Commercial Grade -240SE series Encrypted SSD

Product Manual

'TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments'

August 11, 2020

www.cactus-tech.com

The information in this manual is preliminary and is subject to change without notice. Cactus Technologies ® , Limited shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Cactus Technologies® makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Cactus Technologies® assume any liability arising out of the application or use of its products, and specifically disclaims any and all liability, including without limitation consequential or incidental damages.

Cactus Technologies® products are not designed, intended or authorized for use as components in systems intended for surgical implant into the body or in other applications intended to support or sustain life or for any application where the failure of a Cactus Technologies® product can result in personal injury or death. Users of Cactus Technologies® products for such unintended and unauthorized applications shall assume all risk of such use and shall indemnify and hold Cactus Technologies® and its officers, employees, subsidiaries, affiliates and distributors harmless against all claims, costs, damages, expenses and attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended and unauthorized use, even if such claim alleges that Cactus Technologies® was negligent regarding the design or manufacture of the part.

Table of Contents

1.Introduction to Cactus Technologies® Commercial Grade -240SE Series Encrypted SSD Products

Features:

- Solid state design with no moving parts
- Available in industry standard 2.5”, 9.5mm height form factor
- Capacities of 512GB and 1TB
- Compliant with Serial ATA 3.1 specifications
- ATA-8 ACS2 command set compatible
- Supports Serial ATA Generation I/II/III transfer rate of 1.5/3.0/6.0 Gbps
- Supports ATA SMART Feature Set
- Supports ATA Security Feature Set
- Supports Host Protected Area Feature Set
- Supports Data Set Management (TRIM)
- Supports NCQ w/ max. queue depth of 32
- Supports DevSLP
- FIPS 140-2 compliant hardware AES256 encryption
- Key management through SATA API
- FIPS 140-2 certified hardware HMAC, CMAC, SHA256, TRNG for enhanced security
- Available with regular SATA connector, Smiths Nebula® series rugged SATA connector or Amphenol R-SATA® series rugged connector
- ECC capable of correcting up to 66 bit errors per 1KB
- Enhanced error correction, < 1 error in 10^{14} bits read
- Voltage support: 5.0V±10%
- Available in Standard Temperature version at full SATA III transfer rates or in Extended Temperature version at full SATA II transfer rates

Cactus Technologies® Commercial SSD is a high capacity solid-state flash memory product that complies with the Serial ATA 3.1 standard and is functionally compatible with a SATA hard disk drive. Cactus Technologies® Commercial SSD provides up to 1TB of formatted storage capacity.

Cactus Technologies® Commercial SSD product uses high quality MLC NAND flash memory from well known vendors, such as Toshiba Corporation. In addition, it includes an on-drive intelligent controller that manages interface protocols, data storage and retrieval as well as ECC, defect handling and diagnostics, power management, and clock control. The controller's firmware is upgradeable, thus allowing feature enhancements and firmware updates while keeping the BOM stable.

The encryption engine in Cactus Technologies® Commercial SSD product is provided by eNOVA Corporation X-WALL MX+ device. This device has been certified to FIPS 140 level 2 and 3 standard. Level 2 certificate number is 3013 and the details are listed at the following NIST website:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3013

Level 3 certificate number is 3014 and the details are listed at the following NIST website:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3014

1.1. Supported Standards

Cactus Technologies® Commercial SSD is fully compatible with the following specification:

- ATA 8/ACS2 Specification published by ANSI
- Serial ATA 3.1 Specification published by the Serial ATA International Organization

1.2. Product Features

Cactus Technologies® Commercial SSD contains a high level, intelligent controller. This intelligent controller provides many capabilities including the following:

- Standard ATA register and command set (same as found on most magnetic disk drives).
- Manages details of erasing and programming flash memory independent of the host system
- Sophisticated defect managing capabilities (similar to magnetic disk drives).
- Sophisticated system for error recovery using powerful error correction code (ECC).
- Intelligent power management for low power operation.

1.2.1. Host and Technology Independence

Cactus Technologies® Commercial SSD appears as a standard SATA disk drive to the host system. The drive utilizes a 512-byte sector which is the same as that in an IDE magnetic disk drive. To write or read a sector (or multiple sectors), the host computer software simply issues an ATA Read or Write command to the drive as per the SATA protocol. The host software then waits for the command to complete. The host system does not get involved in the details of how the flash memory is erased, programmed or read as this is all managed by the built-in controller in the drive. Also, with the intelligent on-board controller, the host system software will not require changing as new flash memory evolves. Thus, systems that support the Cactus Technologies® Commercial SSD products today will continue to work with future Cactus Technologies® Commercial SSDs built with new flash technology without having to update or change host software.

1.2.2. Defect and Error Management

Cactus Technologies® Commercial SSD contains a sophisticated defect and error management system similar to those found in magnetic disk drives. The defect management is completely transparent to the host and does not consume any user data space.

The soft error rate for Cactus Technologies® Commercial SSD is much lower than that of magnetic disk drives. In the extremely rare case where a read error does occur, the drive has sophisticated ECC to recover the data.

These defect and error management systems, coupled with the solid-state construction, give Cactus Technologies® Commercial SSDs unparalleled reliability.

1.2.3. Power Supply Requirements

Cactus Technologies® Commercial SSD operates at a voltage range of 5.0 volts ± 10%.

2.Product Specifications

For all the following specifications, values are defined at ambient temperature and nominal supply voltage unless otherwise stated.

