Preliminary Information

Microsemi Corporation

MSM37 and MSM75

Secure SLC NAND SATA BGA Module

with Hardware Authentication and Self Destruct

This product is not qualified or fully characterized and is subject to change without notice.

Secure SLC NAND Flash SATA BGA

General Description

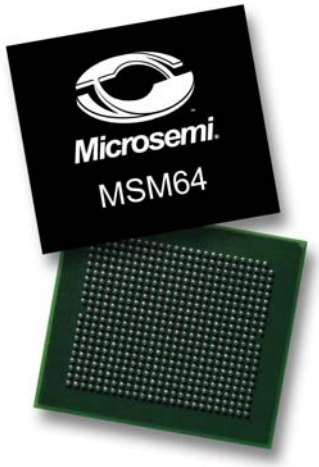
The Microsemi MSM37/MSM75 is a complete SATA storage system packaged as a single 32 mm x 28 mm, 524 pin PBGA. Perfect for embedded defense applications where a full sized 2.5" storage device is too large, the Microsemi SATA BGA combines a SATA flash controller with the latest in small geometry SLC NAND flash and security features including encryption, authentication, anti-tamper (AT), as well as self-destruct features into a single module. The MSM37/MSM75 SATA BGA module is available with 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[1]

- 96 GB/48 GB raw flash capacity before over-provisioning.
- Minimal external components.
- Zero power standby mode (ZPM).
- Wide single supply voltage range: 3.3 to 5.5 V.
- Hardware **AES-128** encryption running CTR mode.
- Hardware authentication.
- AT Integrity, tamper resistant features.
- Temperature rate of change AT mitigation.
- **SHA-256** pass-phrase feature.
- Self-destruct capability.
- AES key purge feature eliminates encryption key.
- Whole module erase with "push-button" trigger option.
- Support for military sanitization protocols.
- 1-bit, Single Level Cell (SLC) NAND flash.
- 16, 9-bit symbol ECC correction capability.
- Sequential R/W 128 KiB performance MSM37: 156/44 MB/s.
- Sequential R/W 128 KiB performance MSM75: 179/83 MB/s.
- Sequential R/W IOPS MSM37: 8693/10421(4K)
- Sequential R/W IOPS MSM75: 10231/18230(4K)
- Random R/W IOPS MSM37: 5028/2432(4K)
- Random R/W IOPS MSM75: 5884/4084(4K)
- "Silent error" protection with 32-bit per sector CRC.
- 2 PB write endurance (MSM75).
- Abrupt power interruption protection.
- Over and under voltage detection and protection.
- Field upgradable firmware using SATA interface.
- 100% dynamic burn-in.
- Module BIST (Built-In Self-Test).
- Write protect option for read-only applications.
- Includes high quality DC blocking capacitors on the SATA signals.
- Operational temperature range of -40 °C to +85 °C
- Storage Temperature: -55 °C to +105 °C.
- Weight: TBD grams.

Applications

Ruggedized mobile defense systems
Battlefield robotics
Data recorders and digital maps
Industrial automation
Transportation systems
Mobile secure medical products

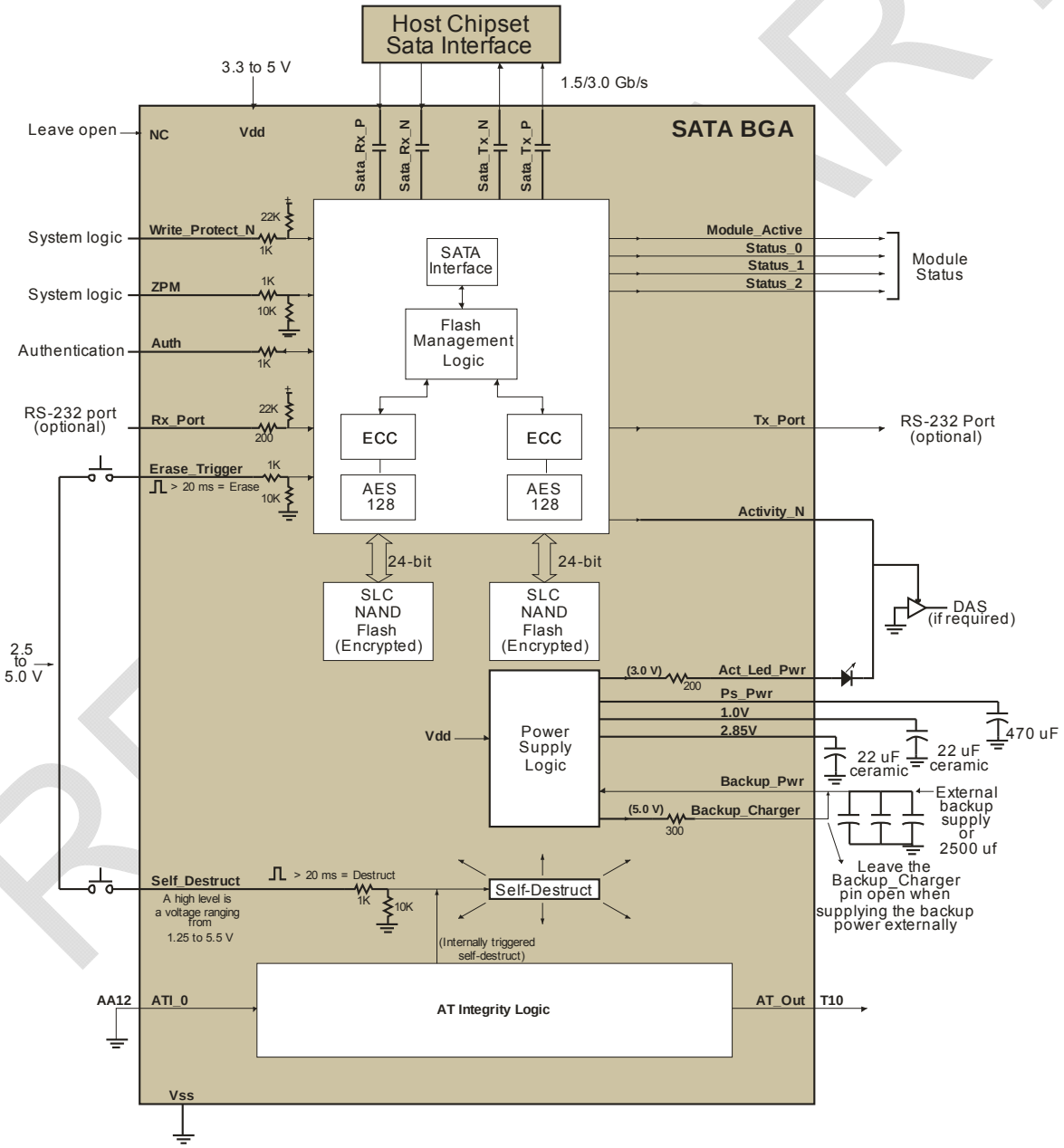


Product image is approximately life size

Note 1: Preliminary. This product is not qualified or fully characterized and is subject to change without notice.
Note 2: One Gigabyte (GB) = 1,000,000,000 bytes.

