Preliminary Information

MPC1848xxHWRM/D
Rev. 2, 2/2003

MPC184 8xx Mode Hardware Reference Manual

Matthew Short

Security Applications

matt.short@motorola.com

This document describes how to design a system with the MPC184 in an 8xx PowerQUICC environment. It covers the following topics:

1 Overview

The MPC184 is a flexible and powerful addition to any networking or computing system using the Motorola PowerQUICC line of integrated communications processors, or any system supporting the PCI bus protocol. The MPC184 is designed to off load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from the host processor. The MPC184 is optimized to process all the algorithms associated with IPSec, IKE, WTLS/WAP and SSL/TLS. In addition, the Motorola family of security co-processors are the only devices on the market capable of executing elliptic curve cryptography which is especially important for secure wireless communications.

MPC184 features include the following:

- 1 Public key execution units (PKEUs) that support the following:
  - RSA and Diffie-Hellman
    - Programmable field size up to 2048-bits
  - Elliptic curve cryptography
    - F_2m and F(p) modes
    - Programmable field size up to 511-bits
- 1 Data Encryption Standard execution units (DEUs)
  - DES, 3DES
  - Two key (K1, K2, K1) or Three Key (K1, K2, K3)
  - ECB and CBC modes for both DES and 3DES
- 1 Advanced Encryption Standard unit (AESU)
  - Implements the Rinjdael symmetric key cipher
  - Implements ECB, CBC and Counter modes
- 1 ARC Four execution unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
- 1 Message digest execution units (MDEUs)
  - SHA-1 with 160-bit or 256-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- 1 Random number generator (RNG)
- 8xx compliant external bus interface, with master/slave logic.
  - 32-bit address/32 -bit data
  - 75 MHz operation
- PCI 2.2 compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data mode, 66MHz
- 4 Crypto-channels, each supporting multi-command descriptor chains
  - Static and/or dynamic assignment of crypto-execution units via an integrated controller
  - Buffer size of 2KBytes for each execution unit, with flow control for large data sizes
- 8KB of internal scratchpad memory for key, IV and context storage
- 1.5V supply, 3.3V I/O
- 252 MAP BGA
- 1.0W power dissipation

2 System Architecture

The MPC184 is designed to integrate easily into any system using the 8xx or PCI bus protocol. The MPC184 is ideal in any system using a Motorola PowerQUICC communications processor (as shown in Figure 1) or any system with 32b PCI such as the Motorola MPC8245 integrated processor (see Figure 2). The ability of the MPC184 to be a master on the 8xx or PCI bus allows the co-processor to offload the data movement bottleneck normally associated with slave devices. The external processor accesses the MPC184 through its device drivers using system memory for data storage. The MPC184 resides in the memory map of the processor, therefore when an application requires cryptographic functions, it simply creates descriptors for the MPC184 which define the cryptographic function to be performed and the location of the data. The MPC184's mastering capability permits the host processor to set up a crypto-channel with a few short register writes, leaving the MPC184 to perform reads and writes on system memory to complete the required task.

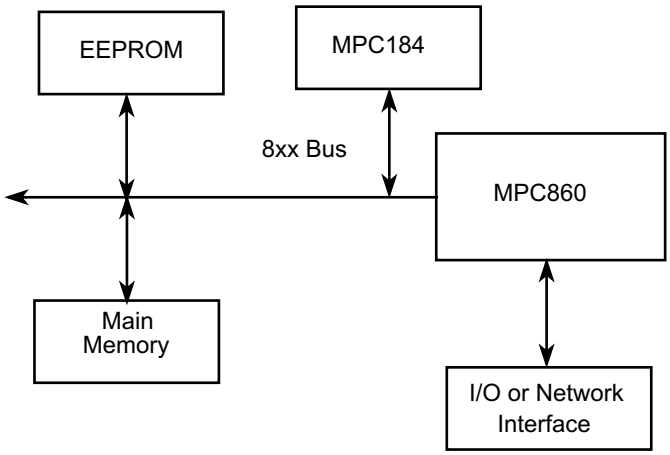


Figure 1. MPC184 Connected to PowerQUICC 8xx Bus

Figure 2 shows the MPC184 communicating with an integrated processor such as the MPC8245.