2.1. System Environmental Specifications

Table 2-1. Environmental Specifications

		Cactus Technologies® Commercial SSD
Temperature	Operating:	0° C to +70° C (Standard), SATA III -40° C to +85° C (extended), SATA II
Humidity	Operating & Non-Operating:	8% to 95%, non-condensing
Vibration	Operating & Non-Operating:	20G, MIL-STD-883G Method 2005.2, Condition A
Shock	Operating & Non-Operating:	3,000 G, MIL-STD-883G Method 2002.4, Condition C
Altitude (relative to sea level)	Operating & Non-Operating:	100,000 feet maximum

Note: extended parts are temperature screened only; long term reliability could be compromised if the product is used at extended temperatures for long periods of time.

Standard temp. parts will operate at full SATA III mode, whereas Extended temp. parts will operate only in SATA II mode.

2.2. System Power Requirements

Table 2-2. Power Requirements

		Cactus Technologies® Commercial SSD	
DC Input Voltage (VCC) 100 mV max. ripple (p-p)		5.0V ±10%	
(Maximum Average Value) See Notes.		SATA II	SATA III
	Idle:	350 mA	280 mA
	Reading:	740 mA	510 mA
	Writing:	1050 mA	680 mA

NOTES: All values quoted are typical at ambient temperature and nominal supply voltage unless otherwise stated.

Sleep mode is specified under the condition that all drive inputs are static CMOS levels and in a “Not Busy“ operating state.

2.3. System Performance

All performance timings assume the drive controller is in the default (i.e., fastest) mode.

Table 2-3. Performance

Read Transfer Rate	Standard temp. SATA III Extended temp. SATA II	Up to 500 MBytes/sec Up to 245 MBytes/sec
Write Transfer Rate	Standard temp. SATA III Extended temp. SATA II	Up to 480 Mbytes/sec Up to 240 MBytes/sec

.

2.4. System Reliability

Table 2-4. Reliability

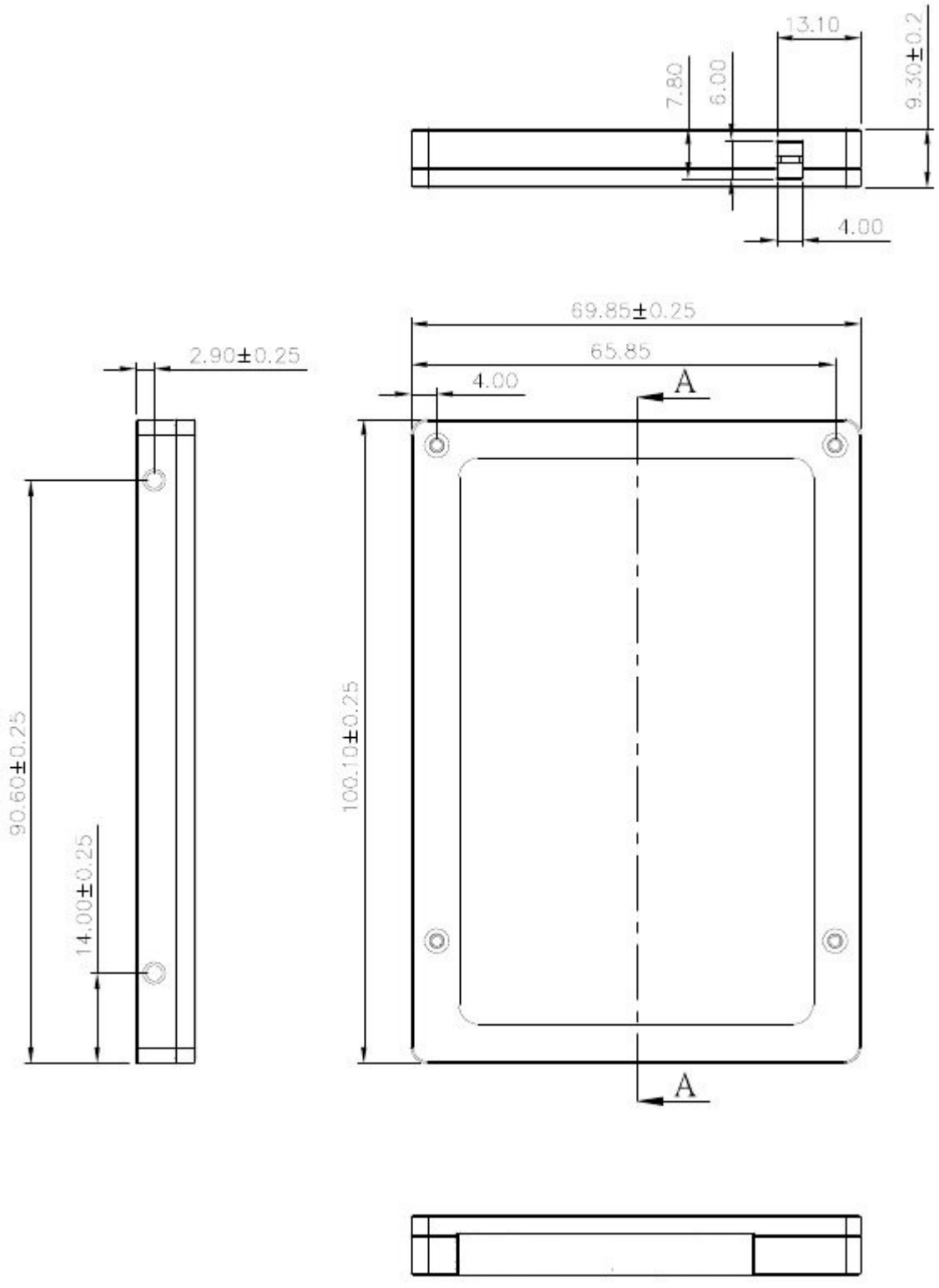
Data Reliability	< 1 non-recoverable error in 10^{14} bits READ
Endurance (estimated TBW): 512GB 1TB	 1536TB 3072TB

Note: estimated TBW assumes workload consisting of mostly large block writes; TBW will be significantly reduced for random, small block writes.