Figure 1 shows the connections necessary to use the MSM37/MSM75 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 erase, sanitize, 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. An optional RS-232 port allows a host controller to monitor the status of the module and enable or disable various operating modes. A feature called AT Integrity supports a multitude of possible Anti-Tamper features.



Note: The MSM37/MSM75 includes high quality DC blocking capacitors on the SATA lines.

Figure 1: Typical application

Electrical Characteristics

Table 1: Absolute Maximum Ratings

Parameter and Condition	Min	Max	Unit
Vdd supply voltage	-0.3	5.5	V
Voltage on Write_Protect_N, ZPM, Auth, Erase_Trigger, Self_Destruct, ATI_[0..N], and Backup_Pwr with respect to Vss.	-0.3	Vdd + 0.3 V	V
Voltage on Rx_Port	-0.3	3.6	V
Maximum input/output current: Write_Protect, ZPM, Auth, Rx_Port, Erase_Trigger, Self_Destruct, ATI_[0..N], ATO_[0..N], AT_Out, Tx_Port, Status_0, Status_1, Status_2 and Module_Active		±2	mA
Maximum source/sink current: Act_Led_Pwr		15/0	mA
Maximum source/sink current: Activity_N		2/6	mA
Maximum source/sink current: Backup_Charger		17/0	mA
Operating temperature	-40	+85	°C
Operating temperature rate of change Warning: If the temperature-rate-of-change anti-tamper feature is enabled, exceeding the programmed temperature-rate-of-change limit will initiate an automatic self-destruct operation.		5	°C/minute
Storage temperature	-55	+105	°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 Operating Characteristics

Parameter	Min	Typ	Max	Unit
Vdd supply voltage	3.20	3.3	5.5	V
Backup_Pwr voltage	5.0	5.0	5.5	V
V_{IL} (Input low voltage) Write_Protect_N, ZPM, Auth, Rx_Port, Erase_Trigger, Self_Destruct, ATI_[0..N]	0		0.5	V
V_{IH} (Input high voltage) Write_Protect_N, ZPM, Auth, Erase_Trigger, ATI_[0..N]	2.0	3.3	Vdd	V
V_{IH} (Input high voltage) Self_Destruct	1.25	3.3	Vdd	V
V_{IH} (Input high voltage) Rx_Port	2.0	3.3	3.6	V
V_{OH} (Output high voltage, 10 uA load) Module_Active, Status_0, Status_1, Status_2, Tx_Port, AT_Out	2.4	3.0	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		5.0	5.1	V
I_{OUT} Act_Led_Pwr current (with 1.5v LED drop)	4	7	8	mA
I_{SC} Backup_Charger short circuit current		16	17	mA
V_{OH} Backup_Charger voltage (no load)		5.0	5.10	V
V_{OH} and V_{OL} of ATO_[0..N]	Typically ATI_0 ± 0.1 V			
V_{OL} (Output low voltage with load of 2 mA) Module_Active, Status_0, Status_1, Status_2, Tx_Port, Activity_N, AT_Out	-	0.1	0.6	V

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

Parameter	Min	Typ	Max	Unit
I_{IH} (Input High Current. Inputs tied to Vdd = 3.3 V) Write_Protect_N, ZPM, Auth, Erase_Trigger, Self_Destruct, ATI_[0..N]			300	uA
I_{IH} Rx_Port (Rx_Port input at Vdd = 3.6 V)			200	uA
I_{IH} (Input High Current. Inputs tied to Vdd = 5.5 V) Write_Protect_N, ZPM, Auth, Erase_Trigger, Self_Destruct, ATI_[0..N]			600	uA
I_{IL} (Input low Current. Inputs tied 0.0 V) Write_Protect_N, ZPM, Auth, Rx_Port, Erase_Trigger, Self-Destruct, ATI_0			200	uA
Idd. Inactive with no SATA commands, Vdd = 3.3 V MSM37 MSM75		 0.175 0.190	 0.195 0.210	A
Idd. 100 % Writes (128 KiB Seq. block), Vdd = 3.3 V MSM37 MSM75		 0.250 0.275	 0.275 0.305	A
Idd. 100 % Reads (128 KiB Seq. block), Vdd = 3.3 V MSM37 MSM75		 0.210 0.235	 0.235 0.260	A
Idd. Inactive with no SATA commands, Vdd = 5.0 V MSM37 MSM75		 0.125 0.135	 0.140 0.150	A
Idd. 100 % Writes (128 KiB Seq. block), Vdd = 5.0 V MSM37 MSM75		 0.175 0.195	 0.195 0.220	A
Idd. 100 % Reads (128 KiB Seq. block), Vdd = 5.0 V MSM37 MSM75		 0.150 0.165	 0.165 0.185	A
Idd during standby and sleep (MSM37 and MSM75, 3.3 V and 5.0 V)		0.11		A
Idd. Destruct operation (20 mS) Vdd = 3.3 V and 5.0 V (from inactive)		0.250		A
Idd. ZPM, deep slumber mode (ZPM = Vdd = 3.3 V) Other inputs at 0V		8	10	ma
Required external backup power capacitance	2500			uF

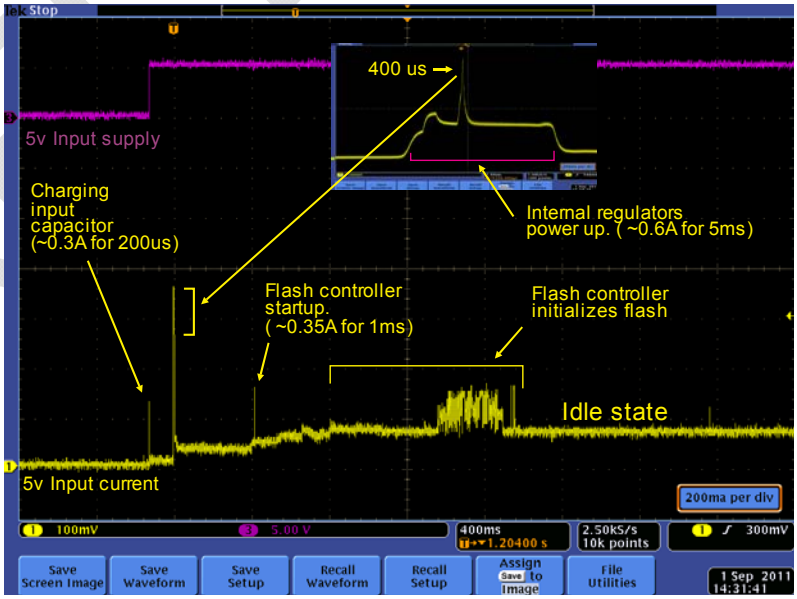


Figure 2: Power-On Inrush Current Plot

Thermal Performance

The MSM37/MSM75 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 MSM37/MSM75. The thermal images in Figure 3a and Figure 3b show the temperature profiles of the MSM37 and MSM75 on the customer evaluation PCB at room temperature.

