Freescale Semiconductor, Inc.

Freescale Semiconductor, Inc.

Matthew Short
Security Applications
matt.short@motorola.com

This document describes how to design a system with the MPC184 in a 32bit PCI environment. It also describes how to design a system to quickly transition from the MPC190 in 32b mode to the MPC184. It covers the following topics:

freescale
semiconductor

Freescale Semiconductor, Inc.

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
- 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.
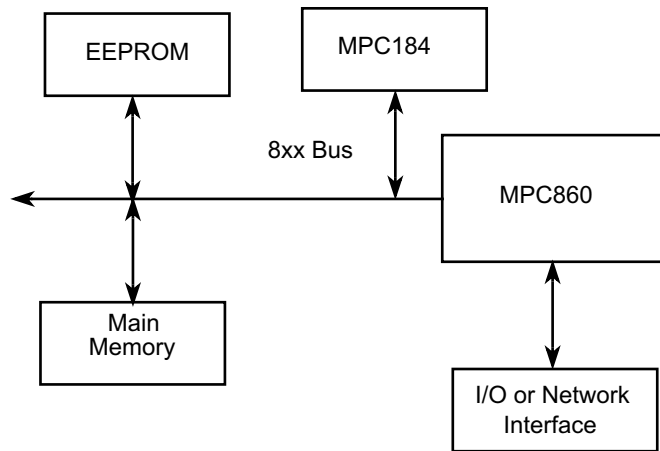

Figure 1. MPC184 Connected to PowerQuicc 8xx Bus

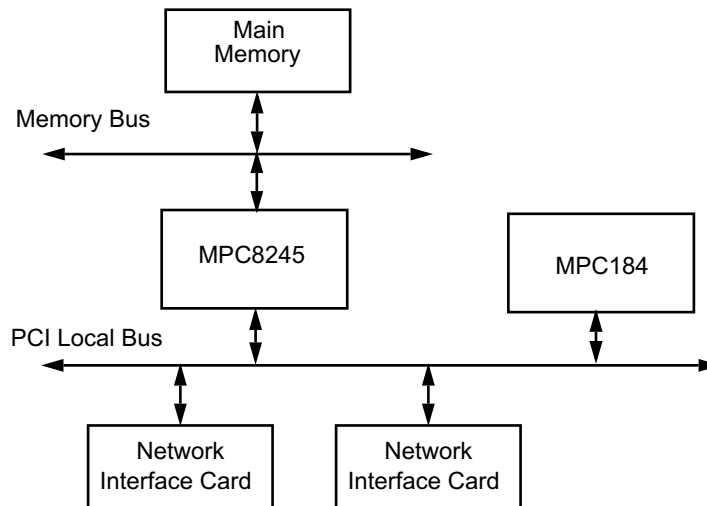Figure 2 shows the MPC184 communicating with an integrated processor such as the MPC8245.

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 32 bit PCI mode. The shaded regions show the pins that MUST be No Connected in 32b PCI mode or must be taken into special consideration for easy migration from the MPC190.

Table 1. MPC184 Pin Diagram

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
A		TMS	TCK	TRST	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC		A
B	TDO	VSS	VSS	VSS	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	B
C	TDI	VSS	VSS	VSS	VSS	3.3V	VSS	3.3V	3.3V	VSS	3.3V	VSS	VSS	VSS	NC	NC	C
D	INTA	GNT	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	NC	NC	D
E	RST#	M66EN	3.3V	3.3V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	3.3V	VSS	NC	NC	E
F	REQ#	Analog Vdd	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	VSS	NC	NC	F
G	VSS	TPA /NC	VSS	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	G
H	CLK	AVSS	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	H
J	VSS	VSS	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	VSS	NC	NC	J
K	AD_30	AD_31	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	K
L	AD_28	AD_29	VSS	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	AD_1	AD_0	L
M	AD_26	AD_27	3.3V	3.3V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	3.3V	VSS	AD_3	AD_2	M
N	AD_24	AD_25	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	AD_5	AD_4	N
P	IDSEL	C/BE_3	VSS	VSS	PLL Bypass	VSS	VSS	3.3V	VSS	3.3V	VSS	VSS	VSS	VSS	AD_7	AD_6	P
R	AD_23	AD_22	VSS	VSS	AD_18	AD_16	FRAME	TRDY	STOP	PERR	PAR	AD_15	AD_13	AD_11	AD_8	C/BE_0	R
T		AD_21	AD_20	AD_19	AD_17	C/BE_2	IRDY	DEVSEL	3.3V	SERR	C/BE_1	AD_14	AD_12	AD_10	AD_9		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 32 bit PCI mode. The shaded regions show the pins that MUST be No Connected in 32b PCI mode or must be taken into special consideration for easy migration from the MPC190. Please also reference Chapter 2, 4 and 7 of the PCI Local Bus Specification Revision 2.2 for other PCI system considerations.

