Microsemi Corporation

MSM048 and MSM096

MSD048 and MSD096

(Shortened data sheet version)

Secure SLC NAND SATA BGA

with Hardware Authentication, Self-Destruct and AT Integrity

NOTE: Microsemi does not publish the full data sheet for this product on the web. Contact your Microsemi sales representative to receive the full data sheet.

Secure SLC NAND Flash SATA BGA

General Description

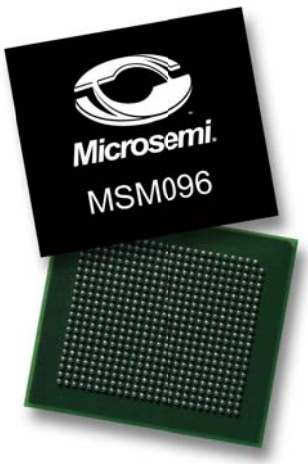
The Microsemi MSM048/MSM096 is a complete SATA storage system packaged as a single 32 mm x 28 mm, 524 pin PBGA. Perfect for single board computer boot devices and embedded defense applications where a full sized 2.5" SSD is too large, the Microsemi SATA BGA combines a SATA flash controller with the latest in small geometry SLC NAND flash, multiple power supplies, and security features including encryption, authentication, RNG, anti-tamper (AT), as well as self-destruct features into a single device. The MSM048/MSM096 SATA BGA is available with host accessible densities of 37.5 GB and 75 GB[2], is compliant to SATA revision 2.6, and supports interface transfer speeds of 1.5 Gb/s and 3.0 Gb/s.

Standard Features

- Host accessible capacity: 37.5 GB MSM048, 75GB MSM096[1]
- Integrated switching power supplies.
- 48 GB and 96 GB devices have same form-factor/pin-out.[1]
- Single supply operation: 3.3 to 5.0 V.
- Minimal external components.
- Zero power standby mode (ZPM).
- 256-bit RNG (Random number generator).
- Hardware **AES-128** encryption running CTR mode.
- Additional features of the DX model
  - Hardware authentication.
  - AT Integrity physical tamper protection.
  - Temperature rate of change, Hi/Low AT mitigation.
  - Self-destruct capability.
  - Multiple automatic destruct options
- **SHA-256** pass-phrase feature.
- AES key purge feature eliminates encryption key.
- Whole device erase with "push-button" trigger option.
- Support for Crypto Erase and Flash Erase.
- 1-bit, Single Level Cell (SLC) NAND flash.
- 16, 9-bit symbol ECC correction capability.
- Uncorrectable bit error rate (UBER): 10^{-17}
- Sequential R/W 128 KiB performance MSM048: 156/44 MB/s.
- Sequential R/W 128 KiB performance MSM096: 179/83 MB/s.
- Sequential R/W IOPS MSM048: 8693/10421(4K).
- Sequential R/W IOPS MSM096: 10231/18230(4K).
- Random R/W IOPS MSM048: 5028/2432(4K).
- Random R/W IOPS MSM096: 5884/4084(4K).
- "Silent error" protection with 32-bit per sector CRC.
- 2.25 PB write endurance (MSM096).
- Over and under voltage detection and protection.
- Field upgradable firmware using SATA interface.
- 100% dynamic burn-in.
- Write protect option for read-only applications.
- Includes high quality DC blocking capacitors on the SATA signals.
- Operational temperature range of -40 ºC to +85 ºC.
- Storage Temperature: -55 ºC to +125 ºC.
- Also available in 2.5" form-factor (MSD model, see Figure 4b)
- Evaluation board is available for bench testing.

Applications

Single Board Computer Boot device
Ruggedized mobile defense systems
Battlefield robotics
Data recorders and digital maps
Industrial automation
Transportation systems
Mobile secure medical products



Product image is approximately life size

Note 1: One Gigabyte (GB) = 1,000,000,000 bytes.

Figure 1 shows the connections necessary to use the MSM048/MSM096 in a typical application. External components are minimal with only a few capacitors needed to supply energy for an orderly shutdown during unexpected power disturbance events. If an external backup 5.0 V supply, separate from Vdd, is available, the backup supply capacitor array can be omitted.

If the application requires an external trigger for Flash Erase, Crypto Erase, or self-destruct operations, connect a switch or logic gate to the Erase_Trigger and/or Self-Destruct inputs as shown. The inputs have internal de-bounce circuitry so there is no need to debounce switch signals externally. For read-only applications or applications that intermittently operate in a read-only mode, drive or tie the Write_Protect_N pin low when write protection is needed. Note that the write protect input is sampled once at power-on time. An optional RS-232 port allows a host controller to monitor the status of the device and enable or disable various operating modes. A feature called AT Integrity supports a multitude of possible Anti-Tamper features.

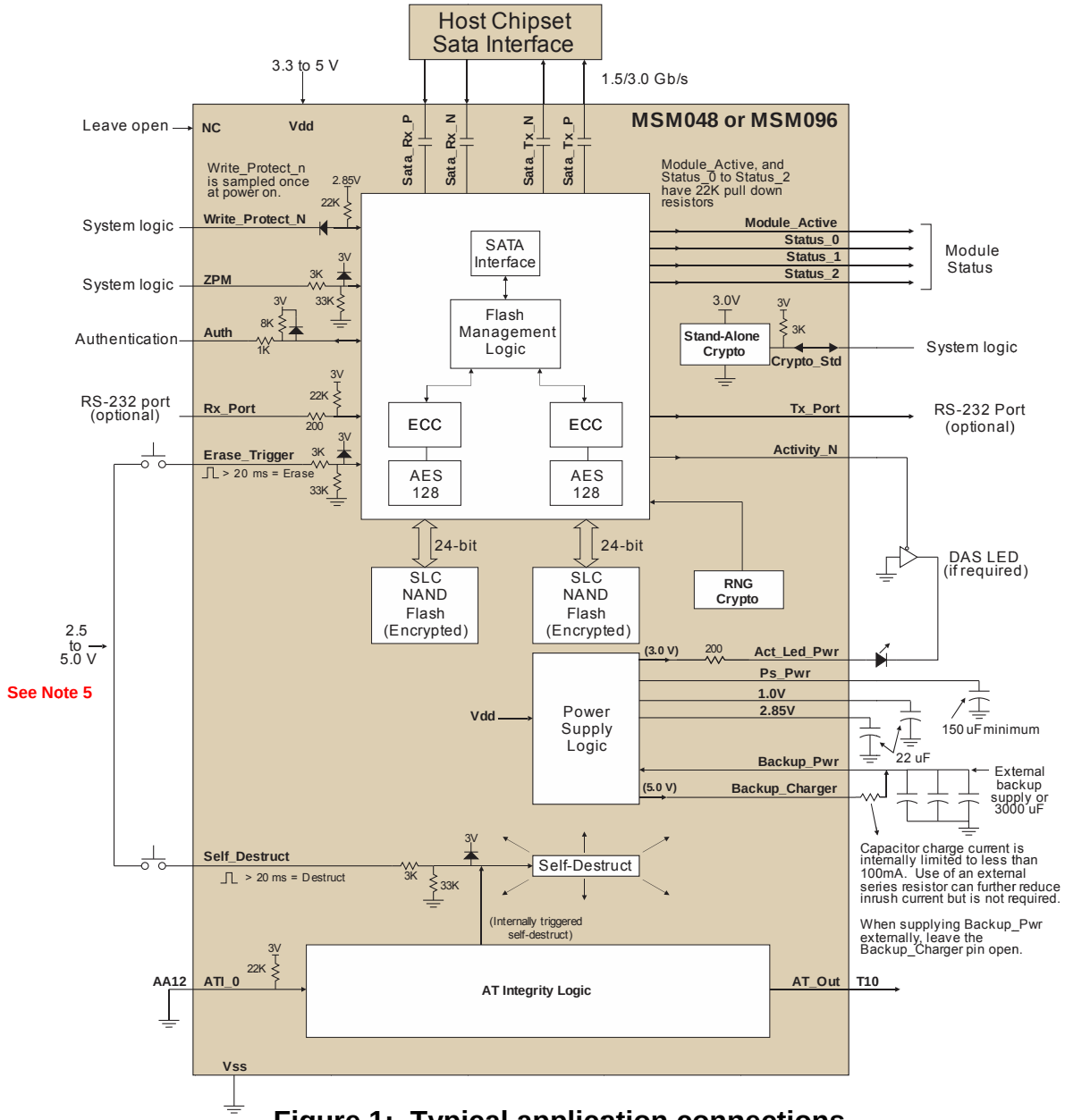


Figure 1: Typical application connections

Notes:
1. MSM048/MSM096 devices include internal high quality DC blocking capacitors on the SATA lines.
2. Self_Destruct and Erase_Trigger functions are combined into one pin on MSD model.
3. External pull-down resistors on ZPM, Erase Trigger and Self-Destruct pins may be beneficial in some applications.
4. To avoid excessive leakage on Auth, Crypto_Std, and Rx-Port pins, do not exceed maximum input voltage, refer to Table 1 and 2.
5. **WARNING: Microsemi recommends caution when considering drive voltage levels for the Erase_Trigger and Destruct inputs. It is critical to adhere to published V_{IL} levels to prevent accidental erase or destruct operations.**

Electrical Characteristics

Table 1: Absolute Maximum Ratings

Parameter and Condition	Min	Max	Unit
Vdd supply voltage	-0.3	5.75	V
Voltage with respect to Vss: Write_Protect_N, ZPM, Erase_Trigger, Self_Destruct	-0.3	Vdd + 0.3	V
Backup_Pwr and Backup_Charger pin Voltage with respect to Vss	-0.3	5.75	V
Voltage with respect to Vss: Auth, Crypto_Std, and Rx_Port	-0.3	3.5	V
Voltage on ATI_[0..N] pins. The ATI chain has a single 22K internal pull-up resistor to 3.0 V. Refer to Figure 6 for connection details. Typically this pin is connected to ground or driven low with an open drain driver.	-0.3	3.3	V
Maximum input/output current: Write_Protect, ZPM, Rx_Port, Erase_Trigger, Self_Destruct, Tx_Port, Status_0, Status_1, Status_2, Module_Active Auth, Crypto_Std, ATI_[0..N], ATO_[0..N], and AT_Out		±2	mA
Maximum source/sink current: Act_Led_Pwr		Source 15 Sink 0	mA
Maximum source/sink current: Activity_N		Source 2 Sink 5	mA
Maximum source current: Backup_Charger (Internally limited)		70	mA
Operating temperature	-40	+85	°C
Operating temperature rate of change Warning: If the temperature-rate-of-change feature is enabled, exceeding the programmed temperature-rate-of-change limit may initiate an automatic self-destruct operation.		10	°C/minute
Thermal shutdown protection operating range	-55	+100	°C
Storage temperature	-55	+125	°C

Stresses greater than those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions greater than those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect reliability of the product.