Insert thermal camera image of eval board here.

Figure 3a MSM37 Thermal Image. **Figure 3b: MSM75 Thermal image.**

Table 3: Module Pin list

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,	Vss	Power	Ground pins.

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, 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.
U17	ZPM	In	ZPM (Zero Power Mode) enables a low power standby mode. During normal operation, this pin must be at a low level. Driving the ZPM pin to a high level causes the MSM37/MSM75 to enter an ultra low power deep slumber mode. Lowest power operation is obtained with Vdd at 3.3 V.

E17	Auth	In/out	Hardware authentication.
V17	Rx_Port	In	Optional 9600 Baud 232 port. Port receive input.
D17	Erase_Trigger	In	Erase and sanitize trigger pin. (Active during ZPM) 0 = Normal operation, 1 = Trigger erase or sanitize operation after a 20 ms debounce. Driving this pin high for 20 ms or longer causes the MSM37/MSM75 to begin an erase or sanitize operation. If this pin is high at power on time, no operation will trigger. To trigger an erase or sanitize 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.
U10	Self_Destruct	In	Module self-destruct. (Active during ZPM mode) 0 = Normal operation, 1 = Self-destruct after 20 ms debounce. 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. **Warning:** The destruct operation produces no heat, sparks, or form factor changes. The process is not reversible. 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	ATI_[0..74]	In	AT Integrity inputs See the description in the AT Integrity section.
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	ATO_[0..73]	Out	AT Integrity. See the description in the AT Integrity section.
T10	AT_Out	Out	AT result status. 0 = No failure. 1 = AT Integrity failure detected.
T12, T14	Back-up_Charger	Out	External backup capacitor array charging signal. Connect these pins to the Backup_Pwr pins. Backup-Charger is a boosted 5 V regulated output for charging a small array of external capacitors connected to the Backup_Pwr pins. The output has 300 ohms in series to limit the charge current. When supplying the Backup_Pwr from an external supply, do not connect these pins.

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 MSM37/MSM75 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.
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 9600 Baud RS-232 port. Port Transmit output.
W16	Status_2	Out	Most significant bit of the module status. Refer to Table 4 for error codes. This signal is invalid when Module_Active is low.
V16	Status_1	Out	Middle bit of the module status. Refer to Table 4 for error codes. This signal is invalid when Module_Active is low.
U16	Status_0	Out	Least significant bit of the module status. Refer to Table 4 for error codes. This signal is invalid when Module_Active is low.
D9	Module_Active	Out	Indicates the module master status. 1 = The module is active and the Status_0, Status_1, and Status_2 signals are valid. 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 internal supply potentially requires additional external capacitance. 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, L25	NC	DNC	**Reserved for future use or factory test. Leave these pins floating. Do not connect.**