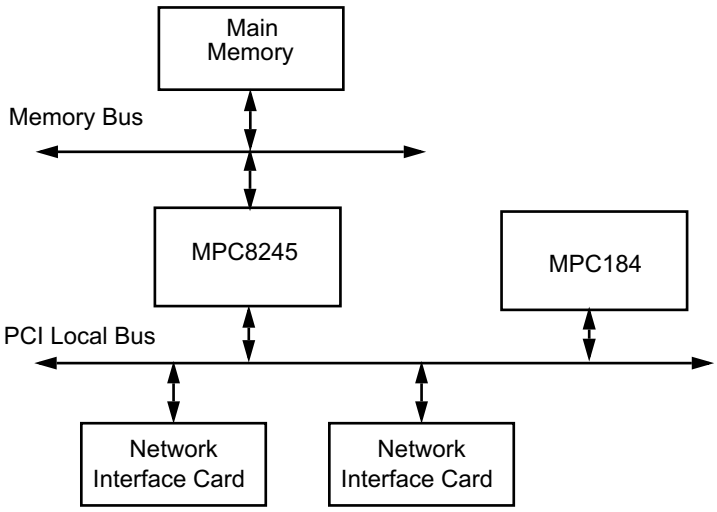


Figure 2. MPC184 Connected to an Integrated Host CPU such as the MPC8245

3 Pin Assignments

Table 1 shows the pin connections for the MPC184 in 8xx mode.

Table 1. MPC184 Pin Diagram

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
A		TMS	TCK	$\overline{\text{TRST}}$	A0	A3	A4	A7	A8	A11	A12	A15	A16	A19	A20		**A**
B	TDO	VSS	VSS	VSS	A1	A2	A5	A6	A9	A10	A13	A14	A17	A18	A21	A22	**B**
C	TDI	VSS	VSS	VSS	VSS	3.3V	VSS	3.3V	3.3V	VSS	3.3V	VSS	VSS	VSS	A24	A23	**C**
D	$\overline{\text{IRQ}}$	BASE 0	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	A25	A26	**D**
E	$\overline{\text{RESET}}$	PLL Range	3.3V	3.3V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	3.3V	VSS	A28	A27	**E**
F	BASE 1	Analog Vdd	3.3V	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	VSS	A29	A30	**F**
G	VSS	TPA /NC	VSS	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	3.3V	BASE 4	A31	**G**
H	CLK	AVSS	3.3V	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	3.3V	BASE 3	RD/$\overline{\text{WR}}$	**H**
J	VSS	VSS	3.3V	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	VSS	TSIZ 1	TSIZ 0	**J**
K	D[30]	D[31]	3.3V	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	3.3V	$\overline{\text{BURST}}$	$\overline{\text{BDIP}}$	**K**
L	D[28]	D[29]	VSS	3.3V	1.5 V	VSS	VSS	VSS	VSS	VSS	VSS	1.5 V	3.3V	3.3V	D[01]	D[00]	**L**
M	D[26]	D[27]	3.3V	3.3V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	1.5 V	3.3V	VSS	D[03]	D[02]	**M**
N	D[24]	D[25]	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	D[05]	D[04]	**N**
P	BASE 2	DP3	VSS	VSS	PLL Bypass	VSS	VSS	3.3V	VSS	3.3V	VSS	VSS	VSS	VSS	D[07]	D[06]	**P**
R	D[23]	D[22]	VSS	VSS	D[18]	D[16]	BR	$\overline{\text{RETRY}}$	$\overline{\text{BI}}$	$\overline{\text{TA}}$	$\overline{\text{TS}}$	D[15]	D[13]	D[11]	D[O8]	DP0	**R**
T		D[21]	D[20]	D[19]	D[17]	DP2	$\overline{\text{BG}}$	$\overline{\text{BB}}$	VSS	$\overline{\text{TEA}}$	DP1	D[14]	D[12]	D[10]	D[09]		**T**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	

4 Signal Descriptions

Table 2 shows the signal descriptions for the MPC184 in 8xx mode.

Note: Address multiplexing is required if the MPC184 is the only external bus master. Please see the "Address Multiplexing(AMX)" section of the Memory Controller chapter in the MPC860 user's manual for more information.