2.5. Physical Specifications

The following sections provide the physical specifications for Cactus Technologies® Commercial SSD products.

2.5.1. 2.5” SSD Physical Specifications


13.10
9.30±0.2
7.80
6.00
4.00
69.85±0.25
65.85
4.00
A
2.90±0.25
90.60±0.25
14.00±0.25
100.10±0.25
A

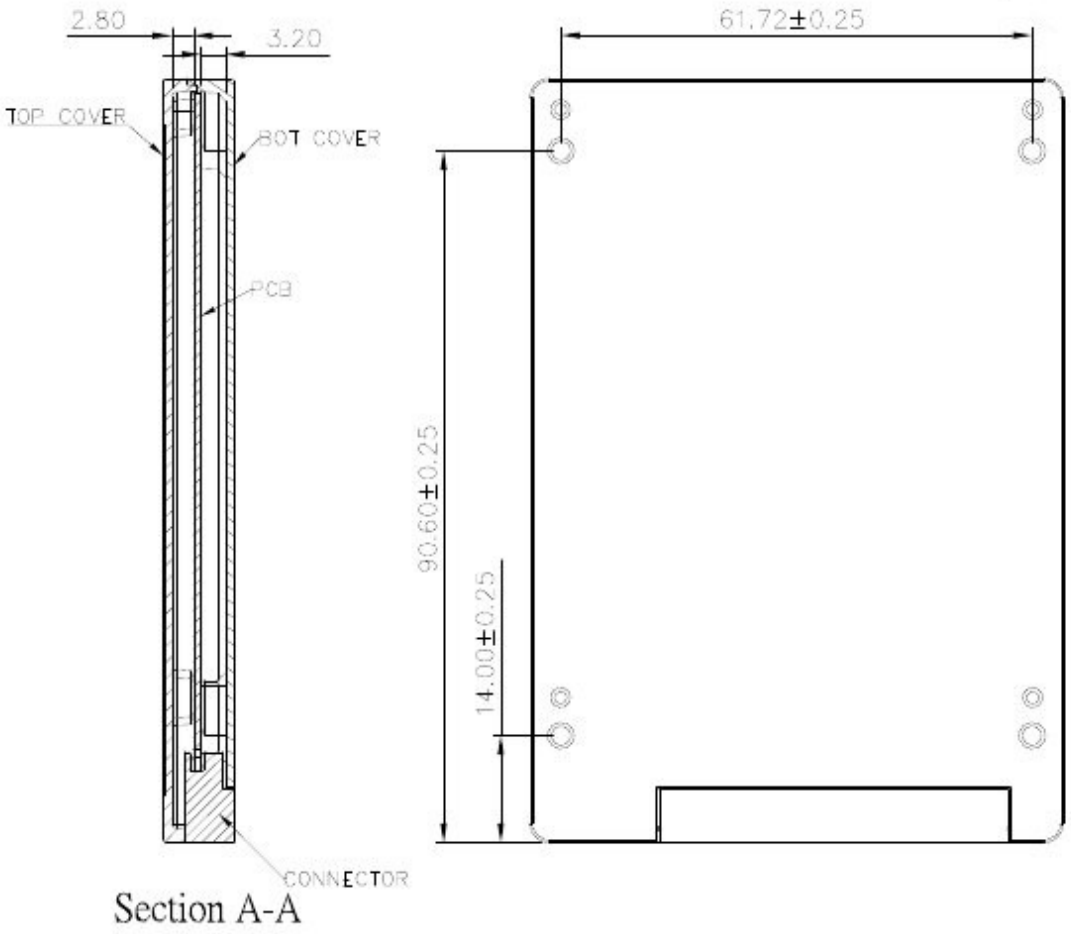


Figure 2-1. 2.5” SSD dimensions

Figure 2-2. SSD w/ Smiths Nebula series rugged connector

Figure 2-3. SSD with Amphenol R-SATA rugged connector

3.Interface Description

The following sections provide detailed information on the Cactus Technologies® Commercial SSD interface.

3.1. SSD Pin Assignments and Pin Type

Cactus Technologies® -240SE series SSD offers three connector options. The 1st one uses industry standard 7+12 SATA connector. The signal/pin assignments and descriptions are listed in Table 3-5.

Table 3-5. SSD Pin Assignments and Pin Type

Signal Segment Pin #	Signal Name	Pin Type
S1	GND	
S2	RXP	Analog In
S3	RXN	Analog In
S4	GND	
S5	TXN	Analog Out
S6	TXP	Analog Out
S7	GND	

Power Segment Pin #	Signal Name	Pin Type
P1	3.3V	
P2	3.3V	
P3	DEVSLP	DevSleep Control
P4	GND	
P5	GND	
P6	GND	
P7	5V	
P8	5V	
P9	5V	
P10	GND	
P11	Reserved	
P12	GND	
P13	12V	
P14	12V	
P15	12V	

The 2nd options uses a rugged SATA connector from Smiths Connectors Nebula® series. This connector offers enhanced shock & vibration resistance. Below are details about this connector:

Device connector part number: KSD22-SMT00H1TAH

Matching host socket part number (vertical): KSD22-VFD04H0TAH

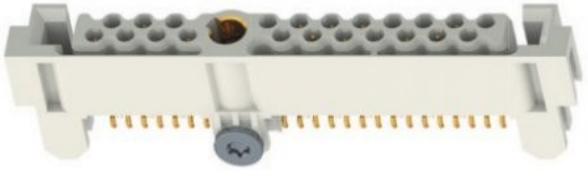
Matching host socket part number (horizontal): KSD22-RFD08H0TAH