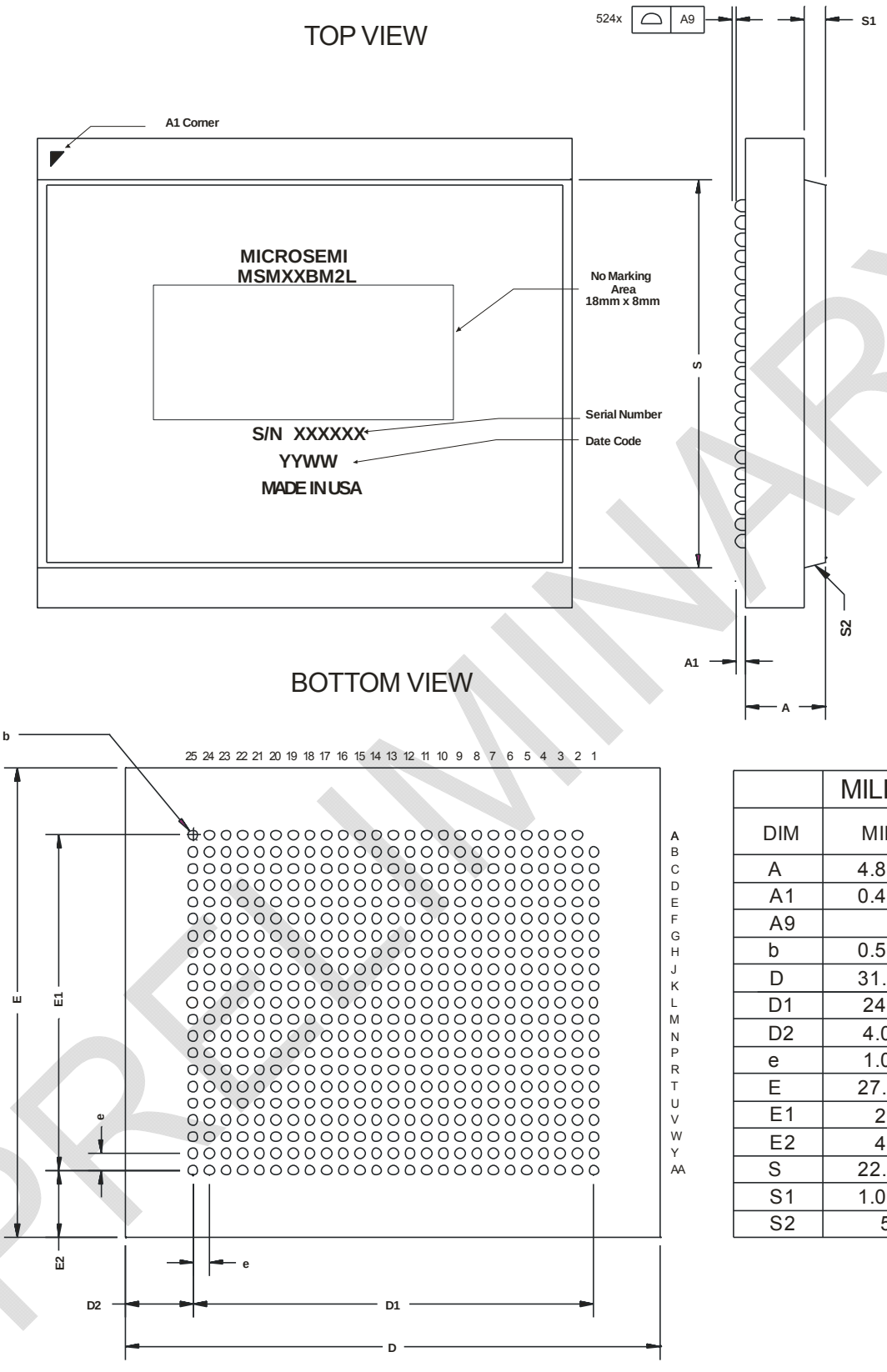
Table 4: Status error codes

Module_Active	Status_2	Status_1	Status_0	Error code description
0	x	x	x	Module unpowered or Vdd is below minimum level.
1	0	0	0	Normal operation.
1	0	0	1	AT Integrity, Authentication, or Temperature-rate-of-change failure.
1	0	1	0	Module is waiting for one or more voltages or the temperature to be-come valid.
1	0	1	1	The module is pass-phrase locked and is awaiting a valid pass-phrase from the host. In this mode, the MSM37/MSM75 ignores all RS-232 commands except the pass-phrase command.
1	1	0	0	Module is waiting for the backup power supply voltage on the Backup_Supply pins to reach a valid level.
1	1	0	1	Self Destruct operation completed. Module is inoperable.[1]
1	1	1	0	Backup power failed during previous power-down cycle. Check external backup power supply.
1	1	1	1	Other failure. Connect 232 port for additional error details.

[1] This state is persistent across power cycles.

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	TBD	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
S1	1.05	1.65
S2	5°	25°

Figure 4: MSM37/MSM75 Module Dimensions

Table 6: System Specifications and Characteristics

Feature	Characteristic
Security and AT features	AES-128 encryption in CTR mode, AES key purge feature, Hardware authentication, AT Integrity, Temperature-rate-of-change, SHA-256 pass-phrase, and Self-Destruct.
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 from external trigger input	Yes. TBD sec (MSM37) TBD sec (MSM75)
Sanitization protocols (MSM37)	NSA 9-12 TBD sec NSA/CSS 130-2 TBD sec Navy NAVSO P-5239-26 TBD sec NISPOM DoD 5220.22-M TBD sec Air Force AFSSI-5020 TBD sec Army AR380-19 TBD sec
Sanitization protocols (MSM75)	NSA 9-12 TBD sec NSA/CSS 130-2 TBD sec Navy NAVSO P-5239-26 TBD sec NISPOM DoD 5220.22-M TBD sec Air Force AFSSI-5020 TBD sec Army AR380-19 TBD sec
Auto Restart of erase/sanitize after power loss	Yes
Internal flash capacity – (MSM75)	96 GiB (1 GiB = 1,073,741,824 bytes)
Internal flash capacity – (MSM37)	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
Factory tracking of flash media by device	Yes. Using a unique string. “ONRHFFFNFPUZVQG”
Sector size	512 bytes
Total LBAs available – (MSM75)	146,533,968
Total LBAs available – (MSM37)	73,277,568
Power to ready time	Less than 2 seconds
Operating system compatibility	OS independent
Support for Trim command	Yes
NCQ 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 PB (MSM75) 1PB (MSM37) 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	Type S1565
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 6: System Specifications and Characteristics (Continued)

Input supply sudden short protection	Yes
Power-on inrush current limiting	Yes, See Figure 2
Life remaing 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

MSM37 Read and Write Performance Benchmarks (Actual performance will vary based on data)