Table 2: Recommended and Typical DC Operational Characteristics

Parameter	Min[1]	Typ[1]	Max[1]	Unit
Vdd supply voltage (see part numbering guide for supply options)	3.14	3.3	5.5	V
Backup_Pwr voltage (if not connected to Backup_Charger)	4.95	5.0	5.5	V
V_{IL} (Input low voltage)[2] Write_Protect_N, ZPM, Rx_Port, Erase_Trigger, Self_Destruct, ATI_[0..N] , and Auth	0.0		0.3	V
V_{IH} (Input high voltage)[2] Write_Protect_N, ZPM, Erase_Trigger, Self_Destruct	2.4		Vdd	V
V_{IH} (Input high voltage) Rx_Port, Auth, ATI_[0..N] pins	2.4		3.3	V
V_{OH} (Output high voltage, 1.5 mA load) Module_Active, Status_0, Status_1, Status_2, Tx_Port, AT_Out	2.5	2.75	3.1	V
V_{OH} (Output high voltage, 10 uA load) Activity_N	2.80	2.85	2.95	V
V_{OH} (Output high voltage, no load) Act_Led_Pwr	2.9	3.0	3.1	V
I_{OUT} Act_Led_Pwr current (with 1.5v LED drop)	4	7	8	mA
V_{OH} Backup_Charger voltage (no load)	4.7	5.0	5.2	V

Note 1: Unless otherwise stated, all values were measured at 25 °C
Note 2: **WARNING. Microsemi recommends caution when considering drive voltage levels for the Erase_Trigger and Destruct inputs. It is critical to adhere to published V_{IL} levels to prevent accidental erase or destruct operations.**

Table 2: Recommended and Typical DC Operating Characteristics (Continued)

Parameter	Min[1]	Typ[1]	Max[1]	Unit
I_{out} Backup_Charger (Internally limited)		65		mA
V_{OH} and V_{OL} of ATO_[0..N]	Typically ATI_0 level ± 0.1 V			
V_{OL} (Output low voltage with load of 1.5 mA) Module_Active, Status_0, Status_1, Status_2, Tx_Port, Activity_N, AT_Out	0.0	.25	0.3	V
I_{IH} (Input High Current. Inputs tied to 3.3 V) Write_Protect_N, ZPM, Erase_Trigger, Self_Destruct, ATI_[0..N]			300	uA
I_{IH} (Input High Current. Inputs tied to 3.5 V) Crypto_Std, Auth and Rx_Port			200	uA
I_{IH} (Input High Current. Inputs tied to Vdd = 5.5 V) Write_Protect_N, ZPM, Erase_Trigger, Self_Destruct, ATI_[0..N]			850	uA
I_{IL} (Input low Current. Inputs tied 0.0 V) Write_Protect_N, ZPM, Rx_Port, Erase_Trigger, Self-Destruct, Auth, Crypto_Std, ATI_0			200	uA
Idd. Inactive with no SATA commands, (Vdd = 3.3 V) MSM048 MSM096		 0.175 0.190	 0.203 0.218	A
Idd. 100 % Writes (128 KiB Seq. block), (Vdd = 3.3 V) MSM048 MSM096		 0.250 0.275	 0.283 0.313	A
Idd. 100 % Reads (128 KiB Seq. block), (Vdd = 3.3 V) MSM048 MSM096		 0.210 0.235	 0.243 0.268	A
Idd. Inactive with no SATA commands, (Vdd = 5.0 V) MSM048 MSM096		 0.135 0.145	 0.155 0.165	A
Idd. 100 % Writes (128 KiB Seq. block), (Vdd = 5.0 V) MSM048 MSM096		 0.185 0.200	 0.205 0.235	A
Idd. 100 % Reads (128 KiB Seq. block), (Vdd = 5.0 V) MSM048 MSM096		 0.150 0.165	 0.170 0.190	A
Idd during standby and sleep (MSM048 and MSM096, 3.3/5.0 V)		120/95		mA
Idd. Destruct operation (20 mS) Vdd = 3.3 V or 5.0 V (from inactive)		0.250		A
Idd. ZPM, deep slumber mode (ZPM = Vdd = 3.3 V) Other inputs at 0V		5	10	mA
Required external backup power capacitance.	3000			uF
Minimum required external capacitor on PS_PWR PS_PWR = Vdd - .025v.	150			uF
Required external ceramic capacitor for 1.0 V internal supply.	22			uF
Required external ceramic capacitor for 2.85 V internal supply.	22			uF
Suggested series charging resistance for BACKUP_CHARGER supply (No resistor required) ----------		0		Ohms

Note 1: Unless otherwise stated, all values were measured at 25 °C.

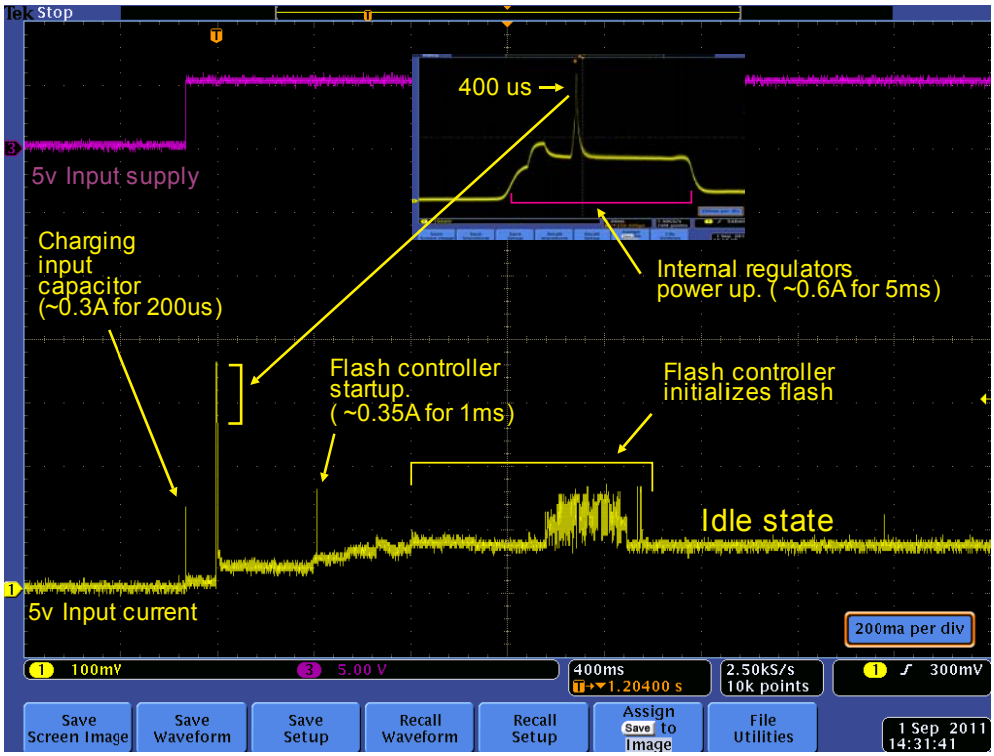


Figure 2: Power-On Inrush Current Plot

Thermal Performance

The MSM048/MSM096 incorporates features to transfer heat into the attached host PCB using multiple thermal vias positioned around heat generating devices. Microsemi conducts a thermal and power assessment of each new version of the MSM048/MSM096. The thermal image in Figure 3 show the temperature profiles of the MSM048/MSM096 on the customer evaluation PCB at room temperature.

