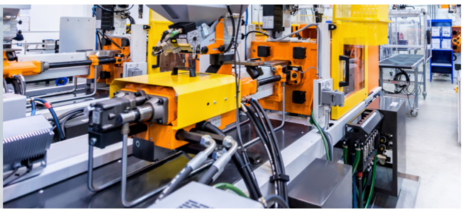
Moore's law is still in effect; as such devices will keep decreasing in size and therefore lose some of the robustness that was inherent in larger legacy modules. Addressing this challenge is essential for DRAM modules that see operation in extreme environments. This is where side fill comes in as a simple and well-proven solution. In a simple cost vs benefit analysis, side fill easily comes out on top as by device failure the impact on the bottom line is much more severe.

Vertical Markets and Product Series

Side fill technology is especially suited for these vertical markets:

In-vehicle

Aerospace & Defense



Automation

Side fill is optional for Innodisk products, however it is highly recommended for the below mentioned product series.

0.738" Very low-profile series (VLP)

Rugged Rugged DRAM

+85°C -40°C Wide Temperature series

Innodisk Corporation

5F., NO.237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com

innodisk

White Paper

Conformal Coating

Conformal coating is a well-tested method to protect DRAM modules from corrosion, wear and other damage by applying a thin, isolating layer over the module.

Introduction

With the growing trend of digitalization there is a steady increase in the use of DRAM modules and other components in hostile and remote environments. Modules are also getting ever more compact, which means smaller track spacing on the printed circuit board (PCB). This development presents a number of challenges to the system integrator.

In addition to thermal and mechanical induced stress, the modules are also susceptible to humidity, chemicals, dust and other particles. These factors can lead to corrosion, short-circuiting and general wear – ultimately decreasing the lifespan of the module. In addition the smaller track spacing also increases the risk for short-circuiting.

By applying a thin layer of acrylics and silicone on the module, conformal coating can help protect against contaminants and increase product lifespan. While the two types of coating the paper addresses have their own advantages, they both increase module ruggedness when applied.

This paper will explain what constitutes these environmental challenges, and the benefits of conformal coating and how it is properly applied.

Background

Conformal coating is so named as the applied layer conforms to the profile of the circuit assembly. It is a measure that meets the demand for better protection of components in harsh environments. This is especially true for aerospace and military applications, where reliability is paramount and operations take place in every climate zone of the world.

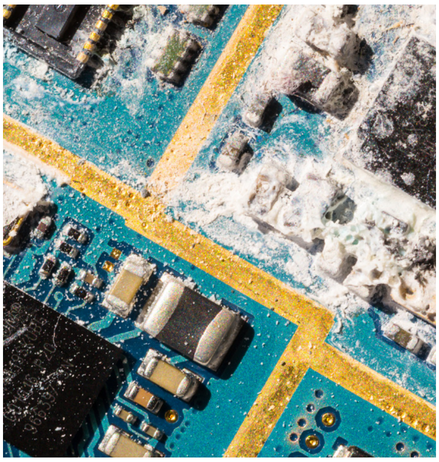
Operations in hot and dry areas are affected by particles such as sand and dust that can severely damage sensitive electronic equipment. Naval vessels operate in high-salinity environments where exposed components will quickly start corroding. Aircraft avionics is potentially even more mission-critical, as any damage to components can have drastic consequences.

There is also a high demand in civilian applications, such as sensitive medical equipment and CNC machinery where humidity is a high-risk factor.

Challenges

Challenges from harsh environments can be split in to two main categories, namely damage from corrosion and damage from short-circuiting.

Corrosion



Corrosion is a natural process where metal reacts with the environment and converts to a more chemically stable form. This happens through oxidation which will produce salts of the metal (e.g. rust) and other byproducts. Corrosion will lead to degraded material strength, which in turn can cause module failure.

Corrosion will happen as long as an oxidation agent (usually oxygen, O_2) is in place. However, once the metal comes in contact with water, electrical conductivity increases and the process speeds up. Any acid will corrode the metal even faster.