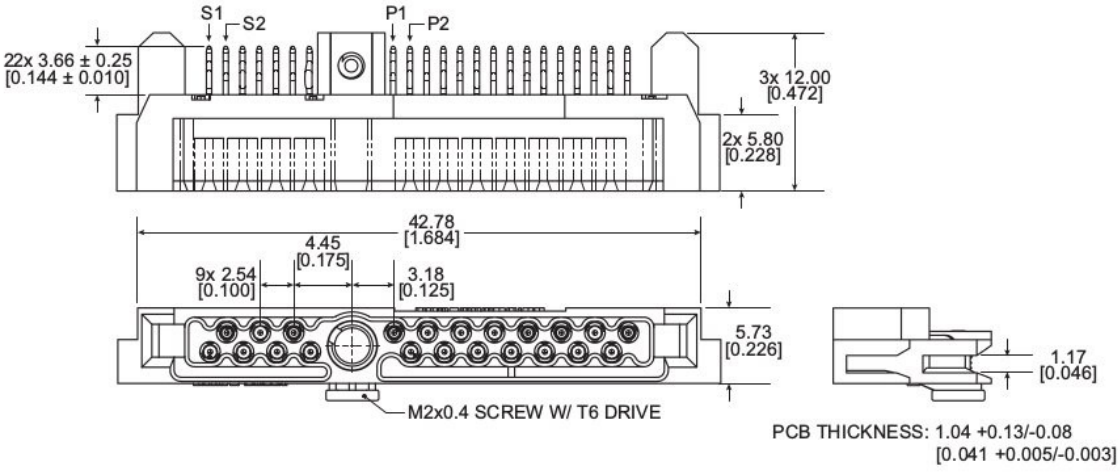
Connector max. insertion cycles: <5000

Connector shock specifications: 100 g, 11 ms, half sine, 6 shocks per axis

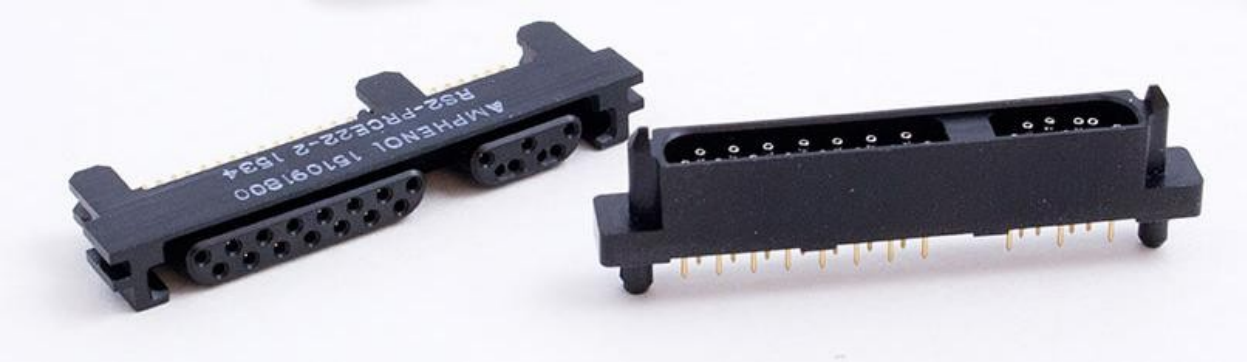
Connector vibration specifications: EIA 364-28, condition V test letter A, 30 g (3 axis, 5 hrs per axis)

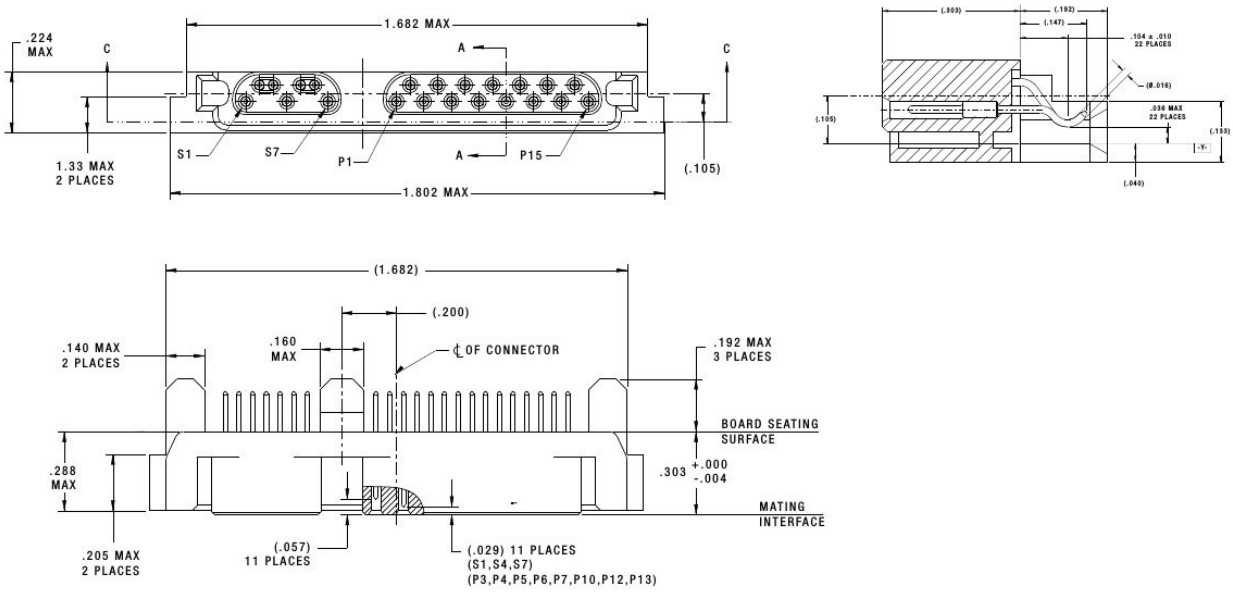
The following diagram shows the mechanical dimensions of the device connector:





The 3rd option uses Amphenol's R-SATA® series connector. This connector offers similar high resistance to shock & vibration as the Smiths connector. The following diagram shows the mechanical dimensions of the device connector:





Below are some details about this connector:
Device connector part number: RS2-PRCE22-X

Matching host socket part number (horizontal, surface mount): RS2-RRSM22-X

Connector max. insertion cycles: <20000

3.2. Electrical Specifications

The following table defines all D.C. Characteristics for the SSD products. Unless otherwise stated, conditions are:

Vcc = 5.0V ± 10%
Ta = 0°C to 70°C (Standard temp.); -40°C to 85°C (Extended temp.)