Table 2. Signal Descriptions

Signal Name	Pin Locations	Signal Type	Description
A[0–31]	A5, B5, B6, A6, A7, B7, B8, A8, A9, B9, B10, A10, A11, B11, B12, A12, A13, B13, B14, A14, A15, B15, B16, C16, C15, D15, D16, E16, E15, F15, F16, G16	I/O	Address Bus—Provides the address for the current bus cycle. A0 is the msb.
TSIZ[0-1]	J16, J15	I/O	Transfer Size 0-1—When accessing a slave in the external bus, used by the bus master to indicate the number of operand bytes waiting to be transferred in the current bus cycle.
RD/$\overline{WR}$	H16	I/O	Read/Write—Driven by a bus master to indicate the direction of the data transfer. A logic one indicates a read from a slave device and a logic zero indicates a write to a slave device.
$\overline{BURST}$	K15	I/O	Burst Transaction—Driven by the bus master to indicate that the current initiated transfer is a burst.
$\overline{BDIP}$	K16	I/O	Burst Data in Progress—When accessing a slave device in the external bus, the master on the bus asserts this signal to indicate that the data beat in front of the current one is the one requested by the master. $\overline{BDIP}$ is negated before the expected last data beat of the burst transfer.
$\overline{TS}$	R11	I/O	Transfer Start—Asserted by a bus master to indicate the start of a bus cycle that transfers data to or from a slave device. Driven by the master only when it has gained the ownership of the bus.
$\overline{TA}$	R10	I/O	Transfer Acknowledge—Indicates that the slave device addressed in the current transaction accepted data sent by the master (write) or has driven the data bus with valid data (read).
$\overline{TEA}$	T10	I/O	Transfer Error Acknowledge—Indicates that a bus error occurred in the current transaction.
$\overline{BI}$	R9	I/O	Burst Inhibit—Indicates that the slave device addressed in the current burst transaction cannot support burst transfers.
$\overline{IRQ}$	D1	O	Interrupt request - Interrupt signal that indicates that one of the modules has asserted its hardware interrupt to indicate that service is needed by the system.
D[0–31]	L16, L15, M16, M15, N16, N15, P16, P15, R15, T15, T14, R14, T13, R13, T12, R12, R6, T5, R5, T4, T3, T2, R2, R1, N1, N2, M1, M2, L1, L2, K1, K2	I/O	Data bus - In write transactions the bus master drives the valid data on this bus. In read transactions the slave drives the valid data on this bus.

Table 2. Signal Descriptions (continued)

Signal Name	Pin Locations	Signal Type	Description
DP[0-3]	R16, T11, T6, P2	I	Data Parity — Provides parity generation and checking for for transfers to a slave device initiated by the MPC860. Parity generation and checking is not supported for external masters.
$\overline{BR}$	R7	I/O	Bus Request—Asserted low when a possible master is requesting ownership of the bus.
$\overline{BG}$	T7	I/O	Bus Grant—Asserted low when the arbiter of the external bus grants the bus to a specific device.
$\overline{BB}$	T8	I/O	Bus Busy—Asserted low by a master to show that it owns the bus.
$\overline{RETRY}$	R8	I	Retry—Input used by a slave device to indicate it cannot accept the transaction.
BASE[0:4]	D2, F1, P1, H15, G15	I	Base Address Select - These 5 bits set the initial Base Address for the MPC185 and address the upper 5 bits of the 32-bit address range. After reset the Base Address may be reprogrammed anywhere in the address space via software. As an example, if BASE[0:4] = 00001, the initial Base Address for Talos is 0800_0000.
CLK	H1	I	System Clock input
$\overline{RESET}$	E1	I	Asynchronous reset signal. Initializes MPC184 to known state.
TPA / NC	G2	O	Test Pad Analog This pin MUST have No Connection
TCK	A3	I	Test Clock If JTAG is NOT used, this pin should be tied to VSS
TDI	C1	I	Test Input If JTAG is NOT used, this pin should be tied to OVDD
TDO	B1	O	Test output If JTAG is NOT used, this pin should be NC
TMS	A2	I	Test Mode Select If JTAG is NOT used, this pin should be tied to OVDD
$\overline{TRST}$	A4	I	Test Reset If JTAG is NOT used, this pin should be tied to VSS
PLL Range	E2	I	PLL Range 0 (OVSS) = 66-100 MHz PLL band 1 (OVDD) = 33-66 MHz PLL band If operating slower than 33MHz, the PLL must be disabled using the PLL Bypass pin ()
PLL Bypass	P5	I	PLL Bypass 0 (OVSS) = PLL Disabled 1 (OVDD) = PLL Enabled
AVSS	H2	I	Analog PLL Ground
Analog VDD	F2	I	Analog PLL Power (+1.5 V)