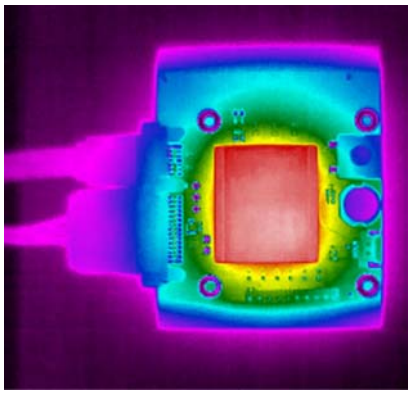


Figure 3a

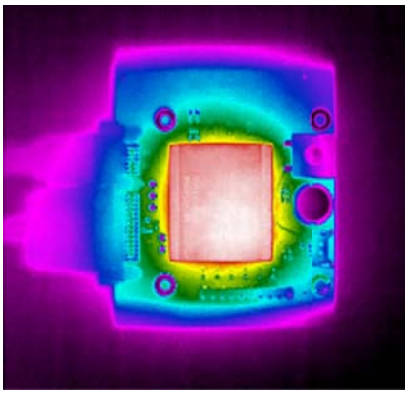


Figure 3b

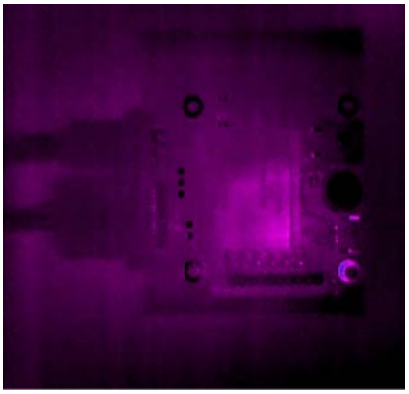


Figure 3c

Figure 3a: Idle. Room temperature 26 °C, Highest module temperature is 36 °C.
Figure 3b: Write. Room temperature 26 °C, Highest module temperature is 39 °C.
Figure 3b: Zero power mode. Module runs in ZPM near Room temperature 26 °C.

(MSM048 is installed on a MSM048BM2L-M00IEV evaluation board)

Table 3: Module Pin list (same pin-out for 48 GB and 96 GB units)

Pin	Pin name	Type	Description
G19, G20, G21, G22, G23, H19, H20, H22, H23, J19, J20, J21, J22, J23	Vdd	Power	Supply voltage pins.
A2, A23, A24, A25, A3, AA1, AA2, AA23, AA24, AA25, AA3, B1, B2, B24, B25, C1, C10, C13, C16, C18, C25, C8, D10, D11, D12, D13, D14, D15, D16, D18, D22, D4, D8, E18, E22, E4, E8, F18, F19, F20, F21, F22, F23, F3, F4, F5, F6, F7, F8, G10, G11, G12, G13, G14, G15, G16, G17, G18, G8, G9, H10, H11, H12, H13, H14, H15, H16, H17, H18, H21, H5, H8, H9, J10, J11, J12, J13, J14, J15, J16, J17, J18, J8, J9, K10, K11, K12, K13, K14, K15, K16, K17, K18, K19, K20, K21, K22, K23, K3, K4, K5, K6, K7, K8, K9, L10, L11, L12, L13, L14, L15, L16, L17, L18, L8, L9, M10, M11, M12, M13, M14, M15, M16, M17, M18, M19, M20, M21, M22, M23, M3, M4, M5, M6, M7, M8, M9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N8, N9, P10, P11,	Vss	Power	Ground pins.

P12, P13, P14, P15, P16, P17, P18, P21, P5, P8, P9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R8, R9, T13, T18, T19, T20, T21, T22, T23, T3, T4, T5, T6, T7, T8, U11, U15, U18, U22, U4, U8, V11, V15, V18, V22, V4, V8, W1, W11, W15, W18, W25, W8, Y1, Y13, Y2, Y24, Y25	Vss	Power	Ground pins.
C15	Sata_Rx_P	In	SATA Rx+ 1.5/3.0 Gb/s differential AC coupled
C14	Sata_Rx_N	In	SATA Rx- 1.5/3.0 Gb/s differential AC coupled
C11	Sata_Tx_P	Out	SATA Tx+ 1.5/3.0 Gb/s differential AC coupled
C12	Sata_Tx_N	Out	SATA Tx- 1.5/3.0 Gb/s differential AC coupled
W10	Write_Protect_N	In	Places the module into a read-only mode of operation. 0 = Write protected, 1 = Normal operation. Note: This input is sampled once at power on time. Changes to the state of this pin when power is applied are ignored until the next power cycle.
U17	ZPM	In	ZPM (Zero Power Mode) enables a low power standby mode. Driving the ZPM pin to a high level causes the MSM048/MSM096 to enter an ultra-low power deep slumber mode. Lowest power operation is obtained with Vdd at 3.3 V. **During normal operation, this pin must be held at a low level.**
E17	Auth	In/out	Hardware authentication.
V17	Rx_Port	In	Optional 19200 baud RS-232 port. Port receive input.

D17	Erase_Trigger	In	Crypto/Flash Erase trigger pin. (Active during ZPM) 0 = Normal operation. 1 = Trigger a crypto or flash erase after a 20 ms debounce. The Erase_Trigger must be enabled using the HWET RS-232 command. Driving this pin high for 20 ms or longer causes the MSM048/MSM096 to begin a Crypto or Flash Erase operation. To trigger a Crypto or Flash Erase operation immediately after power on, drive the pin low for longer than 20 ms, and then drive it high for 20 ms or longer. This pin has an internal pull-down. No external pull down resistor is necessary. Note: This pin has an enable to prevent an accidental erase operation. The host can use the HWET RS-232 command to enable or disable this pin. Refer to the part number guide to determine the default state of the enable. **Warning:** Microsemi recommends caution when considering drive voltage levels for the Erase_Trigger input. Adhere to published V_{IL} levels to prevent accidental secure erase operations.
U10	Self_Destruct	In	Module self-destruct. (Active during ZPM mode) 0 = Normal operation. 1 = Trigger a self-destruct operation after a 20 ms debounce. The Self_Destruct pin must be enabled using the HWSD RS-232 command. If this pin is high at power on, no self-destruct operation will begin. To trigger a self-destruct operation immediately after power on, drive the pin low for longer than 20 ms, and then drive it high for 20 ms or longer. This pin has an internal pull-down. No external pull down resistor is necessary. Note: This pin has an enable to prevent an accidental destruct operation. The host can use the HWSD RS-232 command to enable or disable this pin. Refer to the part number guide to determine the default state of the enable. **Warning:** Microsemi recommends caution when considering drive voltage levels for the Destruct input. Adhere to published V_{IL} levels to prevent an accidental destruct operation. The destruct operation produces no heat, sparks, or form factor changes. The process is not reversible and is persistent across power cycles. After a destruct operation, the Module_Active signal is high and Status_0, Status_1, and Status_2 indicate that a destruct operation completed.

AA12, Y11, AA10, Y9, AA8, Y7, AA6, Y5, AA4, Y3, W2, V2, U2, T1, R2, P1, N2, M1, L2, K2, J1, H2, G1, F2, E1, D2, C2, B3, A4, B5, A6, B7, A8, B9, A10, B11, A12, B13, A14, B15, A16, B17, A18, B19, A20, B21, A22, C23, D23, D25, E24, F25, G24, H25, J24, K25, M24, N25, P24, R25, T24, U25, V23, V25, W23, Y22, AA21, Y20, AA19, Y18, AA17, Y16, AA15, Y14, AA13			Contact factory
Y12, AA11, Y10, AA9, Y8, AA7, Y6, AA5, Y4, W3, V1, V3, U1, T2, R1, P2, N1, M2, K1, J2, H1, G2, F1, E2, D1, D3, C3, B4, A5, B6, A7, B8, A9, B10, A11, B12, A13, B14, A15, B16, A17, B18, A19, B20, A21, B22, B23, C24, D24, E25, F24, G25, H24, J25, K24, L24, M25, N24, P25, R24, T25, U24, V24, W24, Y23, AA22, Y21, AA20, Y19, AA18, Y17, AA16, Y15, AA14			Contact factory
T10			Contact factory
T12, T14	Back-up_Charger	Out	External backup capacitor array charging voltage. Backup-Charger is a boosted 5 V regulated output for charging a small array of external capacitors connected to the Backup_Pwr pins. If input surge current is a concern, add an optional external resistor in series with this pin and the Backup_Pwr pin to limit the Backup_Pwr charge current. When supplying the Backup_Pwr from an external supply, leave these pins open.

U12, U13, U14, V12, V13, V14, W12, W13, W14	Backup_Pwr	In	Backup power supply input. These pins provide a source of 5 V power for the entire module during power-off events. Connect these pins to an external capacitor array or external 5 V power supply. The MSM048/MSM096 can charge the external capacitor array if the Backup_Charger pin connects to the Backup_Charger capacitor array.
W9	Act_Led_Pwr	Out	Current limited supply for driving an activity led. This is an internal generated supply which has a 200 ohm series resistor. No external series resistor is required.
C9	Activity_N	Out	Module activity signal. See Figure 1 for connections to drive an external LED. 0 = Module active, 1 = Module inactive.
W17	Tx_Port	Out	Optional 19200 baud RS-232 port. Port Transmit output.
W16	Status_2	Out	Most significant bit of the module status. Refer to Table 4 for status codes.
V16	Status_1	Out	Middle bit of the module status. Refer to Table 4 for status codes.
U16	Status_0	Out	Least significant bit of the module status. Refer to Table 4 for status codes.
D9	Module_Active	Out	Indicates the module master status. 1 = The module is active. 0 = Module is un-powered or Vdd is below Vdd min.
N3, N4, N5, N6, N7, P3, P4, P6, P7, R3, R4, R5, R6, R7	NC	DNC	**Reserved for future use or factory test.** **Leave these pins floating. Do not connect.**
U5, U6, U7, V5, V6, V7, W5, W6, W7	2.85V	Power	This internal supply requires 22 uf of external capacitance. Not intended to power external devices.
G3, G4, G5, G6, G7, H3, H4, H6, H7, J3, J4, J5, J6, J7	1.0V	Power	This internal supply requires 22 uf of external capacitance. Not intended to power external devices.
C5, C6, C7, D5, D6, D7, E5, E6, E7	NC	DNC	**Reserved for future use or factory test.** **Leave these pins floating. Do not connect.**
U19, U20, U21, V19, V20, V21, W19, W20, W21	Ps_Pwr	Power	This is an isolated version of the Vdd input supply. An external capacitance of 470 uF is required for the MSM048BM2L-500I (5 volt) device. The MSM048BM2L-M00I (3.3 volt) device requires a single 150 uF ceramic capacitor. This supply is not intended to power external devices.