3.2.1. Absolute Maximum Ratings

Parameter	Symbol	MIN	MAX	Units
Storage Temperature	Ts	-55	+100	°C
Operating Temperature	T_A	-40	+85	°C
Vcc with respect to GND	Vcc	-0.3	5.5	V

3.2.2. DC Characteristics

Parameter	Symbol	MIN	MAX	Units
Input Voltage	Vin	-0.5	Vcc + 0.5	V
Output Voltage	Vout	-0.3	Vcc + 0.3	V
Input Leakage Current	I_{LI}	-10	10	uA
Output Leakage Current	I_{LO}	-10	10	uA
Input/Output Capacitance	C_I/C_o		10	pF
Operating Current Idle Active	I_{CC}		 SATA II SATA III 355 285 1100 685	mA

3.2.3. AC Characteristics

Cactus Technologies® SSD products conforms to all AC timing requirements as specified in the SATA-IO specifications. Please refer to that document for details of AC timing for all operation modes of the device.

4.ATA Drive Register Set Definition and Protocol

The communication to or from the SSD is done using FIS. Legacy ATA protocol is supported by using the legacy mode defined in the SATA specifications. In this mode, the FIS has defined fields which provide all the necessary ATA task file registers for control and status information. The Serial ATA interface does not support Primary/Secondary or Master/Slave configurations. Each SATA channel supports only one SATA device, with the register selection as defined by the ATA standard.

4.1. ATA Task File Definitions

The following sections describes the usage of the ATA task file registers. Note that the Alternate Status Register of legacy ATA is not defined for SATA drives.

4.1.1. Data Register

The Data Register is a 16-bit register, and it is used to transfer data blocks between the SSD data buffer and the Host.

4.1.2. Error Register

This register contains additional information about the source of an error when an error is indicated in bit 0 of the Status register. The bits are defined as follows:

D7	D6	D5	D4	D3	D2	D1	D0
BBK	UNC	0	IDNF	0	ABRT	0	AMNF

Bit 7 (BBK) This bit is set when a Bad Block is detected.
Bit 6 (UNC) This bit is set when an Uncorrectable Error is encountered.
Bit 5 This bit is 0.
Bit 4 (IDNF) The requested sector ID is in error or cannot be found.
Bit 3 This bit is 0.
Bit 2 (Abort) This bit is set if the command has been aborted because of a status condition: (Not Ready, Write Fault, etc.) or when an invalid command has been issued.
Bit 1 This bit is 0.
Bit 0 (AMNF) This bit is set in case of a general error.

4.1.3. Feature Register

This register provides information regarding features of the SSD that the host can utilize.

4.1.4. Sector Count Register

This register contains the number of sectors of data requested to be transferred on a read or write operation between the host and the SSD. If the value in this register is zero, a count of 256 sectors is specified. If the command was successful, this register is zero at command completion. If not successfully completed, the register contains the number of sectors that need to be transferred in order to complete the request.

4.1.5. Sector Number (LBA 7-0) Register

This register contains the starting sector number or bits 7-0 of the Logical Block Address (LBA) for any SSD data access for the subsequent command.

4.1.6. Cylinder Low (LBA 15-8) Register

This register contains the low order 8 bits of the starting cylinder address or bits 15-8 of the Logical Block Address.

4.1.7. Cylinder High (LBA 23-16) Register

This register contains the high order bits of the starting cylinder address or bits 23-16 of the Logical Block Address.

4.1.8. Drive/Head (LBA 27-24) Register

The Drive/Head register is used to select the drive and head. It is also used to select LBA addressing instead of cylinder/head/sector addressing. The bits are defined as follows:

D7	D6	D5	D4	D3	D2	D1	D0
1	LBA	1	DRV	HS3	HS2	HS1	HS0

Bit 7 This bit is set to 1.
Bit 6 LBA is a flag to select either Cylinder/Head/Sector (CHS) or Logical Block Address Mode (LBA). When LBA=0, Cylinder/Head/Sector mode is selected. When LBA=1, Logical Block Address is selected. In Logical Block Mode, the Logical Block Address is interpreted as follows:
LBA07-LBA00: Sector Number Register D7-D0.
LBA15-LBA08: Cylinder Low Register D7-D0.
LBA23-LBA16: Cylinder High Register D7-D0.
LBA27-LBA24: Drive/Head Register bits HS3-HS0.
Bit 5 This bit is set to 1.
Bit 4 (DRV) DRV is the drive number. This should always be set to 0.
Bit 3 (HS3) When operating in the Cylinder, Head, Sector mode, this is bit 3 of the head number. It is Bit 27 in the Logical Block Address mode.
Bit 2 (HS2) When operating in the Cylinder, Head, Sector mode, this is bit 2 of the head number. It is Bit 26 in the Logical Block Address mode.
Bit 1 (HS1) When operating in the Cylinder, Head, Sector mode, this is bit 1 of the head number. It is Bit 25 in the Logical Block Address mode.
Bit 0 (HS0) When operating in the Cylinder, Head, Sector mode, this is bit 0 of the head number. It is Bit 24 in the Logical Block Address mode.