Table 2. Signal Descriptions (continued)

Signal Name	Pin Locations	Signal Type	Description
VSS	B2, B3, B4, C2, C3, C4, C5, C7, C10, C12, C13, C14, D3, E14, F6, F7, F8, F9, F10, F11, F14, G1, G3, G6, G7, G8, G9, G10, G11, H6, H7, H8, H9, H10, H11, J1, J2, J6, J7, J8, J9, J10, J11, J14, K6, K7, K8, K9, K10, K11, L3, L6, L7, L8, L9, L10, L11, M14, N3, P3, P4, P6, P7, P9, P11, P12, P13, P14, R3, R4, T9	I	Ground
IVDD	E5, E6, E7, E8, E9, E10, E11, E12, F5, F12, G5, G12, H5, H12, J5, J12, K5, K12, L5, L12, M5, M6, M7, M8, M9, M10, M11, M12	I	Core Power (+1.5 V)
OVDD	C6, C8, C9, C11, D4, D5, D6, D7, D8, D9, D10, D11, D12, D13, D14, E3, E4, E13, F3, F4, F13, G4, G13, G14, H3, H4, H13, H14, J3, J4, J13, K3, K4, K13, K14, L4, L13, L14, M3, M4, M13, N4, N5, N6, N7, N8, N9, N10, N11, N12, N13, N14, P8, P10	I	I/O Power (+3.3v)

5 Electrical and Thermal Characteristics

This chapter provides the AC and DC electrical specifications as well as the thermal characteristics of the MPC184.

5.1 Absolute Maximum Ratings

Table 3 lists ranges of absolute maximums of the MPC184.

Table 3. Absolute Maximum Ratings

Characteristic	Name	Absolute Min	Absolute Max	Unit
Power supply voltage—Core	V_{DD}	-0.5	+2.0	Volts
Power supply voltage—I/O	V_{DDQ}	-0.5	+4.1	Volts
Storage temperature	—	-55	+125	°C
Static input pin voltage	—	-0.4	+4.1	Volts

Note: V_{DDQ} must not exceed V_{DD} by more than 2.2V at any time.
Note: Permanent device damage may occur if ABSOLUTE MAXIMUM RATINGS are exceeded. Functional operation should be restricted to RECOMMENDED OPERATING CONDITIONS. Exposure to higher than recommended voltages for extended periods of time could affect device reliability.
Note: This device contains circuitry to protect the inputs against damage due to high static voltages or electric fields; however, it is advised that normal precautions be taken to avoid application of any voltage higher than maximum rated voltages to this high-impedance circuit.

5.2 Package Thermal Characteristics

Table 4 shows thermal resistances for the 252-pin MBGA package.

Table 4. Package Thermal Characteristics

Rating		Symbol	Max	Unit
Junction to ambient [1, 2](@1m/s)	Single–layer board Four–layer board	R	24 18	°C/W
Junction to board [3] (bottom)		R	12	°C/W
Junction to case [4] (top)		R	6	°C/W

1 Junction temperature is a function of on-chip power dissipation, package thermal resistance, mounting site (board) temperature, ambient temperature, air flow, board population, and board thermal resistance.

2 Per SEMI G38-87.

3 Indicates the average thermal resistance between the die and the printed circuit board via the cold-plate method, per JESD 51-8.

4 Indicates the average thermal resistance between the die and the case top surface via the cold plate method (MIL SPEC-883 Method 1012.1).

5.3 Operating Conditions and Electrical Characteristics

Table 5 shows AC and DC electrical characteristics. Unless specified otherwise, conditions are as follows:

V_{SS} = 0 V DC and T_A = 0° C to 70° C.