C4, C19, C20, C21, C22, D19, D20, D21, E3, E12, E15, E19, E20, E21, E23, F9, F10, F11, F12, F13, F14, F15, F17, L6, L7, L19, L20, L21, L22, L23, T11, T15, T16, U3, U23, V9, W22, W4, N19, N20, N21, N22, N23, P19, P20, P22, P23, R19, R20, R21, R22, R23, E14, F16, E9, T9, E16, L4, C17, E11, L5, E13, U9, V10, E10, T17, L3, L1	NC	DNC	**Reserved for future use or factory test. Leave these pins floating. Do not connect.**
L25	Crypto_Std	I/O	Contact factory

Table 4: Status codes on signals: Module_Active, Status_0, Status_1 and Status_2

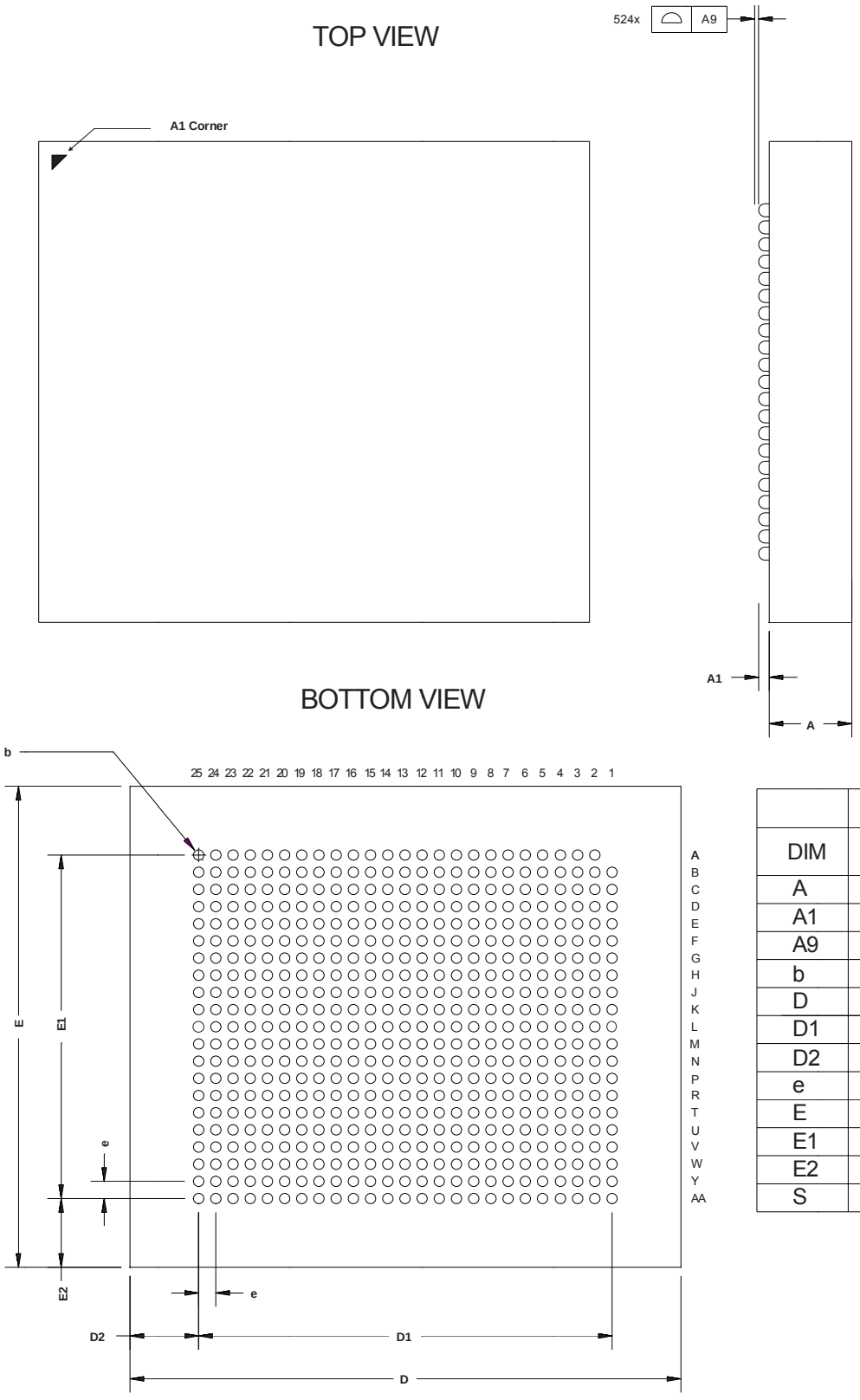
Module_Active[1]	Status_2[1]	Status_1[1]	Status_0[1]	Status code description
0	0	0	0	Module is unpowered or Vdd is below minimum required voltage.
0	0	0	1	Module is waiting for one or more internal voltages, external backup supply, or the temperature to move into acceptable ranges.
0	0	1	0	Reserved for future use.
0	0	1	1	Reserved for future use.
0	1	0	0	Reserved for future use.
0	1	0	1	Reserved for future use.
0	1	1	0	Reserved for future use.
0	1	1	1	Module in deep sleep ZPM mode. (Zero Power Mode)[2]
1	0	0	0	Normal operation.
1	0	0	1	Authentication failed.
1	0	1	0	Reserved for future use.
1	0	1	1	Contact factory for details
1	1	0	0	Contact factory for details
1	1	0	1	Contact factory for details
1	1	1	0	Contact factory for details
1	1	1	1	Contact factory for details

[1] The polarity of these signals can be inverted using an RS-232 command.
Status lines have weak internal pull-down resistors.
The RS-232 status command can provide additional status information and may be beneficial when multiple status events occur concurrently.

[2] Do not use the AT integrity self-destruct mode during ZPM (zero power mode) because AT integrity events are ignored during ZPM to save power.

Table 5: Mechanical and Thermal Properties

Parameter	Value	Units
Form Factor	PBGA	-
Pin array	524	pins
Thickness (including BGA balls)	6.1 max	mm
Length	32 ± 0.25	mm
Width	28 ± 0.25	mm
Weight (MSM model)	12	grams
Weight (MSD model)	158	grams
θ_{JC} Thermal conduction to case	27 (est)	°C/W
θ_{JB} Thermal conduction to PCB	18.6 (est)	°C/W



	MILLIMETERS	
DIM	MIN	MAX
A	4.80	5.50
A1	0.40	0.60
A9	0.15	
b	0.50	0.70
D	31.75	32.25
D1	24.00 BSC	
D2	4.00 BSC	
e	1.00 BSC	
E	27.75	28.25
E1	20.00 BSC	
E2	4.00 BSC	
S	22.95	24.00

Figure 4a: MSM048/MSM096 Dimensions for Module Form-Factor (48 GB and 96 GB form-factor and pin-out are identical)