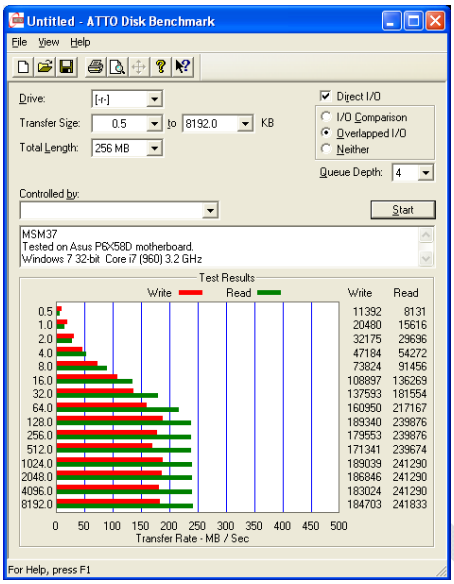


Figure 5a: ATTO

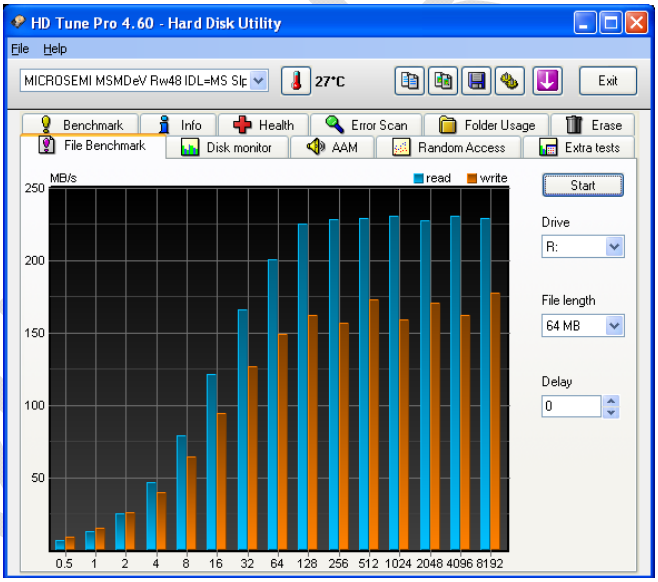


Figure 5b: HD Tune Pro 4.6 file benchmark

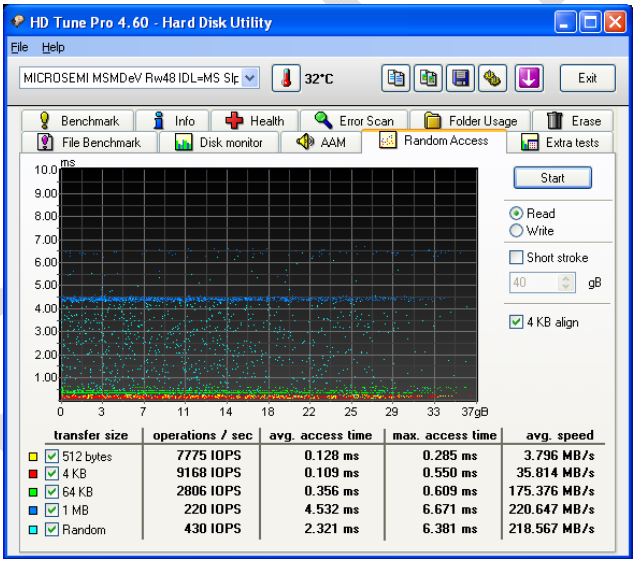


Figure 5c: HD Tune 4.6 Random Read

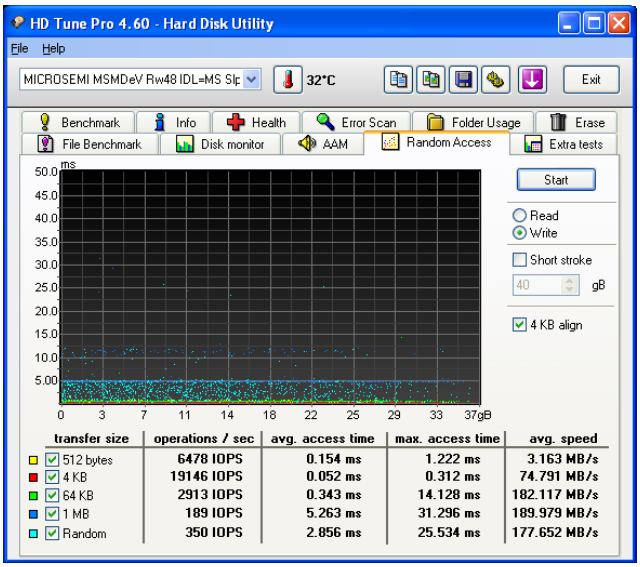


Figure 5d: HD Tune Pro 4.6 Random Write

Iometer results (version 2006.07.27) for the MSM37

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 MSM75

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

MSM37/MSM75 Description

The MSM37/MSM75 is a complete SATA based system-in-a-module developed by Microsemi Corporation to address the need for secure storage in a compact BGA form factor.

The MSM37/MSM75 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, AES 128 encryption, SHA-256 crypto logic, AT logic, temperature-rate-of-change monitoring, and self-destruct circuitry.

With the application of power, a voltage supervisor in the MSM37/MSM75 module begins monitoring the Vdd voltage level. Once Vdd reaches approximately 3.2 V, the voltage supervisor sets the Module_Active signal to a high level and begins monitoring the backup power supply voltage, Backup_Pwr.

Internally, a voltage booster boosts 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. 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 MSM37/MSM75 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 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 flash processor to shut down. After the flash processor completes the shut down operation, 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 MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 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 note that the retention capabilities of the NAND flash diminish with use as the device approaches the natural write endurance limit. The flash in the MSM37/MSM75 has an initial retention capability of about 10 years. The retention capability at end of life may be less than 30 days. Using a SMART command, the host system can monitor a “Life remaining” attribute to determine if the MSM37/MSM75 is approaching end-of-life.

Low Power Modes

The Serial ATA specification defines two power saving modes, *partial* and *slumber*. The MSM37/MSM75 implements both power management modes and well as a proprietary Deep Slumber mode. Pulling the ZPM pin to a high level allows the MSM37/MSM75 mode to enter a very low power Deep Slumber mode. The MSM37/MSM75 treats the ZPM mode in the same way as it treats a hot swap or power down event. The MSM37/MSM75 completes the command currently in progress and then proceeds to an orderly shutdown. During the ZPM mode, the MSM37/MSM75 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

The MSM37/MSM75 has built in circuitry 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 significant heat and the form factor of the module remains unchanged during and after the destruct operation. The destruct method inflicts damage to one or more components within the module, is permanent across power cycles, and is not reversible. Data in the flash devices 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.

Additionally, the MSM37/MSM75 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.

The MSM37/MSM75 contains a programmable feature to perform an automatic self-destruct operation, after multiple authentication failures, AT Integrity failures, and Temperature-rate-of-change events. These features are programmable by Microsemi at production time or in the field using commands from the RS-232 port.

AT Integrity

The MSM37/MSM75 contains a feature called AT Integrity. The AT Integrity feature utilizes unused BGA balls with internal and possible external logic to enable the module to detect changes in the environment around the MSM37/MSM75. Such changes might indicate that a tamper event is in progress or that the module sustained physical damage and could potentially lose power and/or connectivity. The AT_Out signal indicates the status of the AT Integrity logic. A low level at the AT_Out pin indicates that the module is operating normally. A high level on the AT_Out pin indicates that the AT Integrity logic detected an external environmental change, damage, or tamper event. In response to an AT Integrity event, the module writes an error code to the status signals Status_0, Status_1, and Status_2, completes any command in progress, and then proceeds to an orderly shutdown in a low power mode similar to ZPM. The module remains in the low power standby mode until a new power-up cycle occurs in which the AT_Out signal is low. A host system can monitor possible AT Integrity events by evaluating the status signals Status_0, Status_1, and Status_2 or connecting to the integrated RS-232 port and issuing a status command.

The MSM37/MSM75 supports triggering of an automatic self-destruct after an AT Integrity event using a setup procedure from the RS-232 port or by ordering the part number with the feature enabled. While using the RS-232 port to enable automatic self-destruction after an AT Integrity event is the most secure approach, applications that do not support an RS-232 port can still utilize the self-destruct feature by externally connecting the AT_Out pin to the Self-Destruct input pin. Similarly, connecting the AT_Out pin to the Erase_Trigger pin causes the MSM37/MSM75 to perform a whole module erase operation after an AT Integrity event.

To prevent accidental self-destruct operations on newly manufactured units, AT Integrity will not trigger a self-destruct operation until one power-on cycle completes with no pending AT Integrity event. Once the first power-on cycle completes and no AT Integrity event is pending, the self-destruct circuitry immediately enables.

The diagram in Figure 6 shows the connections necessary to implement the most basic form of the AT Integrity feature. As implemented in figure 6, AT Integrity can detect BGA balls that have broken lose, or an attempt to operate the module in an environment that does not include proper AT Integrity connections. Microsemi can implement custom versions of AT Integrity that contain sophisticated features, sensors, and waveform analysis based on customer requirements.