Table 5. DC Electrical Characteristics

Characteristic	Name	Min	Max	Units
Power supply voltage—Core	V_{DD}	1.35	1.65	V_{DC}
Power supply voltage—I/O	V_{DD}	3.0	3.6	V_{DC}
Input low voltage (Vdd = min)	V_{il}	-0.3	0.8	V_{DC}
Input high voltage (Vdd = max)	V_{ih}	2.0	V_{DDQ}+0.3	V_{DC}
AC supply current	I_{DD}	—	400	mA
Standby supply current	I_{SS}	—	150	mA
Input leakage current @ $V_{DD} \geq V_{in} \geq V_{SS}$	I_{leak}	—	±10	μA

5.4 AC Timing Characteristics

Table 6 shows the AC timing specifications for use with an PowerQUICC 2. All Timings assume a 35pF load.

Table 6. AC Electrical Characteristics

Condition	Name	Min	Max	Units
Clock frequency	F_{clock}	—	66	Mhz
Clock cycle time	t_{KHKH}	15	—	nS

Table 6. AC Electrical Characteristics

Condition	Name	Min	Max	Units
Clock-to-signal valid delay	t_{KHQV}	—	5.2	nS
Clock-to-signal hold	t_{KHQX}	2.8	—	
Input setup time to clock-bused signals	t_{DVKH}	1.7	—	nS
Input hold time clock	t_{KHDX}	2.3	—	nS

5.5 IEEE 1149.1 AC Timing Specifications

All units in Table 7 are nanoseconds.

Table 7. JTAG AC Timing Specifications

Condition	Name	Min	Max
TCK cycle time	t_{THTH}	60	—
TCK clock high time	t_{TH}	25	—
TCK clock low time	t_{TL}	25	—
TDO access time	t_{TLQV}	1	10
$\overline{\text{TRST}}$ pulse width	t_{TSRT}	40	—
Setup times Capture TDI TMS	t_{CS} t_{DVTH} t_{MVTH}	5 5 5	—
Hold timesCapture TDI TMS	t_{CH} t_{THDX} t_{THMX}	13 14 14	—

6 Case Outline Package Dimensions

Figure 3 and Figure 4 show the case outline package dimensions.