4.1.9. Status Registers

These registers return the status when read by the host. Reading the Status register does clear a pending interrupt while reading the Auxiliary Status register does not. The meaning of the status bits are described as follows:

D7	D6	D5	D4	D3	D2	D1	D0
BUSY	RDY	DWF	DSC	DRQ	CORR	0	ERR

Bit 7 (BUSY) The busy bit is set when the device has access to the command buffer and registers and the host is locked out from accessing the command register and buffer. No other bits in this register are valid when this bit is set to a 1.

Bit 6 (RDY) RDY indicates whether the device is capable of performing operations requested by the host. This bit is cleared at power up and remains cleared until the device is ready to accept a command.

Bit 5 (DWF) This bit, if set, indicates a write fault has occurred.

Bit 4 (DSC) This bit is set when the device is ready.

Bit 3 (DRQ) The Data Request is set when the device requires that information be transferred either to or from the host through the Data register.

Bit 2 (CORR) This bit is set when a Correctable data error has been encountered and the data has been corrected. This condition does not terminate a multi-sector read operation.

Bit 1 (IDX) This bit is always set to 0.

Bit 0 (ERR) This bit is set when the previous command has ended in some type of error. The bits in the Error register contain additional information describing the error.

4.1.10. Device Control Register

This register is used to control the drive interrupt request and to issue an ATA soft reset to the drive. The bits are defined as follows:

D7	D6	D5	D4	D3	D2	D1	D0
HOB	X	X	X	1	SW Rst	-IEn	0

Bit 7 This bit is used in 48-bit addressing mode. When cleared, the host can read the most recently written values of the Sector Count,Drive/Head and LBA registers. When set, the host will read the previous written values of these registers. A write to any Command block register will clear this bit.

Bit 6 This bit is an X (Do not care).

Bit 5 This bit is an X (Do not care).

Bit 4 This bit is an X (Do not care).

Bit 3 This bit is ignored by the drive.

Bit 2 (SW Rst) This bit is set to 1 in order to force the drive to perform an AT Disk controller Soft Reset operation. The drive remains in Reset until this bit is reset to '0'.

Bit 1 (-IEn) The Interrupt Enable bit enables interrupts when the bit is 0. When the bit is 1, interrupts from the drive are disabled. This bit is set to 0 at power on and Reset.

Bit 0 This bit is ignored by the drive.

4.1.11. Drive Address Register

This register is provided for compatibility with the AT disk drive interface. It is recommended that this register not be mapped into the host's I/O space because of potential conflicts on Bit 7. The bits are defined as follows:

D7	D6	D5	D4	D3	D2	D1	D0
X	-WTG	-HS3	-HS2	-HS1	-HS0	-nDS1	-nDS0

Bit 7 This bit is unknown.
Implementation Note:
Conflicts may occur on the host data bus when this bit is provided by a Floppy Disk Controller operating at the same addresses as the SSD. Following are some possible solutions to this problem:

1. Locate the SSD at a non-conflicting address (i.e., Secondary address (377) when a Floppy Disk Controller is located at the Primary addresses).
2. Do not install a Floppy and a SSD in the system at the same time.
3. Implement a socket adapter that can be programmed to (conditionally) tri-state D7 of I/0 address 3F7/377 when a SSD product is installed and conversely to tri-state D6-D0 of I/O address 3F7/377 when a floppy controller is installed.
4. Do not use the SSD's Drive Address register. This may be accomplished by either a) If possible, program the host adapter to enable only I/O addresses 1F0-1F7, 3F6 (or 170-177, 176) to the SSD or b) if provided use an additional Primary/Secondary configuration in the SSD that does not respond to accesses to I/O locations 3F7 and 377. With either of these implementations, the host software must not attempt to use information in the Drive Address Register.

Bit 6 (-WTG) This bit is 0 when a write operation is in progress, otherwise, it is 1.
Bit 5 (-HS3) This bit is the negation of bit 3 in the Drive/Head register.
Bit 4 (-HS2) This bit is the negation of bit 2 in the Drive/Head register.
Bit 3 (-HS1) This bit is the negation of bit 1 in the Drive/Head register.
Bit 2 (-HS0) This bit is the negation of bit 0 in the Drive/Head register.
Bit 1 (-nDS1) This bit is 0 when drive 1 is active and selected.
Bit 0 (-nDS0) This bit is 0 when the drive 0 is active and selected.

5.ATA Command Description

This section defines the ATA command set supported by Cactus Technologies® Commercial SSDs.

5.1. ATA Command Set

Table 5-6 summarizes the supported ATA command set .

Table 5-6. ATA Command Set

COMMAND	Code
Check Power Mode	E5h, 98h
Data Set Management	06h
Execute Drive Diagnostic	90h
Flush Cache	E7h
Flush Cache Ext	EAh
Identify Drive	ECh
Idle	E3h, 97h
Idle Immediate	E1h, 95h
Initialize Drive Parameters	91h
NOP	00h
Read Buffer	E4h
Read DMA	C8h
Read DMA Ext	25h
Read FPDMA Queued	60h
Read Multiple	C4h
Read Multiple Ext	29h
Read Native Max Address	F8h
Read Native Max Address Ext	27h
Read Sector(s)	20h, 21h
Read Sector(s) Ext	24h
Read Verify Sector(s)	40h, 41h
Read Verify Sector(s) Ext	42h

COMMAND	Code
Security Disable Password	F6h
Security Erase Prepare	F3h
Security Erase Unit	F4h
Security Freeze Lock	F5h
Security Set Password	F1h
Security Unlock	F2h
Seek	70h
Set Features	EFh
Set Max Address	F9h
Set Max Address Ext	37h
Set Max Set Password	F9h
Set Max Lock	F9h
Set Max Freeze Lock	F9h
Set Max Unlock	F9h
Set Multiple Mode	C6h
Set Sleep Mode	E6h, 99h
SMART	B0h
Stand By	E2h, 96h
Stand By Immediate	E0h, 94h
Write Buffer	E8h
Write DMA	CAh
Write DMA Ext	35h
Write FPDMA Queued	61h
Write Multiple	C5h
Write Multiple Ext	39h
Write Sector(s)	30h
Write Sector(s) Ext	34h