If the end application includes other protection sensors, external to the MSM37/MSM75, combining several sensor outputs with the AT_Out signal can allow multiple events to trigger an automatic self-destruct operation. Figure 6 shows an example of the MSM37/MSM75 with a normally closed external sensor that opens when triggered. The open state of the sensor allows an external pull-up resistor to initiate an automatic self-destruct operation.

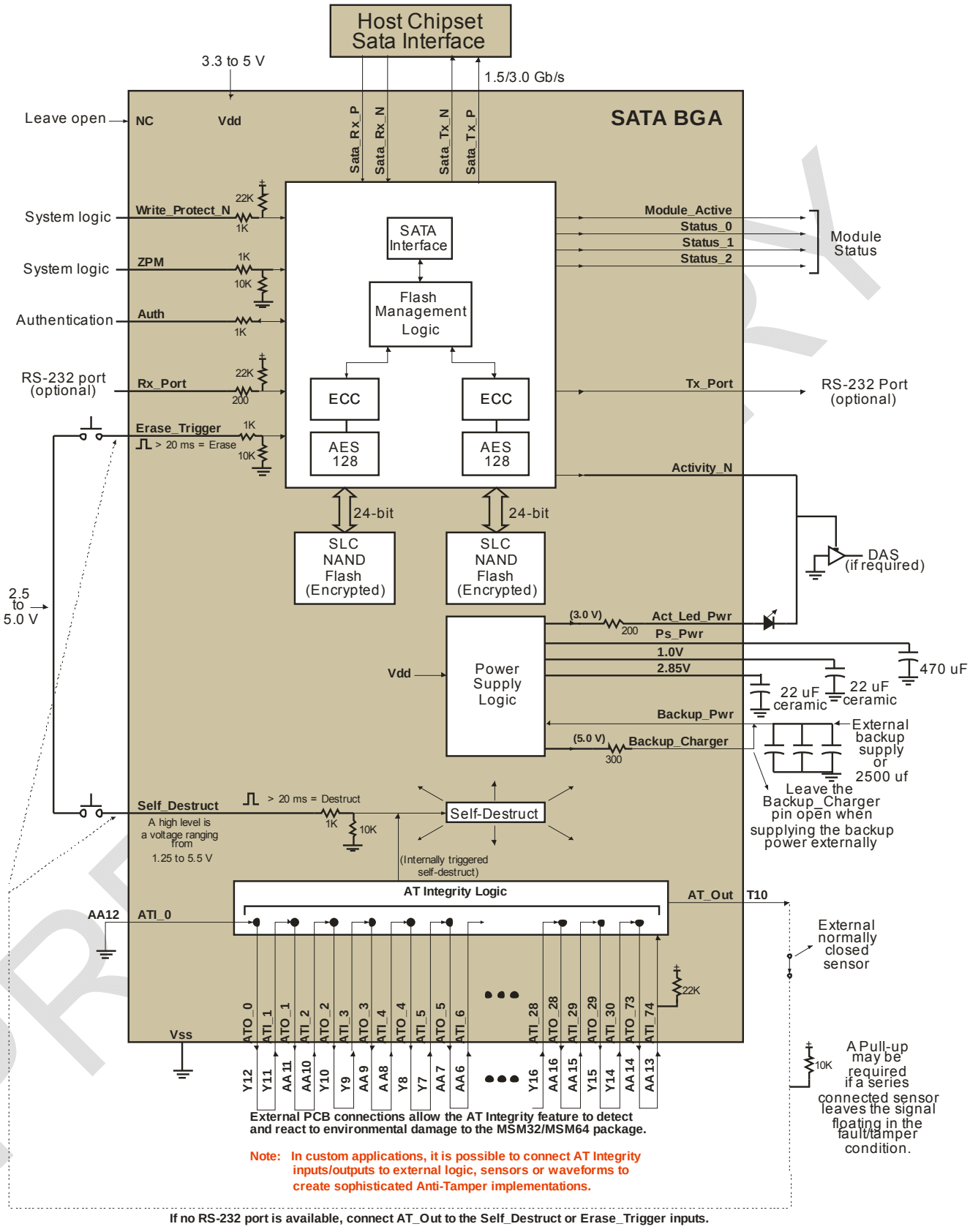


Figure 6: Basic AT Integrity connections. Out-of-environment and physical damage detection.

Table 7 contains a list of connections that are necessary to implement the basic AT Integrity implementation as shown in figure 6.

Table 7: Connections required for implementing the basic form of AT Integrity feature.

Module Pins	Comment	
AA12	Connect to system ground.	(ATI_0)
Y12, Y11	Connect together.	(ATO_0, ATI_1)
AA11, AA10	Connect together.	(ATO_1, ATI_2)
Y10,Y9	Connect together.	(ATO_2, ATI_3)
AA9, AA8	Connect together.	(ATO_3, ATI_4)
Y8, Y7	Connect together.	(ATO_4, ATI_5)
AA7, AA6	Connect together.	(ATO_5, ATI_6)
Y6, Y5	Connect together.	(ATO_6, ATI_7)
AA5, AA4	Connect together.	(ATO_7, ATI_8)
Y4, Y3	Connect together.	(ATO_8, ATI_9)
W3, W2	Connect together.	(ATO_9, ATI_10)
V1, V2	Connect together.	(ATO_10, ATI_11)
V3, U2	Connect together.	(ATO_11, ATI_12)
U1, T1	Connect together.	(ATO_12, ATI_13)
T2, R2	Connect together.	(ATO_13, ATI_14)
R1, P1	Connect together.	(ATO_14, ATI_15)
P2, N2	Connect together.	(ATO_15, ATI_16)
N1, M1	Connect together.	(ATO_16, ATI_17)
M2, L2	Connect together.	(ATO_17, ATI_18)
K1, K2	Connect together.	(ATO_18, ATI_19)
J2, J1	Connect together.	(ATO_19, ATI_20)
H1, H2	Connect together.	(ATO_20, ATI_21)
G2, G1	Connect together.	(ATO_21, ATI_22)
F1, F2	Connect together.	(ATO_22, ATI_23)
E2, E1	Connect together.	(ATO_23, ATI_24)
D1,D2	Connect together.	(ATO_24, ATI_25)
D3, C2	Connect together.	(ATO_25, ATI_26)
C3, B3	Connect together.	(ATO_26, ATI_27)
B4,A4	Connect together.	(ATO_27, ATI_28)
A5, B5	Connect together.	(ATO_28, ATI_29)
B6, A6	Connect together.	(ATO_29, ATI_30)
A7, B7	Connect together.	(ATO_30, ATI_31)
B8, A8	Connect together.	(ATO_31, ATI_32)
A9, B9	Connect together.	(ATO_32, ATI_33)
B10, A10	Connect together.	(ATO_33, ATI_34)
A11, B11	Connect together.	(ATO_34, ATI_35)
B12, A12	Connect together.	(ATO_35, ATI_36)
A13, B13	Connect together.	(ATO_36, ATI_37)
B14, A14	Connect together.	(ATO_37, ATI_38)
A15, B15	Connect together.	(ATO_38, ATI_39)