Table 2. Signal Descriptions

Signal Name	Pin Locations	Signal Type	Type	Description
Address/Data and Command Pins (37)				
AD[31:0]	K2, K1, L2, L1, M2, M1, N2, N1, R1, R2, T2, T3, T4, R5, T5, R6, R12, T12, R13, T13, R14, T14, T15, R15, P15, P16, N15, N16, M15, M16, L15, L16	I/O	T/S	Multiplexed Address/Data Bus
C/BE[3-0]#	P2, T6, T11, R16	I/O	T/S	Bus Command/Byte Enables
PAR	R11	I/O	T/S	Parity (Even Parity across AD[31:0], C/BE [3:0]
Interface Control (7)				
FRAME#	R7	I/O	S/T/S	Assertion of FRAME# by an Initiator indicates the beginning of a bus transaction. FRAME is deasserted 1 cycle before conclusion of the transaction.
TRDY#	R8	I/O	S/T/S	Assertion of TRDY# by a target indicates readiness to complete a bus transaction.
IRDY#	T7	I/O	S/T/S	Assertion of IRDY# by an Initiator indicates readiness to complete a bus transaction.
STOP#	R9	I/O	S/T/S	Asserted by a target to request termination a bus transaction.
IDSEL	P1	I	IN	Initialization device select is used as chip select pin during Type 0 configuration transactions.
DEVSEL#	T8	I/O	S/T/S	Asserted by a target when claiming a transaction (following subtractive decode of its address).
M66EN	E2	I	IN	When asserted (at initialization time), the MPC184 enables its internal PLL to operate in the 33-66MHz range.
PLL Bypass	P5	I	IN	PLL Bypass 0 (OVSS) = PLL Disabled 1 (OVDD) = PLL Enabled
Arbitration (2)				
REQ#	F1	O	T/S	Bus Request from Initiator to Arbiter
GNT#	D2	I	T/S	Bus Grant from Arbiter to Initiator
System (3)				
CLK	H1	I	IN	System Clock input
RST#	E1	I	IN	Asynchronous reset signal. Initializes MPC184 to known state.
TPA	G2	O		Test Pad Analog This pin MUST have No Connection
Error Reporting (2)				

Table 2. Signal Descriptions (continued)

Signal Name	Pin Locations	Signal Type	Type	Description
SERR#	T10	O	O/D	System Error is active low when unrecoverable system error is detected.
PERR#	R10	I/O	S/T/S	Parity Error is active low when Parity Error is detected
Interrupt Signals (1)				
INTA#	D1	O	O/D	Interrupt Request
JTAG/Boundary Scan (5)				
TCK	A3	I		Test Clock If JTAG is NOT used, this pin must be tied to VSS
TDI	C1	I		Test Input If JTAG is NOT used, this pin must be tied to OVDD
TDO	B1	O		Test output If JTAG is NOT used, this pin must be NC
TMS	A2	I		Test Mode Select If JTAG is NOT used, this pin must be tied to OVDD
TRST#	A4	I		Test Reset If JTAG is NOT used, this pin must be tied to VSS
Powers/Grounds/No Connects (195)				
Analog VDD	F2			Analog PLL Power MPC184 = +1.5 V MPC190 = +1.8 V
AVSS	H2			Analog PLL Ground
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			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			Core Power MPC184 = +1.5 V MPC190 = +1.8 V

Table 2. Signal Descriptions (continued)

Signal Name	Pin Locations	Signal Type	Type	Description
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, T9			I/O Power (+3.3v)
NC	G16, F15, F16, E15, E16, D15, D16, C15, C16, B15, B16, A15, B14, A14, B13, A13, B12, A12, B11, A11, B10, A10, B9, A9, B8, A8, B7, A7, B6, A6, B5, A5, J15, J16, H15, H16, G15, K16, K15			These pins MUST have No Connection

5 Electrical and Thermal Characteristics

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

5.0.1   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.