6. S.M.A.R.T. Feature Set

Cactus Technologies® -240SE Series SSDs supports S.M.A.R.T. attribute reporting. This following subcommands are supported when programmed into the Feature Register:

Value	Command	Value	Command
D0h	Read Data	D5h	Reserved
D1h	Read Attribute Threshold	D6h	Reserved
D2h	Enable/Disable Autosave	D8h	Enable SMART operationes
D3h	Save Attribute Values	D9h	Disable SMART operations
D4h	Execute OFF-LINE Immediate	DAh	Return Status

6.1. S.M.A.R.T Data Structure

The Read Data commands returns 512 bytes of data in the following structure:

Byte	Description
0-1	Revision code
2-361	Vendor specific
362	Off-line data collection status
363	Self-test execution status byte
364-365	Total time in seconds to complete off-line data collection activitiies
366	Vendor specific
367	Off-line data collection capabilities
368-369	SMART capabilities
370	Error logging capabilities: bit[7:1] – reserved: bit[0]: 1=device error logging supported
371	Vendor specific
372	Short self-test routine recommended polling time (in minutes)
373	Extended self-test routine recommended polling time (in minutes)
374	Convevance self-test routine recommended polling time (in minutes)
375-385	Reserved
386-395	Firmware Version/Date Code
396-397	Reserved
398-399	Reserved
400-405	'SM2246'
406-510	Vendor specific
511	Data structure checksum

6.2. S.M.A.R.T Attributes

The following table lists the attributes returned in bytes 2-361 of the 512-byte SMART data. Each attribute occupies 12 byte of data. Byte 0 is Attribute ID, bytes 1-2 are status flags, bytes 3-4 are reserved bytes; the table below shows the definitions of bytes 5-11:

Attribute ID	Attribute values							Attribute Name
01h	MSB	00	00	00	00	00	00	Read error rate
05h	LSB	MSB	00	00	00	00	00	Reallocated sectors count
09h	LSB			MSB	00	00	00	Power on hours
0Ch	LSB			MSB	00	00	00	Power cycle count
A0h	LSB			MSB	00	00	00	Uncorrectable sector count when read/write
A1h	LSB	MSB	00	00	00	00	00	Number of valid spare block

Attribute ID	Attribute values							Attribute Name
A3h	LSB	MSB	00	00	00	00	00	Number of initial invalid block
A4h	LSB			MSB	00	00	00	Total erase count
A5h	LSB			MSB	00	00	00	Max. Erase count
A6h	LSB			MSB	00	00	00	Min. Erase count
A7h	LSB			MSB	00	00	00	Average erase count
A8h	LSB			MSB	00	00	00	Max. erase count spec.
A9h	LSB			MSB	00	00	00	Percent remaining life
AFh	LSB			MSB	00	00	00	Program fail count in worst die
B0h	LSB	MSB	00	00	00	00	00	Erase fail count in worst die
B1h	LSB			MSB	00	00	00	Total wear level count
B2h	LSB	MSB	00	00	00	00	00	Runtime invalid block count
B5h	LSB			MSB	00	00	00	Total program fail count
B6h	LSB	MSB	00	00	00	00	00	Total erase fail count
BBh	LSB			MSB	00	00	00	Uncorrectable error count
C0h	LSB	MSB	00	00	00	00	00	Power-off retract count
C2h	MSB	00	00	00	00	00	00	Controlled temperature (fixed at 27C)
C3h	LSB			MSB	00	00	00	Hardware ECC recovered
C4h	LSB			MSB	00	00	00	Reallocation event count
C6h	LSB			MSB	00	00	00	Uncorrectable error count offline
C7h	LSB	MSB	00	00	00	00	00	UltraDMA CRC error count
E1h	LSB						MSB	Total LBAs written (in units of 32MB)
E8h	LSB	MSB	00	00	00	00	00	Available reserved space
F1h	LSB						MSB	Total LBAs written (in units of 32MB)
F2h	LSB						MSB	Total LBAs read (in units of 32MB)

7.Encryption Key Management

Cactus Technologies® -240SE Series SSDs offer two methods for handling encryption key exchange – a simple VS command to send the DEK from host to device or a more complex and secure method of using HMAC DRNG handshake. The following sections discuss these two methods.

7.1. Method 1: simple VS command for host DEK to device

In this method, host sends the DEK to the device via the following VS command:

Register	Value
Feature	0xA5
Count	0
LBA Low	0
LBA Mid	0
LBA High	0
Device	0
Command	0xFE

One sector of data is then transferred over in the following format:

Bytes	Content
0-31	Encryption Media Key
32-63	Encryption IV Scramble Key
64-95	Decryption Media Key
96-127	Decryption IV Scramble Key
128-511	Don't care

Note that the Scramble key is required for AES XTS mode and is optional for other modes. The encryption and decryption keys are the same value.

Upon successful completion of this command, the STATUS Register will return 0x50 value.

This method of key change is simple to implement; however, the DEK is sent over in plain text and can be captured. For a more secure method of handling the DEK, we offer the 2nd method described below.

7.2. Method 2: Secure HMAC Encrypted DEK Protocol

HMAC stands for Key-Hashed Message Authentication Code, a well-known and frequently used secure authentication protocol approved by US Government. An encrypted tunnel on the hardware interface is built during authentication. If the HMAC key was lost or stolen, the content remains safe and secure.