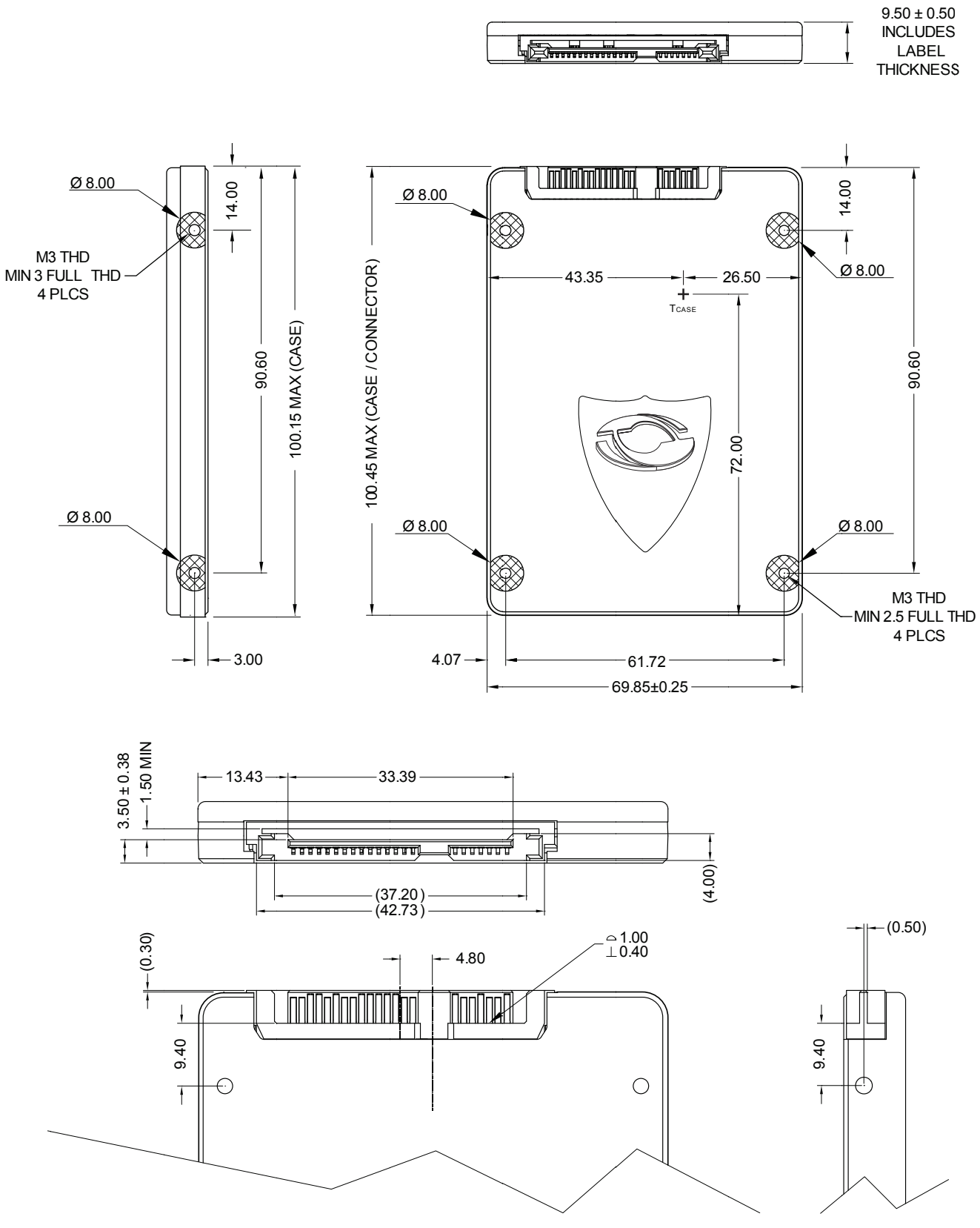


Figure 4b: MSD048/MSD096 dimensions for 2.5” Form-Factor

Table 6: MSD048 and MSD096 Connector Pin Descriptions (2.5" Form-Factor)

Pin	Name	Description
S1	Ground	Power supply ground. Connects to S4 and S7.
S2	SATA Rx_P	Positive SATA differential receive signal from host system.
S3	SATA Rx_N	Negative SATA differential receive signal from host system.
S4	Ground	Power supply ground. Connects to S1 and S7.
S5	SATA Tx_N	Negative SATA differential transmit signal to host system.
S6	SATA Tx_P	Positive SATA differential transmit signal to host system.
S7	Ground	Power supply ground. Connects to S1 and S4.
P1	Deep Slumber trigger[3]	Pull pin to 3.3v to enter from Deep Slumber mode. See note 2.
P2	Erase/Destruct trigger[3]	Erase trigger input. Optional destruct trigger input. See note 1.
P3	Unused[3]	Unused.
P4	Erase/Destruct return[3]	Return path for erase/destruct trigger on P2. See note 1.
P5	Ground[3]	Power supply ground. Connects to P6, P10, and P12.
P6	Ground[3]	Power supply ground. Connects to P5, P10, and P12.
P7	5 V	3.3 V to 5 V power. Connects to P8 and P9.
P8	5 V	3.3 V to 5 V power. Connects to P7 and P9.
P9	5 V	3.3 V to 5 V power. Connects to P7 and P8.
P10	Ground	Power supply ground. Connects to P5, P6, and P12.
P11	DAS/DSS	Device Activity Signal/Disable Staggered Spin up.
P12	Ground	Power supply ground. Connects to P5, P6, and P10.
P13	Secure erase return[3]	Legacy secure erase return. See note 1.
P14	Unused[3]	Unused
P15	Unused[3]	Unused

Notes:

1. A pulse applied to pins P2 and P4 can trigger an erase or destruct operation. Two external erase/destruct trigger modes exist. The operation of P2 is programmable using a RS-232 command or can be set by the factory.
   Mode 1: Connect pin P2 to a voltage capable of supplying 5-12 mA at 3.3v. The MSD048/MSD096 has internal current limiting so the external voltage can range from 3.3 to 50v with no series resistor required. Connect a switch between pin P4 and ground. When the switch is closed, 5-12 mA runs from the supply connected to pin P2, out pin P4, through the external switch to the external voltage ground (return). There is no significant current draw (<10 uA) on the external supply until the switch is closed. During closure, the switch should be able to sink 5-12 mA while maintaining less than 0.5v at pin P4.

   Mode 2: Mode 2 is a legacy erase/destruct mode that uses the 12V pin (P13) for the ground return path. To implement mode 2 erase/destruct triggering, connect pin P2 to a voltage capable of supplying 5-12 mA at 3.3v. The MSD048/MSD096 has internal current limiting so the external voltage can range from 3.3 to 50v with no series resistor required. Connect a switch between pin P13 and ground. When the switch is closed, 5-12 mA runs from the supply connected to pin P2, out pin P13, through the external switch to the external voltage ground (return). There is no significant current draw (< 10ua) on the external supply until the switch is closed. During closure, the switch should be able to sink 5-12 mA while maintaining less than 0.5v at pin P13.

2. The MSD048/MSD096 can enter a very low power Deep Slumber mode by pulling the Deep Slumber trigger pin P1 high for 20 ms. To exit the Deep Slumber mode, pull pin P1 to ground.

3. ***Standard SATA cable connectors often have pins P1, P2, P3 shorted together, pins P13, P14,P15 shorted together and pins P4, P5 and P6 shorted together. Since the MSD048/MSD096 uses some of these pins for erase, destruct and Deep Slumber features, use of connectors with shorted pins may produce unexpected results. Be sure to evaluate connector choices carefully prior to using them in a design.***

Table 7: System Specifications and Characteristics

Feature	Characteristic
Security and AT features	AES-128 encryption in CTR mode, AES key purge feature. Contact factory for full data sheet.
Random number generator (RNG)	Yes. Results accessible using the RS-232 port.
AES key purge operation	Key erasure and new random key generated in < 4 sec
Self-Destruct completion time	Less than 0.100 seconds for self-destruct operation, then 4 seconds for the AES key over-write, plus whole module erase time (if enabled).
Whole module erase	Yes. < 20 sec (MSM048) < 40 sec (MSM096)
Auto restart of Crypto or Flash Erase after power loss	Yes
Internal flash capacity – (MSM096)	96 GiB (1 GiB = 1,073,741,824 bytes)
Internal flash capacity – (MSM048)	48 GiB (1 GiB = 1,073,741,824 bytes)
Type of flash storage media	12/24 die, 32 Gbit each. 25nm, 1-bit SLC NAND
Sector size	512 bytes
Total LBAs available – (MSM096)	146,533,968
Total LBAs available – (MSM048)	73,277,568
Power to ready time	Less than 2 seconds
Operating system compatibility	OS independent
NCQ and Trim command support	Yes
ECC	Reed Solomon. Corrects 16, 9-bit symbols per sector.
UBER (uncorrectable bit error rate)	1×10^{-17}
“Silent data corruption” protection	Yes, 32-bit per sector CRC
Minimum write endurance (total bytes written) Note: This is an estimate only.	2.25 PB (MSM096) 1.1 PB (MSM048) Based on 100K PE cycles
Wear leveling	Yes (both read and write operations)
Bit Disturb scrubbing	Approximately once per 1000 hours of operation
NAND flash processor	Sandforce SF-1565
Data compression to extend flash life	Yes
Boot code	Boot code stored in flash media
Power disturbance protection	Yes, from energy stored in external array of capacitors
Over/Under voltage protection	Yes
Brown-out/Black-out protection	Yes

Table 7: System Specifications and Characteristics (Continued)

Input supply sudden short protection	Yes
Power-on inrush current limiting	Yes, See Figure 2
Life remaining indicator (0 to 100%)	Yes, using S.M.A.R.T. command (0xE7)
Temperature	Yes, using S.M.A.R.T. command (0xC2)
Power on hours indication	Yes, using S.M.A.R.T. command (0x09)
External capacitor array health. (0 to 100%)	Yes, using S.M.A.R.T. command (0xEB)
ESD protection	2000 V
Status and mode indications	Activity LED and Status signals.
Field upgradable firmware	Yes
Operating Temperature	-40°C to +85 °C

MSM048 Read and Write Performance Benchmarks (Actual performance will vary based on data)