5.0.2   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	$^\circ$C/W
Junction to board [3] (bottom)		R	12	$^\circ$C/W
Junction to case [4] (top)		R	6	$^\circ$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).

5.0.3   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 $T_A = 0^\circ$ C to 120° 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_{DDQ}	3.0	3.6	V_{DC}
Input low voltage (Vdd = min)	V_{il}	-0.5	0.3 V_{DDQ}	V_{DC}
Input high voltage (Vdd = max)	V_{ih}	0.5 V_{DDQ}	V_{DDQ}+0.5	V_{DC}
AC supply current (I/O power not included)	I_{DD}	—	400	mA
Standby supply current	I_{SS}	—	150	mA
Input leakage current @ $V_{DDQ} \geq V_{in} \geq V_{SS}$	I_{leak}	—	±10	μA
Output high voltage (I_{oh} = -500 μA)	V_{oh}	0.9 V_{DDQ}	—	V_{DC}
Output low voltage (IOL = 1500μA) I_{ol} = 3.2 mA, C_L = 35 pF ($\overline{IRQ}$) I_{ol} = 3.2 mA, C_L = 50 pF (D[0:31])	V_{ol}	—	0.1 V_{DDQ}	V_{DC}
Output high current [1]	I_{OH}(AC)	-12 V_{DDQ}	-32 V_{DDQ}	μA
Output low current [2]	I_{OL}(AC)	16 V_{DDQ}	38 V_{DDQ}	μA

[1] V_{OUT} = 0.3 V_{DDR} for I_{OH} (min), V_{OUT} = 0.7 V_{DDQ} for I_{OH} (max)

[2] V_{OUT} = 0.6 V_{DDR} for I_{OL} (min), V_{OUT} = 0.18 V_{DDQ} for I_{OL} (max)

5.0.4   AC Timing Specifications

Table 6 shows the AC timing specifications for the master clock and reset signals. Unless specified otherwise, conditions are as follows:

$1.65\ \text{V} \leq \text{IVDD} \leq 1.95\ \text{V};\ \text{VSS} = 0\ \text{V};\ \text{T A} = 0°\ \text{C to } 70°\ \text{C},\ \pm\ 5\%.$

Table 6. AC Timing Specifications—Clock and Reset Pins

Condition	Name	Min	Typ	Max	Units
Output rise/fall time	T_{rfc}	—	—	3	nS
MCLK frequency	F_c	—	66	—	MHz
MCLK duty cycle	F_{dc}	45	50	55	%
$\overline{\text{RESET}}$ pulse width	T_{rst}	16	—	—	cycles
$\overline{\text{RESET}}$ input rise/fall time	T_{rfr}	—	—	1	μS

5.0.5   AC Timing Characteristics

Table 7 shows the AC timing specifications for data signals.

Table 7. AC Electrical Characteristics

Condition	Name	Min	Max	Units
Input Signals				
Clock frequency	F_{clock}	—	66	Mhz
Clock cycle time	t_{cyc}	15	—	nS
Clock-to-signal valid delay [1, 2]	t_{val}	2	6	nS
Input setup time to clock-bused signals	t_{su}	3	—	nS
Input setup time to clock point-to-point signals	$t_{su\ (Pip)}$	5	—	nS
Input hold time clock	t_n	0	—	nS
Float to active delay	t_{on}	2	—	nS
Active to float delay	t_{off}	—	14	nS

[1]   Maximum times are measured with the circuit load shown in Figure 3 and Figure 5.

[2]   Minimum times are measured at the package pin with the circuit load shown in Figure 4.

Figure 3, Figure 4, and Figure 5 show timing circuits.

Pin

1/2 in. max.