In this key exchange method, host system will first initialize the drive with shared secrets. Cactus Technologies® will provide the host software needed to the customer to perform this initialization. Once the drive has been properly initialized, the process of key exchange involves a challenge/response handshake between the host and the drive. Once the proper challenge response is received from the drive, a KEK (Key Encryption Key) known to both host and drive will be generated. This KEK is used to encrypt the DEK (Data Encryption Key), which the host will then send over an to the drive via a VS command. The drive will use its internally generated KEK to decrypt the encrypted DEK, which in turn is used to decrypt drive data.

Note that the KEK is random and different on every use, thus defeating any attempts to snoop the SATA bus to obtain the DEK.

For further information about the details of the command protocols involved in this method, an NDA is required; please contact Cactus Technologies® for details.

7.3. Host Utilities for Key Exchange

Cactus Technologies® will provide Windows OS host software needed to perform key exchange for both SetDEK and HMAC options. For SetDEK option, since it is a simple ATA VS command, Linux or other OS support should be fairly straightforward and can be done by the user.

For HMAC option, support in Linux is possible but will depend on the particular Linux distro and kernel version. Cactus Technologies® will work with customer on a case by case basis if Linux support is required.

7.4. Volatile Key Storage

Cactus Technologies® -240SE CrytoSSD products do not store the DEK in non-volatile memory. The DEK is only stored in internal SRAM in the security chip. This SRAM is write only and contents cannot be read out. Furthermore, once power is removed, the contents of the SRAM is gone, thus the DEK must be resend upon every power up.

Due to the volatile storage of the DEK, it is a simple matter to do a 'crypto erase' by simply cutting power to the drive. As an additional option, in HMAC mode, user can also short the jumper on the back of the drive for at least 3secs to trigger a DEK erase. This is not strictly necessary but is provided in case the user does not have an option to cut power to the drive.

Appendix A. Ordering Information

Model KDXFI-240SEY-Z-09

Where: X is drive capacities:
512G ---------- 512GB
1T ---------- 1TB

Where: I is temperature grade
blank ---------- standard; SATA III
I ---------- extended (contact factory for lead time); SATA II
(Extended temp. parts are available only in SATA II mode)

Where: Y is connector option
blank ---------- standard SATA connector
R1 ---------- rugged Smiths Nebula connector
R2 ---------- rugged Amphenol R-SATA connector

Where: Z is key exchange option
D ---------- SetDEK option
H ---------- HMAC option

Where: 09 is for Extended temp. parts only

Example:

(1) 512GB 2.5” SSD w/ SetDEK option ---------- KD512GF-240SE-D
(2) 51GB 2.5” SSD w/ SetDEK option, extended temp. ---------- KD512GFI-240SE-D-09
(3) 1TB 2.5” SSD w/ SetDEK option, Smiths connector ---------- KD1TF-240SER1-D
(4) 1TB 2.5” SSD w/ SetDEK option, Amphenol connector-------- KD1TF-240SER2-D
(5) 1TB 2.5” SSD w/ HMAC option ---------- KD1TF-240SE-H

Appendix B.Technical Support Services

B.1.Direct Cactus Technologies® Technical Support

Email: tech@cactus-tech.com

Appendix C.Cactus Technologies® Worldwide Sales Offices

Email: sales@cactus-tech.com

Email: americas@cactus-tech.com

Appendix D.Limited Warranty

I. WARRANTY STATEMENT

Cactus Technologies® warrants its Commercial Grade products only to be free of any defects in materials or workmanship that would prevent them from functioning properly for two years from the date of purchase or when rated TBW is exceeded, whichever occurs first. This express warranty is extended by Cactus Technologies® Limited to customers of our products.

II. GENERAL PROVISIONS

This warranty sets forth the full extent of Cactus Technologies® responsibilities regarding the Cactus Technologies® Commercial Grade Flash Storage Products. Cactus Technologies®, at its sole option, will repair, replace or refund the purchase price of the defective product. Cactus Technologies® guarantees our products meet all specifications detailed in our product manuals. Although Cactus Technologies® products are designed to withstand harsh environments and have the highest specifications in the industry, they are not warranted to never have failure and Cactus Technologies® does not warranty against incidental or consequential damages. Accordingly, in any use of products in life support systems or other applications where failure could cause injury or loss of life, the products should only be incorporated in systems designed with appropriate redundancy, fault tolerant or backup features.

III. WHAT THIS WARRANTY COVERS

For products found to be defective, Cactus Technologies® will have the option of repairing, replacing or refunding the purchase price the defective product, if the following conditions are met:

A. The defective product is returned to Cactus Technologies® for failure analysis as soon as possible after the failure occurs.

B. An incident card filled out by the user, explaining the conditions of usage and the nature of the failure, accompanies each returned defective product.

C. No evidence is found of abuse or operation of products not in accordance with the published specifications, or of exceeding maximum ratings or operating conditions.

All failing products returned to Cactus Technologies® under the provisions of this limited warranty shall be tested to the product’s functional and performance specifications. Upon confirmation of failure, each product will be analyzed, by whatever means necessary, to determine the root cause of failure. If the root cause of failure is found to be not covered by the above provisions, then the product will be returned to the customer with a report indicating why the failure was not covered under the warranty.

This warranty does not cover defects, malfunctions, performance failures or damages to the unit resulting from use in other than its normal and customary manner, misuse, accident or neglect; or improper alterations or repairs. Cactus Technologies® Limited may repair or replace, at its discretion, any product returned by its customers, even if such product is not covered under warranty, but is under no obligation to do so.

IV. RECEIVING WARRANTY SERVICE

According to Cactus Technologies® warranty procedure, defective product should be returned only with prior authorization from Cactus Technologies® Limited. Please contact Cactus Technologies® Customer Service department (tech@cactus-tech.com) with the following information: product model number and description, nature of defect, conditions of use, proof of purchase and purchase date. If approved, Cactus Technologies® will issue a Return Material Authorization or Product Repair Authorization number with shipping instructions.