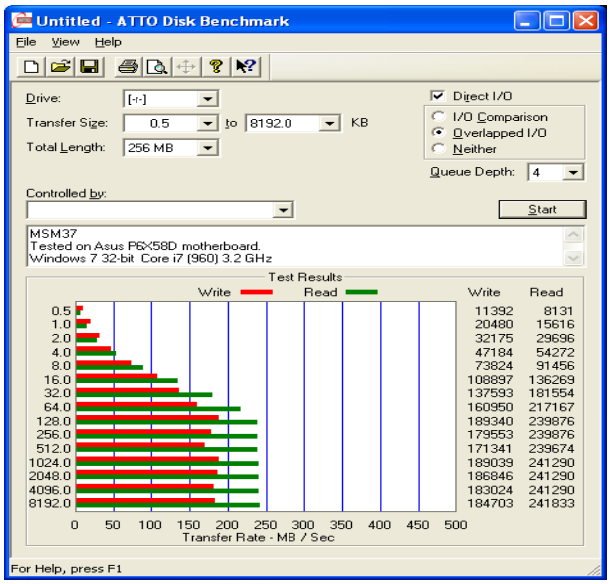


Figure 5a: ATTO

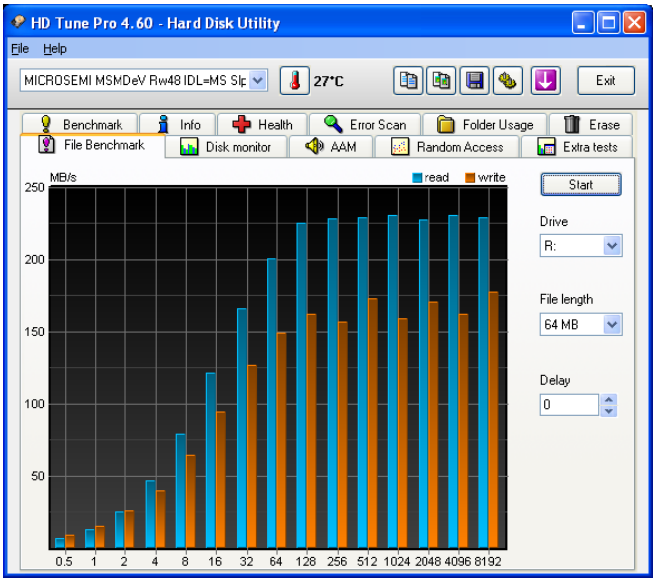


Figure 5b: HD Tune Pro 4.6 file benchmark

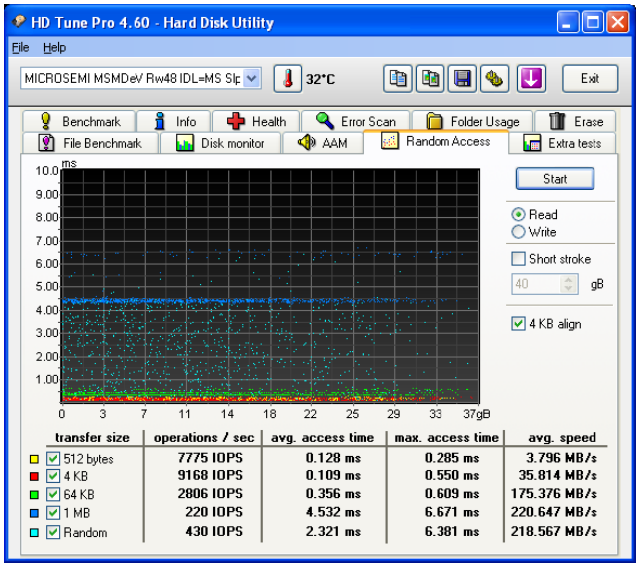


Figure 5c: HD Tune 4.6 Random Read

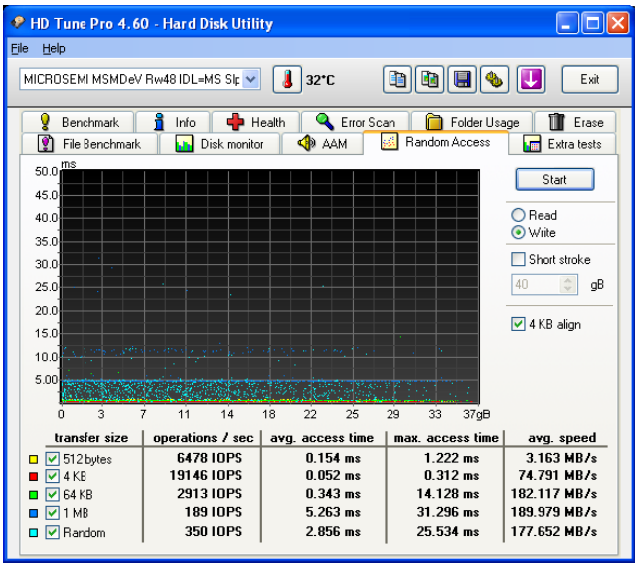


Figure 5d: HD Tune Pro 4.6 Random Write

Iometer results (version 2006.07.27) for the MSM048

Sequential MBps

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Read	5	10	18	33	54	78	105	132	156
75%R 25%W	6	10	16	29	41	51	64	76	80
50%R 50%W	6	11	17	29	36	44	51	48	51
25%R 75%W	7	13	19	31	38	41	39	39	39
100% Write	7	15	21	40	43	43	43	43	44

Random MBps

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Read	2	5	10	19	35	59	87	116	147
75%R 25%W	2	4	9	17	29	45	65	89	112
50%R 50%W	2	4	8	15	24	37	52	64	55
25%R 75%W	1	3	6	10	15	22	31	37	38
100% Write	1	3	5	9	14	20	28	30	28

Sequential IOPS

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Read	11005	10798	9683	8693	6984	5026	3391	2118	1252
75%R 25%W	13233	10547	8583	7588	5288	3276	2053	1229	640
50%R 50%W	13935	12206	8739	7430	4658	2851	1648	783	410
25%R 75%W	15418	13831	9801	8043	4913	2637	1253	636	319
100% Write	16319	15891	10993	10421	5521	2788	1399	694	358

Random IOPS

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Read	5467	5398	5248	5028	4489	3810	2797	1858	1179
75%R 25%W	5022	5021	4715	4421	3731	2939	2099	1426	897
50%R 50%W	4688	4546	4257	3943	3168	2428	1693	1024	441
25%R 75%W	3558	3429	3081	2718	2024	1468	1015	604	305
100% Write	3205	3110	2809	2432	1843	1333	903	492	228

Iometer results (version 2006.07.27) for the MSM096

Sequential MBps

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Reads	5	11	21	39	65	95	126	156	179
75%R 25%W	7	12	21	39	57	77	98	124	147
50%R 50%W	7	12	20	39	55	73	96	121	131
25%R 75%W	8	14	21	41	55	72	89	98	98
100% Writes	8	15	23	71	86	82	81	84	83

Random MBps

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Reads	3	6	11	22	41	71	113	157	197
75%R 25%W	2	5	11	21	36	59	87	122	156
50%R 50%W	2	5	10	19	32	49	70	99	127
25%R 75%W	2	5	9	17	27	40	56	79	105
100% Writes	2	4	8	15	24	35	48	69	92

Sequential IOPS

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Reads	11846	11549	10998	10231	8345	6102	4052	2496	1436
75%R 25%W	14638	12872	10830	10103	7309	4943	3161	1999	1177
50%R 50%W	15404	13236	10507	10073	7084	4715	3085	1941	1048
25%R 75%W	16407	14527	11008	10559	7147	4636	2850	1577	786
100% Writes	17162	15860	12091	18230	11121	5292	2617	1349	670

Random IOPS

	512 B	1 KiB	2 KiB	4 KiB	8 KiB	16 KiB	32 KiB	64 KiB	128 KiB
100% Reads	6228	6184	6104	5884	5322	4600	3617	2526	1578
75%R 25%W	6136	5955	5704	5420	4686	3783	2791	1957	1252
50%R 50%W	5872	5631	5328	5029	4113	3166	2248	1588	1020
25%R 75%W	5460	5181	4819	4473	3500	2612	1817	1278	840
100% Writes	5059	4771	4391	4084	3074	2256	1557	1112	739

MSM048/MSM096 Description

The MSM048/MSM096 is a complete SATA based system-in-a-module developed by Microsemi Corporation to address the need for secure, high density storage in a compact BGA form factor.

The MSM048/MSM096 contains a state-of-the-art flash processor, 12/24 NAND flash die, 5 power supplies, voltage supervisor logic, power isolation logic, over/under voltage isolation, hardware authentication, Random number Generator, AES 128 encryption, SHA-256 crypto logic, AT logic, temperature-rate-of-change monitoring, self-destruct logic and a user accessible stand-alone crypto device.

With the application of power, a voltage supervisor in the MSM048/MSM096 module begins monitoring the Vdd voltage level. Once Vdd reaches approximately 2 V, the voltage supervisor begins monitoring the backup power supply voltage, Backup_Pwr. Once the Backup_Pwr supply reaches acceptable levels the voltage supervisor sets the Module_Active signal to a high level.

Internally, a buck/boost regulator regulates Vdd to 5.0 V and outputs the boosted voltage on the Backup_Charger pin. The Backup_Charger pin typically connects to the Backup_Pwr pins and an external array of backup power supply capacitors. The Backup_Charger pin provides a low current trickle charge to the backup power supply capacitors. Optionally, an external resistor can be connected between the Backup_Charger pin and the Backup_Pwr capacitor array to further limit inrush current. Capacitors in the Backup_Pwr array supply several milli-seconds of full power operation during power down events. The ability to continue operation for a short time after a total power loss allows the MSM048/MSM096 to shut down in an orderly fashion under all power disturbance conditions.

Once the voltage on the Backup_Pwr pins (and the connected capacitor array) reaches a fully charged value of 5.0 V, the voltage supervisor enables regulators that power the integrated flash processor. When the flash processor regulators reach valid voltages, the voltage supervisor enables the flash processor to begin normal operation. If any failure occurs during the power-on sequence, the voltage supervision writes an error code to the status signals, Status_0, Status_1, and Status_2 and restarts the entire power-up process.

After a successful power-on cycle, the voltage supervisor continually monitors Vdd and all module voltages. Any significant voltage disturbance causes the voltage supervisor to switch to the Backup_Pwr supply and signal the internal flash processor to shut down. After the flash processor completes an orderly shutdown, the voltage supervisor disables the internal regulators, waits for Vdd to stabilize, then resumes a normal power-on sequence.

Normal operation

In the normal operating mode, the MSM048/MSM096 operates as a standard SATA storage device compliant with the Serial ATA (SATA) specification version 2.6. The SATA interface operates at speeds of 1.5 Gbps and 3 Gbps. When the MSM048/MSM096 first communicates with the host system, it attempts communication at 3 Gbps and automatically switches to 1.5 Gbps if the initial communication is unsuccessful.