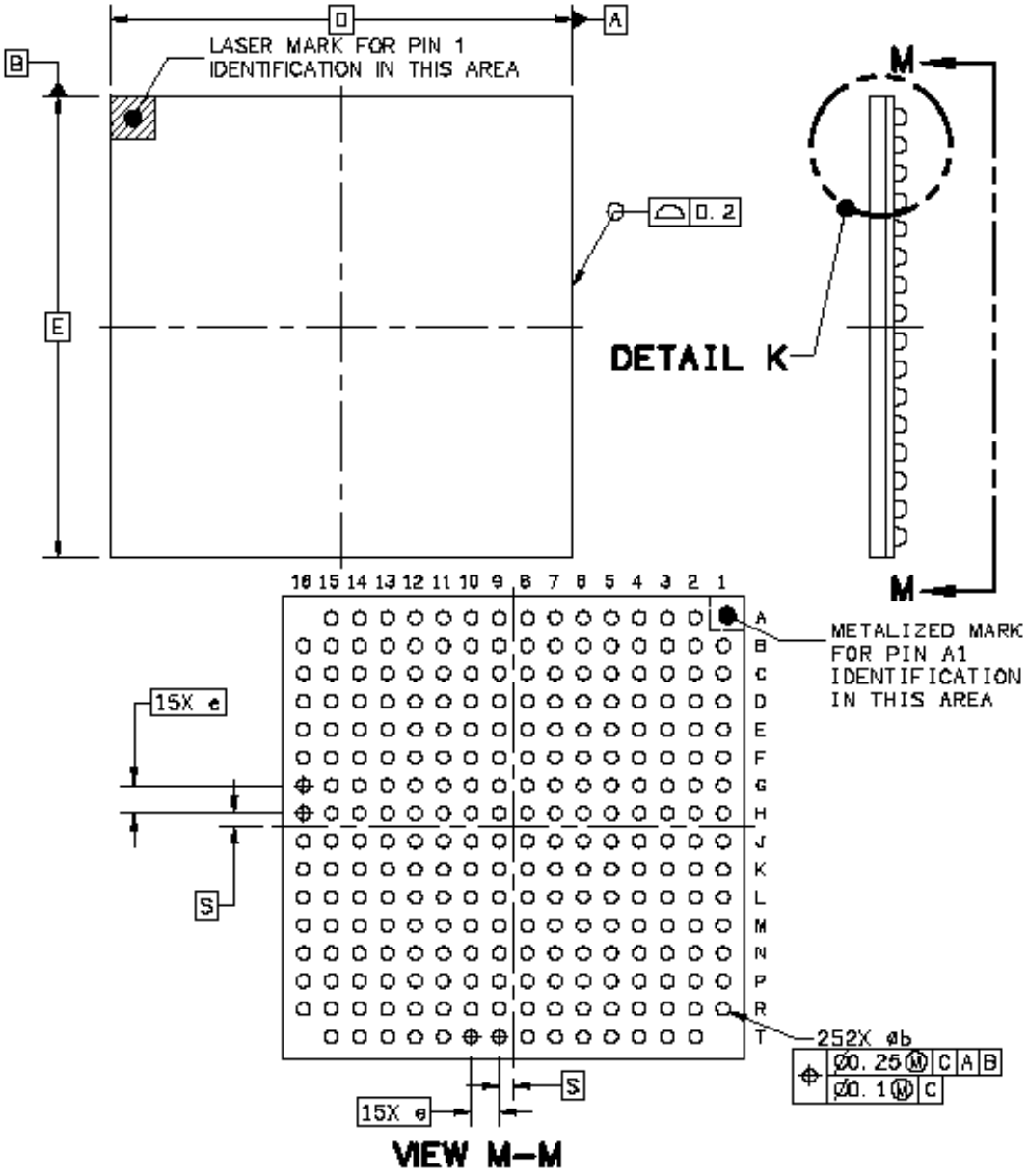
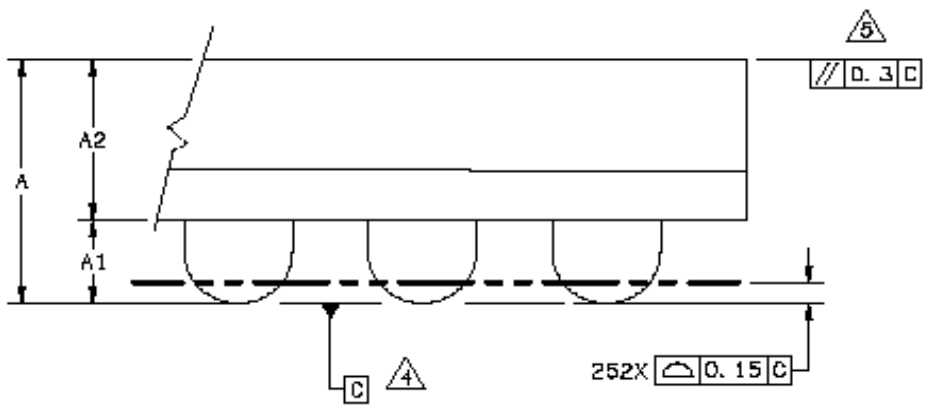


Figure 3. Case Dimensions



DETAIL K
ROTATED 90° CLOCKWISE

DIM	MIN	MAX
A	—	1.9
A1	0.5	0.7
A2	1.16 REF	
b	0.6	0.9
D	21 BSC	
E	21 BSC	
e	1.27 BSC	
S	0.635 BSC	

NOTES

1. DIMENSIONING AND TOLERANCING PER ASME Y14.5M-1994.
2. DIMENSIONS IN MILLIMETERS.
3. DIMENSION b IS THE MAXIMUM SOLDER BALL DIAMETER MEASURED PARALLEL TO DATUM C.
4. DATUM C THE SEATING PLANE, IS DETERMINED BY THE SPHERICAL CROWNS OF THE SOLDER BALLS.
5. PARALLELISM REQUIREMENT SHALL EXCLUDE ANY EFFECT OF MARKING ON TOP SURFACE.

Figure 4. Detail of Case Dimensions