Output
Buffer

25 Ω

10 pF
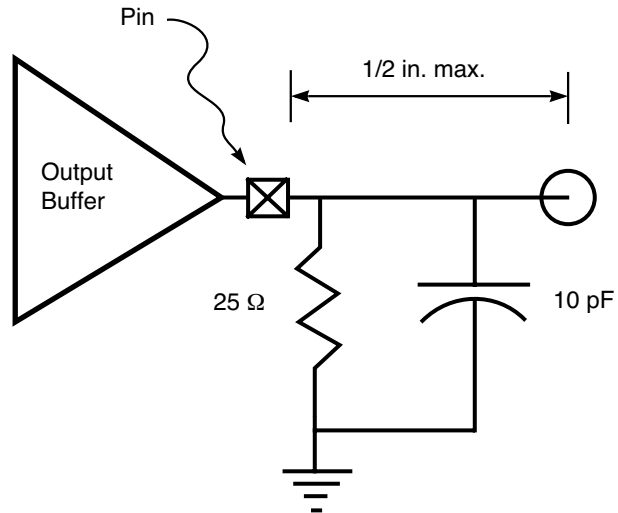
Figure 3. T_{val} (max) Rising Edge

Pin

1/2 in. max.

Output
Buffer

1K Ω

10 pF

1K Ω

Vcc
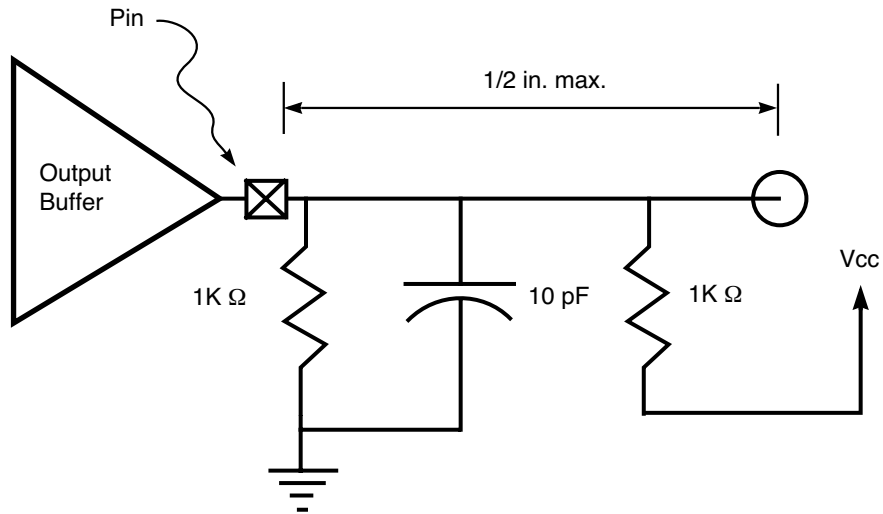
Figure 4. T_{val} (min) and Slew Rate
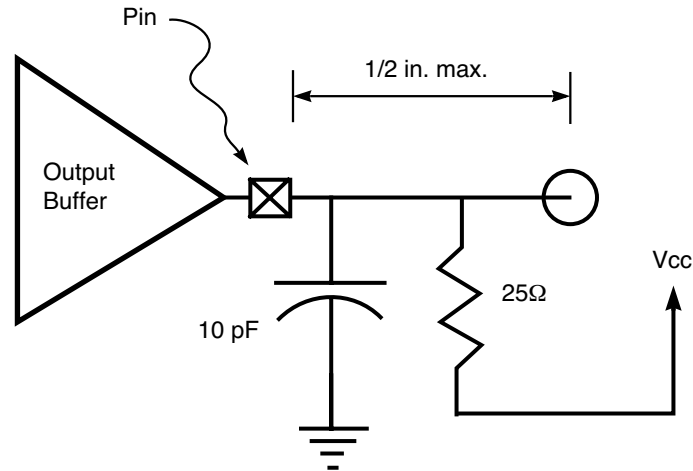
Figure 5. T_{val} (max) Falling Edge

5.0.6   IEEE 1149.1 AC Timing Specifications

All units in Table 8 are nanoseconds.