Like most flash based storage systems, the MSM048/MSM096 attains the highest level of performance when the host system writes or reads data in block sizes of 64 KiB and larger. Additionally, like all NAND flash-based storage systems the media is consumable and will eventually wear out. Systems designers need to be aware that the retention capabilities of the NAND flash diminish with continued use as the device approaches the natural write endurance limit. The flash in the MSM048/MSM096 has an initial retention capability of about 10 years. The retention capability at end of life may be less than 30 days.

Low Power Modes

The Serial ATA specification defines two power saving modes, *partial* and *slumber*. The MSM048/MSM096 implements both power management modes and well as a Microsemi proprietary Deep Slumber mode (ZPM). Pulling the ZPM pin to a high level allows the MSM048/MSM096 to enter a very low power Deep Slumber mode. The MSM048/MSM096 treats the ZPM mode in the same way as it treats a hot swap or power down event. The MSM048/MSM096 completes the command currently in progress and then proceeds to an orderly shutdown.

During the ZPM mode, the MSM048/MSM096 ignores commands on the SATA bus so it is important that external logic control the ZPM pin in order to wake the module from the ZPM mode and resume normal device operation as required by the host system.

Destruct operation (combined with Erase_Trigger on MSD model)

The MSM048/MSM096 has built in algorithms capable of initiating a one-time self-destruct operation in less than 100 ms. The destruct process is covert and produces no spark, flame, or heat, and the form factor of the module remains unchanged during and after the destruct operation. The destruct method inflicts changes to control algorithms/logic within the module, and erases internal product firmware. The process is permanent across power cycles, and is not reversible. Data in the flash media is inaccessible. Once the destruct operation completes, the module operates in a low power mode similar to ZPM. The status signals Status_0, Status_1 and Status_2 indicate that a self-destruct operation completed. To prevent accidental destruct and erase operations, Microsemi supports a part number to ship devices with the Self_Destruct and Erase_Trigger pins pin disabled. The host can use the HWET and HWSD RS-232 command to individually enable or disable each trigger input.

The MSM048/MSM096 further protects stored data by triggering a whole module erase, and/or an AES key purge operation ***in parallel*** with the self-destruct. After the self-destruct operation completes, the NAND media is no longer accessible, is erased, and a different AES key replaces the previous AES key.

The Self_Destruct input contains a weak (10K) pull down resistor to prevent an unintentional destruct operation. In applications that do not need the self-destruct feature, tie the Self_Destruct pin to ground.

To trigger a destruct operation, bring the Destruct pin high for 20 ms or longer or use the RS-232 module destruct command.

The MSM048/MSM096 contains a programmable feature to perform an automatic self-destruct operation, after multiple authentication failures, AT Integrity failures, or temperature-rate-of-change events. These features are programmable using commands from the RS-232 port. Refer to Table 9 for instructions on how to implement security features with RS-232 commands.

Encryption and AES Key Purge

The MSM048/MSM096 protects data at rest in the flash storage media using a self-generated key and hardware based AES-128 encryption running in a CTR mode.

The MSM048/MSM096 supports an AES key purge feature, which renders data to a forensically unrecoverable encrypted state by elimination of the encryption key. The AES key purge operation completes in 4 seconds. The feature eliminates the AES key and erases all module meta-data (cache data, tables, and pointers). When the purge operation completes, the MSM048/MSM096 is in a new device state. All previous stored data is unrecoverable because both the AES key and the translation tables went through an initialization process.

Hardware Authentication

The MSM048/MSM096 contains hardware authentication logic that is capable of preventing the module from operating in unauthorized environments. The module implements authentication using random 256-bit SHA-256 hashed challenges to an external crypto device or a crypto host simulator. Removing the module from an authorized environment causes the module to cease further operations and shutdown to a low power mode similar to ZPM. It is also possible to setup the MSM048/MSM096 to initiate an erase and/or self-destruct operation after detection of attempted operation in an unauthorized environment.

The action taken by the MSM048/MSM096 module is often application dependent. Use the RS-232 interface to setup and program the hardware authentication mode. Hardware authentication may require additional external logic.

256-bit Pass-Phrase

The MSM048/MSM096 has the ability to inhibit all storage operations and ignore RS-232 commands until the host system supplies the module with a valid Pass-Phrase using the RS-232 interface. The module uses SHA-256 to hash an initial Pass-Phrase sent by a host system. Internal logic saves a hashed version of the host supplied initial Pass-Phrase in a secure memory. The module begins Pass-Phrase locked operation at the beginning of each power-on cycle if the module was Pass-Phrase locked during a previous power cycle. Pass-Phrase locked operation is persistent across power cycles so it is not necessary to re-lock the module prior to each successive power cycle. The module remains in Pass-Phrase locked mode across all successive power cycles until a Pass-Phrase Off command executes.

With the application of power, the module enters a low power mode if the Pass-Phrase locked mode is active. The module monitors the RS-232 port for a Pass-Phrase from the host system. During this phase, the module maintains the storage interface in a disabled state. When the host system supplies a Pass-Phrase value, the module hashes it with SHA-256 and compares the hashed pass phrase to the previously stored (hashed) Pass-Phrase. If the two Pass-Phrases match, the MSM048/MSM096 unlocks and begins operating normally. Microsemi ships modules with the Pass-Phrase feature disabled. To begin Pass-Phrase locked operation, use the RS-232 port to install an initial Pass-Phrase.

It is not possible to exit the Pass-Phrase locked mode if the current Pass-Phrase is unknown. If the Pass-Phrase is unknown, the only way to restore the operation of the module is to trigger a whole module erase operation. Refer to Table 9 for a description of Pass-Phrase and other RS-232 security commands. Microsemi can customize the operation of the Pass-Phrase feature to meet the requirements of customer applications. Contact Microsemi for details.

Crypto Erase or Flash Erase Operations

A Crypto or whole module Flash Erase feature is available. The Crypto Erase clears the encryption key and generates a new key. The Flash Erase feature erases the NAND flash.

Warning: To avoid potential permanent corruption of the flash controller, it is critical that the host system avoid a power loss event within 4 seconds of triggering Crypto Erase or Flash Erase operations.

The MSM048/MSM096 supports three triggering methods: An external switch attached to the Erase_Trigger input, the ATA security feature set, or a RS-232 command. The ATA Security Feature Set uses the Security Erase Unit and Security Erase Prepare ATA commands. The MSM048/MSM096 Programmer's guide includes additional information.

ECC (Error Correction)

NAND flash devices are based on a consumable technology. Continued read and write operations cause bit disturb errors and a slow continuous degradation of the storage media. While nothing can stop the degradation of the NAND media, data management techniques and error correction can greatly extend the life of products incorporating NAND flash. Using a Reed-Solomon error-correction algorithm, the Microsemi MSM048/MSM096 module has the ability to correct 16, 9-bit symbols in *each* 512 byte sector across the entire SSD. This translates into an Uncorrectable Bit Error Rate (UBER) of per 10^{-17}.

Bit Disturb Scrubbing

The individual bits in NAND flash are susceptible to corruption from random bit-disturb errors. These errors build up slowly over time and will, if left uncorrected, eventually cause uncorrectable ECC errors and early device failure. The causes of the errors are the very operations that make the flash device useful: read, program, and erase operations. Each time one of these operations occurs, a tiny bit of energy leaks/disturbs nearby storage cells. Over time, the continuing energy disturbances cause bits to flip state. When enough bits in a given sector flip state, the error correction logic can no longer correct all the errors and an uncorrectable ECC failure occurs. The MSM048/MSM096 flash processor contains algorithms to mitigate bit disturb errors by reading, correcting, and re-writing the entire contents of the flash media once every 1000 hours of operation. This "bit re-fresh" removes the opportunity for the bit-disturb errors to build up to the 16-symbol correction limit of the MSM048/MSM096 flash processor.

CRC (Cyclic Redundancy Check) and Silent Data Corruption

The Microsemi MSM048/MSM096 includes a 32-bit CRC, which acts as a final check for the integrity of data returned to the host system. The CRC function provides protection against "silent data corruption". The CRC operation does not correct errors; instead, it verifies that the data returned by the ECC is the data originally written by the host. Like any other flash-based storage device, as the number of write cycles issued to the MSM048/MSM096 approaches the write endurance limit, ECC errors become more and more frequent. At the end of life, with continued use, the number of bit errors eventually exceeds the number of ECC symbols that the module can correct. At this point, the MSM048/MSM096 CRC logic detects any uncorrectable ECC errors and notifies the host system of the error. Without CRC protection, "silent data corruption" would go unrecognized and possibly lead to unpredictable operation in the host system.

Power Disturbance Protection

A majority of storage device field-failures in extended environment applications are traceable to different types of power disruptions. Power spikes, noise, unexpected power loss, brownouts, and various other host based power supply problems can lead to permanent corruption and data loss. Many commodity storage products use batteries or super capacitors to provide hold-up time for the flash controller/processor to backup critical tables and proceed to an orderly shutdown during power disturbances.

Using batteries and super capacitors is acceptable for comparatively benign environments like that of an enterprise server but in extended environments common to the defense market, temperature extremes cause these devices to quickly degrade and fail. Once degraded, the next power disturbance causes an unrecoverable failure.

Realizing this as a critical issue in high reliability mission critical systems, the Microsemi MSM048/MSM096 utilizes a small array of external capacitors and "on-chip" proprietary power management circuitry. When the MSM048/MSM096 detects a significant power disturbance event, the power management circuitry fully isolates the module from the external power source, and begins using energy stored in the external capacitor array to fully power module while it proceeds to an orderly shutdown.