B16, A16	Connect together.	(ATO_39, ATI_40)
A17, B17	Connect together.	(ATO_40, ATI_41)
B18, A18	Connect together.	(ATO_41, ATI_42)
A19, B19	Connect together.	(ATO_42, ATI_43)
B20, A20	Connect together.	(ATO_43, ATI_44)
A21, B21	Connect together.	(ATO_44, ATI_45)
B22, A22	Connect together.	(ATO_45, ATI_46)
B23, C23	Connect together.	(ATO_46, ATI_47)
C24, D23	Connect together.	(ATO_47, ATI_48)
D24, D25	Connect together.	(ATO_48, ATI_49)
E25, E24	Connect together.	(ATO_49, ATI_50)
F24, F25	Connect together.	(ATO_50, ATI_51)
G25, G24	Connect together.	(ATO_51, ATI_52)
H24, H25	Connect together.	(ATO_52, ATI_53)
J25, J24	Connect together.	(ATO_53, ATI_54)
K24, K25	Connect together.	(ATO_54, ATI_55)
L24, M24	Connect together.	(ATO_55, ATI_56)
M25, N25	Connect together.	(ATO_56, ATI_57)
N24, P24	Connect together.	(ATO_57, ATI_58)
P25, R25	Connect together.	(ATO_58, ATI_59)
R24, T24	Connect together.	(ATO_59, ATI_60)
T25, U25	Connect together.	(ATO_60, ATI_61)
U24, V23	Connect together.	(ATO_61, ATI_62)
V24, V25	Connect together.	(ATO_62, ATI_63)
W24, W23	Connect together.	(ATO_63, ATI_64)
Y23, Y22	Connect together.	(ATO_64, ATI_65)
AA22, AA21	Connect together.	(ATO_65, ATI_66)
Y21, Y20	Connect together.	(ATO_66, ATI_67)
AA20, AA19	Connect together.	(ATO_67, ATI_68)
Y19, Y18	Connect together.	(ATO_68, ATI_69)
AA18, AA17	Connect together.	(ATO_69, ATI_70)
Y17, Y16	Connect together.	(ATO_70, ATI_71)
AA16, AA15	Connect together.	(ATO_71, ATI_72)
Y15, Y14	Connect together.	(ATO_72, ATI_73)
AA14, AA13	Connect together.	(ATO_73, ATI_74)

Encryption and AES Key Purge

The MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 contains hardware authentication logic that is capable of preventing the module from operating in unauthorized environments. The module implements authentication by evaluating and monitoring circuitry surrounding the module. Removing the module from an authorized environment causes the module to cease further operations and shutdown to a low power mode similar to ZPM. Detection of attempted operation in an unauthorized environment can result in the MSM37/MSM75 initiating an erase and/or self-destruct operation. The action taken by the MSM37/MSM75 module is often application dependent. Use the RS-232 interface to enable the hardware authentication mode. Hardware authentication may require additional external logic.

SHA-256 Pass-Phrase

The MSM37/MSM75 has the ability to inhibit normal operation; including ignoring all RS-232 commands except the PO command until the host system supplies a valid pass-phrase. The MSM37/MSM75 uses SHA-256 crypto logic to hash an initial pass-phrase sent by a host system. Internal logic saves the 256-bit hashed version of the host pass-phrase in memory. After saving the hashed version of the pass-phase, the memory locations containing the original plain text pass-phrase are over-written. The plain text pass-phrase is resident in memory only until hashing completes. When the host system needs access to the MSM37/MSM75, it must send a pass-phrase for validation. SHA-256 crypto logic hashes the “sent” pass-phrase and compares it to the previously stored (hashed) pass-phrase. If the two pass-phrases match, the MSM37/MSM75 begins operating normally. If the pass-phrases do not match, the MSM37/MSM75 delays 30 seconds, then begins monitoring for a new pass-phrase. The MSM37/MSM75 ships with the pass-phrase feature disabled. To enter a new pass-phrase, use the PE command from the RS-232 interface. To enable the pass-phrase mode using a previously entered pass-phrase, use the PE command with no pass-phrase. To disable a pass-phrase mode in a module that currently has the mode enabled, use the PO command. It is not possible to disable an active pass-phrase 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 using the external Erase_Trigger pin. Refer to Table 8 for a description of the pass-phrase commands. Microsemi can customize the operation of the pass-phrase feature to meet the requirements of customer applications. Contact Microsemi for details.

Erase and Sanitize Operations

Both the whole module flash erase and standard military sanitization options are available. The pre-programmed sanitize protocols comply with military and government specifications including NISPOM DoD 5220.22-M, NSA 9-12, Air Force AFSSI-5020, Army AR380-19, and Navy NAVSO P-5239-26.

The MSM37/MSM75 supports three triggering methods: An external switch or signal attached to the Erase_Trigger input, the Sanitize Device Set, and the ATA security feature set. The ATA Security Feature Set uses the Security Erase Unit, Enhanced Security Erase, and Security Erase Prepare commands. The Sanitize Device Set uses Crypto Scramble Ext, Block Erase Ext, and Overwrite Ext commands. The MSM37/MSM75 Security erase guide has programming details.

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 MSM37/MSM75 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 MSM37/MSM75 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 refresh" removes the opportunity for the bit-disturb errors to build up to the 16-symbol correction limit of the MSM37/MSM75 flash processor.

CRC (Cyclic Redundancy Check) and Silent Data Corruption

The Microsemi MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 utilizes a small array of external capacitors and "on-chip" proprietary power management circuitry. When the MSM37/MSM75 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 MSM37/MSM75 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 MSM37/MSM75 design team works in labs at the trusted facility in Phoenix Arizona. This is the same facility which manufacturers, assembles, and tests the M50/M100 secure storage device.

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 MSM37/MSM75 module. The port will respond with a ">" prompt when it receives a hex "D" character. Commands are not case sensitive and are listed in Table 8. All commands should include a trailing hex "D" character. The RS-232 port setup requires a 19,200 baud rate with 8 data bits, one stop bit, and no parity.