While dust and other small particles will not directly affect the corrosion process, they will still absorb humidity from the air and consequently start corroding any metal it comes in contact with.

Short-circuiting

Short-circuiting happens when electricity travels an unintended path between two points with little resistance, and can cause irreparable damage to the module. In the case of DRAM modules, this happens when moisture, damage from corrosion or any other material acts as a conductor between two points on the PCB or another source of electric current.

With the track spacing on the DRAM module getting smaller, the risk for short-circuiting increases.

Solutions

Conformal Coating Options

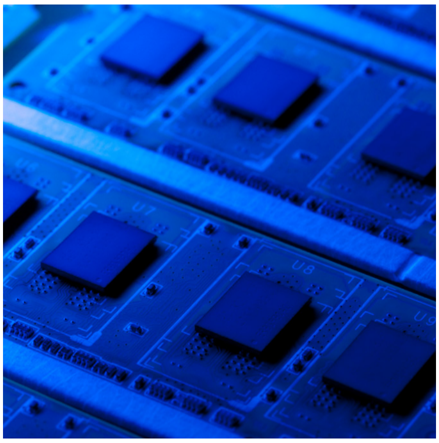
Conformal coating acts as a barrier between the harmful effects of the environment and the DRAM module. When choosing acrylics or silicones as a coating agent, it is important to first understand their respective advantages (see table 1).

Acrylics	Silicones
· Easy to remove when undergoing maintenance · Easy to re-apply · Good moisture resistance · High dielectric strength · Industrial temperature ranges (up to 85°C)	· High chemical resistance · Good moisture resistance · High dielectric strength · Very high temperature ranges (up to 200°C)

Table 1: Advantages of silicones and acrylics

As can be seen from the table above, acrylics are easy to apply and remove making it very convenient when the module undergoes maintenance. Silicones are able to withstand harsher conditions, but due to being resistant to most solvents and high heat, it is harder to remove for repair purposes. Both coatings offer high dielectric strength which means both insulation against the environment and protection against short-circuiting.

Coating Process



The coating is done in full accordance with IPC-J-STD-001 Rev F. Before the process begins the mating surfaces of the connector are properly masked. The coating is then sprayed on in a thickness of around 0.072mm, well within the range stated in IPC-J-STD-001. The process is repeated over several sessions with an hour in-between to allow the coating to cure. The curing itself is done through an automated UV light process.

Coating Removal

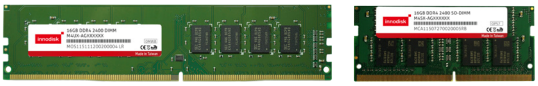
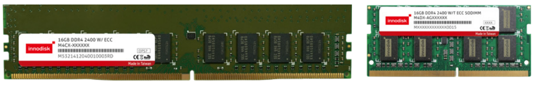
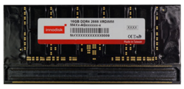
If modules need to undergo maintenance the coating first needs to be removed. This is done through ultra-sound which will cause bubbles to form in small cavities between the PCB and the coating. This in turn enables the easy removal of the coating from the module allowing further maintenance work to take place.

Conclusion

DRAM modules are becoming more prevalent in challenging environments; as such there is a growing demand for increased protection. Conformal coating is an effective measure that protects against humidity, dust, contaminants and other chemicals that can lead to corrosion, short-circuiting and other damages.

The Innodisk Solution

Conformal coating is a suitable addition to any system operating under challenging conditions. We recommend the below DRAM modules with conformal coating for an optimal, ruggedized solution:

Series	Product
Embedded Series	Unbuffered Long DIMM/ SODIMM 
	Unbuffered Long DIMM/ SODIMM with ECC 
Wide Temperature	Wide Temperature
	Wide Temperature with ECC
Rugged Series	Rugged DIMM
	XR-DIMM 

Innodisk Corporation

5F., NO. 237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com