Table 8. 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
$\overline{TRST}$ 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 6 and Figure 7 show the case outline package dimensions.
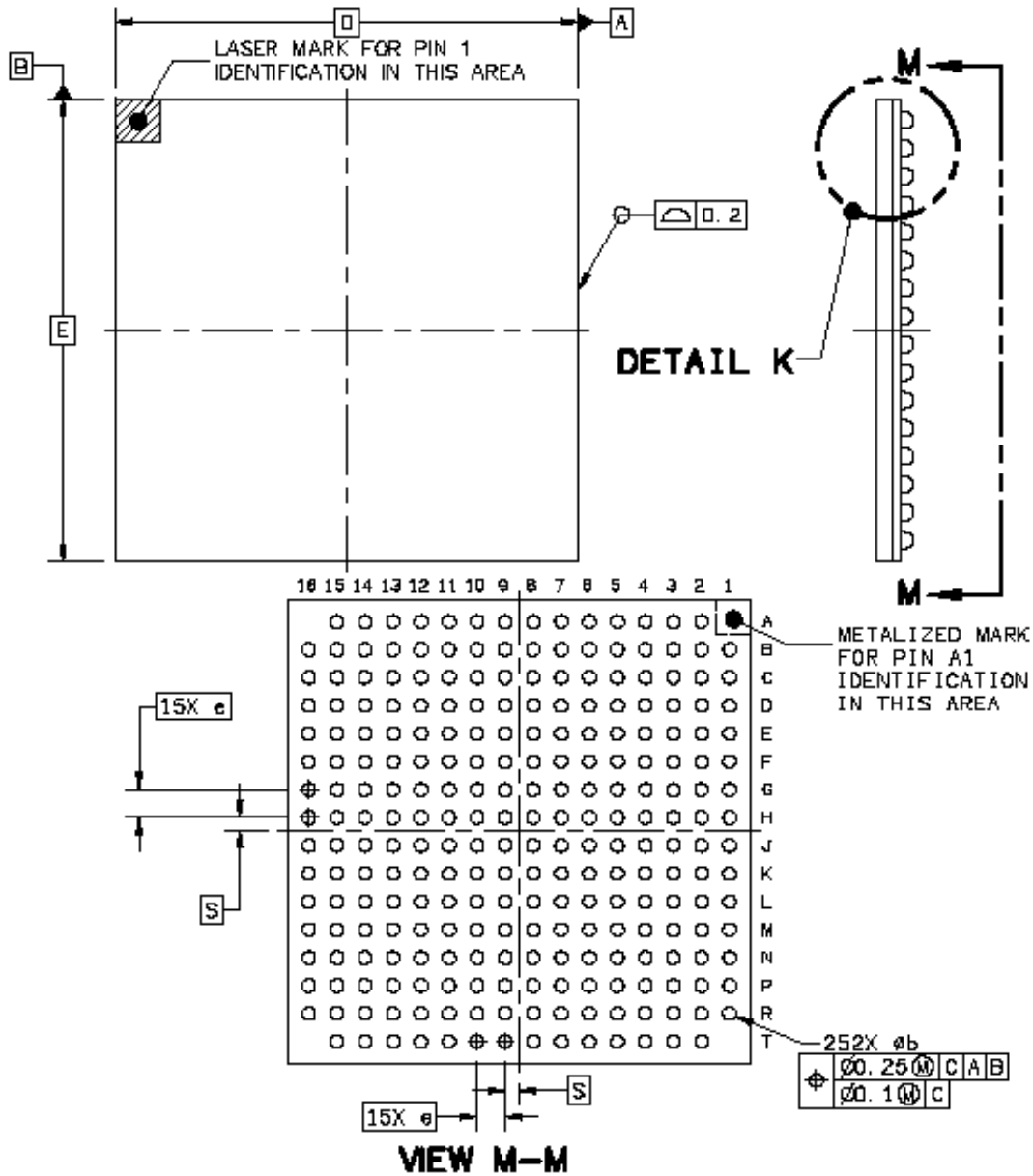
Figure 6. Case Dimensions

Freescale Semiconductor, Inc.