Table 8: RS-232 port commands

Command	Function
ST	Display the status of the module. - Display the levels of all inputs and outputs. - Display measured results of all internal voltages. - Display the current temperature. - Display the serial number of the unit. - Display details about any error conditions. - Display the module revision number. - Display the status of all operating and destruct modes.
ET(last 4 digits of serial number)	Generate an erase trigger event.
MD(last 4 digits of serial number)	Perform a module self-destruct operation.[1]
AE(last 4 digits of serial number)	Test the host system and enable hardware authentication. Begin the authentication process and enable hardware authentication. This process is non-reversible. Once authentication successfully activates it cannot be de-activated.
AD(last 4 digits of serial number)**N**	Enable automatic self-destruct if hardware authentication fails "**N**" times during a single power cycle.[1] **N** = 1-15.
ID(last 4 digits of serial number)	Enable automatic self-destruct if an AT Integrity failure occurs. The MSM37/MSM75 comes with this feature enabled at production time if a specific part number is ordered. Refer to the ordering information page.[1]
TD(last 4 digits of serial number)**N**	Enable automatic self-destruct if the temperature-rate-of-change exceeds more than **N** degrees in any 1-second interval. N = 1-15. Selecting 15 will enables a self-destruct operation for any temperature change of 15 or more degrees in a 1-second interval.[1]
PE(64 hex nibbles)	Use this command to enter a new 256-bit pass-phrase then enable the pass-phrase mode. The mode is active across power cycles until disabled using the PO (Pass-Phrase Off) command. The pass-phrase mode cannot cause a self-destruct operation; it only delays the start of normal operation. Note: The module ignores this command if the pass-phrase mode is already active. Use the PO command to disable the active pass-phrase mode, and then use the PE command to enter a new pass-phrase.
PE	Enable the pass-phrase mode using a previously stored pass-phrase.
PO(64 hex nibbles)	Turn Off the pass-phrase mode. Devices ship from Microsemi with the pass-phrase mode disabled. Note: The module ignores this command if the pass-phrase mode is already disabled. The only way to recover from a lost pass-phrase is to execute a whole module erase or sanitize operation using the external trigger input.
CL(last 4 digits of serial number)	Cancel all automatic self-destruct modes.

Note 1: Only devices containing self-destruct circuitry can self-destruct. Refer part number guide.

MSM37/MSM75 Part Numbering Guide

M	SM	XX	B	M	2	L	–	ES	0000	I
1	2	3	4	5	6	7	–	8	9	10

Field 1: Manufacturer
M = Microsemi Corp

Field 2: Form Factor
SM = 32 mm x 28 mm BGA. 524 pins.

Field 3: NAND Capacity to Host
37 = 37.5 GB (48 GiB internal)
75 = 75.0 GB (96 GiB internal)

Field 4: Encryption
B = AES-128 Encryption

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 : Classification
ES = Engineering Sample. (Preliminary performance values)
Blank = Fully Qualified product

Field 9: Customizable Features
0000 = No Self-Destruct circuitry.
D100 = Includes Self-Destruct circuitry and AT Integrity circuitry. Feature ships in the disabled (no destruct) state. Use an RS-232 command to enable the self-destruct feature or use external pin connections to connect AT_Out to the Self-Destruct or Erase_Trigger inputs.
D200 = Includes Self-Destruct circuitry and temperature-rate-of-change circuitry. The MSM37/MSM75 will perform an automatic self-destruct operation when a temperature-rate-of-change event occurs that exceeds 10 degrees in any one-second period and power is applied.
D300 = Includes D100 and D200 features.
D700 = Includes D100, D200 but ships with the AT Integrity feature in the enabled state. Unit will perform an automatic self-destruct operation on the first AT Integrity failure.
SP00 = Customer defined security features.

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

Update Log

Revision: Date	Description
Revision 00.17 : 6/21/2011	Added DC blocking capacitors to diagrams.
Revision 00.21 : 7/13/2011	Added Update log page to released data sheet.
Revision 00.22 : 7/13/2011	Added early power estimates from lab tests at 5v.
Revision 00.23 : 7/13/2011	Changed all instances of “idle” to inactive.
Revision 00.24 : 7/14/2011	Idd values at 5 V units were mA. Changed to mW. There were two Idd Destruct at 3.3 V. Changed the second instance to 5.0 V.
Revision 00.25 : 7/21/2011	Added 22 uF and 470 uF power supply capacitors to application drawings Added L1 and L25 balls to BGA pattern and pin tables (NC pins) Fixed missing underscore in signal names on page 4. Required external backup power capacitance changed from 3500 uF to 2500 uF
Revision 00.26 : 7/26/2011	Changed pin count from 522 to 524 on pages 2, 11, 12, and 24. Storage temperature on page 4 changed from -50 °C to -55 °C Upgraded UBER specification from 10^{-16} to 10^{-17} on pages 2, 13, 21.
Revision 00.27 : 8/01/2011	Page 5. Added typical and max supply currents for 3.3v. Page 5. Added a comment to the self-destruct supply current specification that indicates that the supply current is measured from an inactive state. Changed instances of 64 GB and 32 GB on page 13 to MSM64 and MSM32 to avoid confusion.
Revision 00.28 : 8/09/2011	Page 11. Changed wording for no-connects to read **“Reserved for future use or factory test. Leave these pins floating. Do not connect.”** Page 10: After lab testing we determined we could eliminate some voltages and wanted to simplify signal names. 2.85V pins are now NC pins. 1.0V_Vx pins are now NC pins. 2.85V_Stby pins are now called 2.85V. Still needs 22uf externally. 1.0V_Stby pins are now called 1.0V pins. Still needs 22uf externally. Block Diagrams: Updated to changed 2.85V_Stby, 1.0V_Stby to 2.85V and 1.0V.
Revision 00.29 : 9/14/2011	Global change of MSM32 and MSM64 to MSM37 and MSM75 Added details about the RS-232 connection protocol requirements on page 24. Added placeholder for thermal conduction to case and PCB. Page 11. Changed RS-322 to RS-232 on page 25. Added Idd and ZPM mode current using 25 nm flash device data. Page 5. Added power inrush plot. Page 5. Updated ordering information to include a commercial device variation. Page 25. Added performance plots. Page 14. Inserted a new page for MSM75 performance. New page is page 15. Removed comment about physical destruct on page 18. Added LBA counts to table on page 13. Added Estimates for θ_{JC} anf θ_{JB} on page 11.