The external capacitor array that supplies the energy during power loss events must be large enough to maintain full power to the module during the entire power down process. Refer to Table 2 to determine the minimum required external backup power supply capacitance. Microsemi does not recommend the use of super capacitors as the energy storage device in the backup power supply. Super capacitors contain components that break down at high temperatures (greater than 50° C) and freeze at low temperatures.

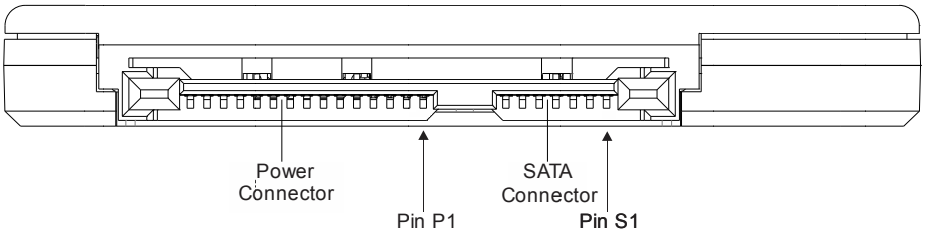
Design and Manufacturing

The MSM048/MSM096 was designed by US citizens and manufactured in a trusted (DMEA accredited) US facility with full BOM and assembly control and cleared staff for classified programs. The MSM048/MSM096 design team works in labs at the trusted facility in Phoenix Arizona. This is the same facility which manufacturers, assembles, and tests the MSD50/MSD100 and other secure storage products.

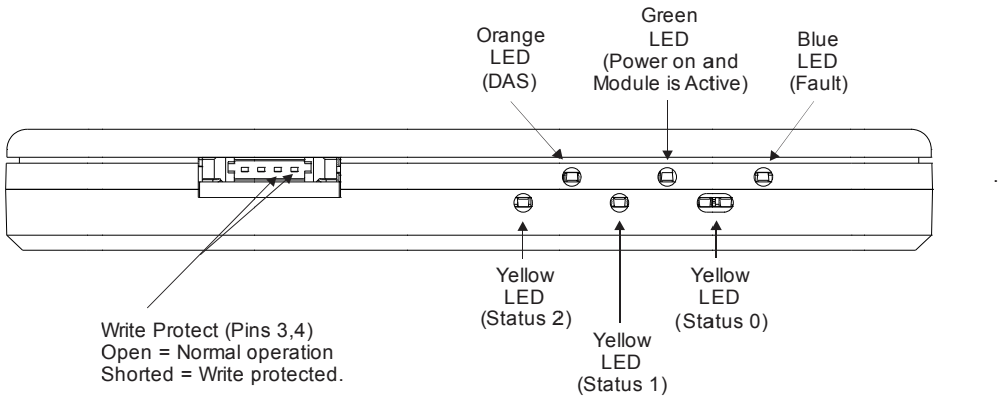
Differences in Operation of the MSD model (2.5" Form-Factor)

The MSD048 and MSD096 models have a different from factor than the MSM048 and the MSM096. The MSD048/MSM096 models are designed around the industry standard 2.5" form-factor instead of a BGA from factor. A summary of the feature differences appear in the list below.

- The MSD models do not support AT Integrity features.
- The MSD model ZPM (deep slumber mode) is located on pin P1 of the power segment of the SATA connector.



- The MSD model Erase_Trigger pin is located on pin P2 of the power segment of the SATA connector.
- The MSD model Auth pin is located on pin P3 of the power segment of the SATA connector.
- The MSD model shares the Erase_Trigger pin (P2) for both erase and destruct operations. An RS-232 command programs the operation of the pin or the unit can be special ordered with erase or destruct operation pre-programmed.
- The MSD model includes all required external components as well as operating LEDs.



- The status signals on the MSD model are available on LEDs and from the RS-232 port.
- The MSD model has the write protect pin located on the RS-232 port.

RS-232 Communications Port

An RS-232 port with 3.3 V logic levels connects to the Rx_Port and Tx_Port pins of the MSM048/MSM096 module and MSD048/MSD075 SSD. The RS-232 port can be used to determine the status of the module and execute commands that enable/disable the module's features (i.e., authentication, self destruct, etc.). Table 9 lists the supported RS-232 commands. The module implements the port with 3.3 V LVTTL levels. The RS-232 port setup requires 19,200 baud with 8 data bits, one stop bit, and no parity.

Notes:

- The RS-232 commands are not case sensitive.
- The RS-232 commands use ASCII hexadecimal values.
- The RS-232 commands must include a trailing carriage-return character, 0x0D.
- The RS-232 commands must not include spaces.
- Table 9 describes the RS-232 commands with bracket characters surrounding the input arguments; the bracket characters must not be included in the RS-232 command.
- The module responds with an error message with format E:<message> when a command does not complete successfully.
- Any command that is ignored because of an improper prior setup, mode, or input syntax error cause the module to respond with an error message with format E:<message>.
- The module responds to all RS-232 commands with a trailing carriage-return character (0x0D), new-line characters (0x0A), and prompt '>' character (0x3E).
- Some of the RS-232 commands change the operating mode; use the ST (status) command to determine the active modes and module status.
- Refer to Table 10 for examples of command usage.
- Once the module is commanded to execute a self-destruct command, the RS-232 port responds to all commands with the '!' character followed by a carriage-return character (0x0D), and new-line characters (0x0A). The self-destruct operation is irreversible. It is not possible to recover or restore the module to a working state after executing a self-destruct operation.

Table 9: RS-232 commands[2]

Command	Command description
	Contact Microsemi for the full data sheet.

Table 10: RS-232 command examples

RS-232 Command Examples	Description
	Contact Microsemi for the full data sheet.

MSM048/MSM096/ MSD048/MSD096 Part Numbering Guide

M	SM	XXX	B	M	2	L	–	M	00	I	P
1	2	3	4	5	6	7		8	9	10	11

Example part numbers:

MSM048BM2L-M00C, MSM048BM2L-MDXC, MSM048BM2L-M00I, MSM048BM2L-MDXI
MSM096BM2L-M00C, MSM096BM2L-MDXC, MSM096BM2L-M00I, MSM096BM2L-MDXI
MSM048BM2L-M00CP, MSM048BM2L-MDXCP, MSM048BM2L-M00IP, MSM048BM2L-MDXIP
MSM096BM2L-M00CP, MSM096BM2L-MDXCP, MSM096BM2L-M00IP, MSM096BM2L-MDXIP

Field 1: Manufacturer
M = Microsemi Corp

Field 2: Form Factor
SM = 32 mm x 28 mm BGA module. 524 pins.
SD = 2.5” standard SSD form-factor.

Field 3: NAND Capacity to Host
048 = 37.5 GB (48 GiB internal capacity prior to over-provisioning)
096 = 75.0 GB (96 GiB internal capacity prior to over-provisioning)

Field 4: Encryption
B = AES-128 Encryption using SF-1565 processor

Field 5: Media Manufacturer
M = Micron

Field 6: Media Type
2 = 1-bit SLC NAND flash, 32-Gbit technology (25 nm) device

Field 7 : Construction
L = Leaded BGAs

–

Field 8: Power supply Option
M = 3.3 V to 5.0 V power supply range.

Field 9: Customizable Features
00 = **(MSM and MSD models)** No Authentication, No Self-Destruct, No AT Integrity.
DT = **(MSD model in 2.5” form factor)** Authentication, Self-Destruct, No AT Integrity. The MSD model combines the Self_Destruct and Erase_Trigger functions into one pin.
DX = **(MSM model in BGA form-factor)** Authentication, Self-Destruct, AT Integrity.

Field 10 : Operating Temperature
I = Industrial (-40 °C to +85 °C)
C = Commercial (0 °C to 70 °C)

Field 11 : Classification.
Blank = Fully qualified product shipped with trigger pins enabled.
P = Fully qualified product shipped in protected mode that has the trigger pins disabled. Product is shipped with the external triggers, Erase_Trigger and Self_Destruct, in the disabled state. Use the HWET, HWSD RS-232 commands to enable the external trigger(s).

MSM048 and MSM096 EVALUATION BOARD

Figure 7 shows an image of the evaluation board for the MSM048 or MSM096. The part number for the 48 GB evaluation board is **MSM048BM2L-M00CEV** and the 96 GB version is **MSM096BM2L- M00CEV.**

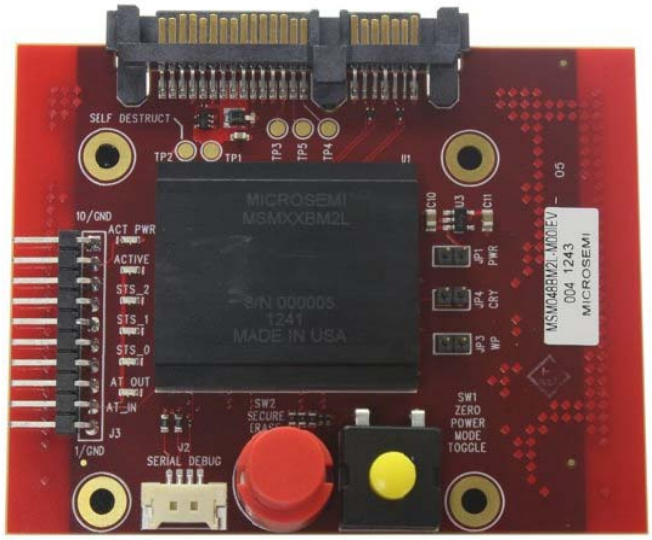


Figure 7: MSM048/MSM096 evaluation board.