DETAIL K
ROTATED 90° CLOCKWISE

DIM	MIN	MAX	NOTES
A	—	1.9	1. DIMENSIONING AND TOLERANCING PER ASME Y14.5M-1994.
A1	0.5	0.7	
A2	1.16 REF		2. DIMENSIONS IN MILLIMETERS.
b	0.6	0.9	△3 DIMENSION b IS THE MAXIMUM SOLDER BALL DIAMETER MEASURED PARALLEL TO DATUM C.
D	21 BSC		
E	21 BSC		△4 DATUM C THE SEATING PLANE, IS DETERMINED BY THE SPHERICAL CROWNS OF THE SOLDER BALLS.
e	1.27 BSC		
S	0.635 BSC		△5 PARALLELISM REQUIREMENT SHALL EXCLUDE ANY EFFECT OF MARKING ON TOP SURFACE.
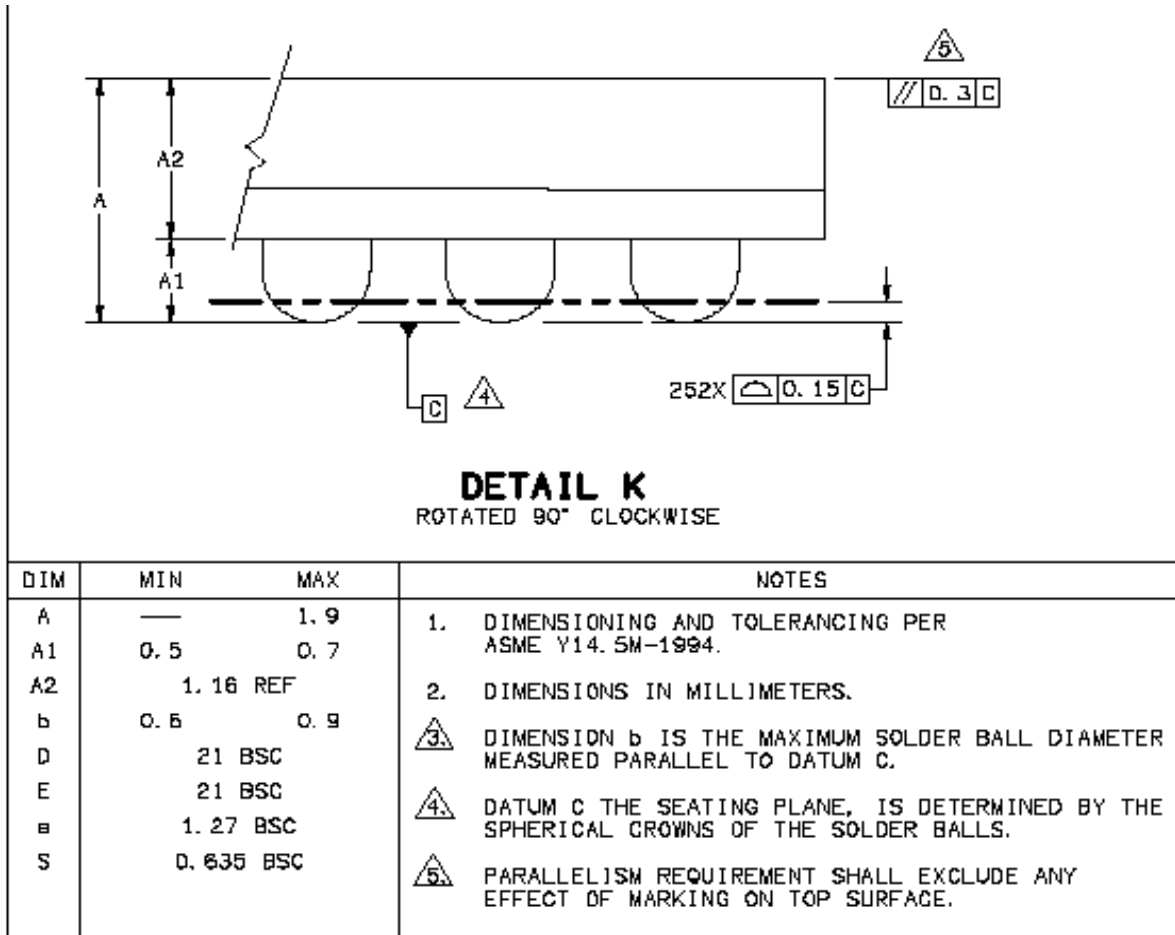
Figure 7. Detail of Case Dimensions

THIS PAGE INTENTIONALLY LEFT BLANK

Freescale Semiconductor, Inc.

THIS PAGE INTENTIONALLY LEFT BLANK

Freescale Semiconductor, Inc.

Home Page:
www.freescale.com
email:
support@freescale.com
USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
(800) 521-6274
480-768-2130
support@freescale.com
Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com
Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku
Tokyo 153-0064, Japan
0120 191014
+81 2666 8080
support.japan@freescale.com
Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com
For Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
(800) 441-2447
303-675-2140
Fax: 303-675-2150
LDCForFreescaleSemiconductor
@hibbertgroup.com

![freescale semiconductor logo]