Rev 0; 3/08

Secure Microprocessor Chip

DS5003

General Description

The DS5003 secure microprocessor incorporates sophisticated security features including an array of mechanisms that are designed to resist all levels of threat, including observation, analysis, and physical attack. As a result, a massive effort is required to obtain any information about its memory contents. Furthermore, the "soft" nature of the DS5003 allows frequent modification of the secure information, thereby minimizing the value of any secure information obtained by such a massive effort. The device is an enhanced version of the DS5002FP secure microprocessor chip with additional scratchpad RAM.

Differences from the DS5002FP

The DS5003 implements only one additional feature from the DS5002FP: it adds 128 bytes of internal scratchpad memory (for a total of 256 bytes) similar to that used in 8032/8052 architectures. This additional memory is accessible through indirect addressing 8051 instructions such as "mov a, @r1," where r1 now can have a value between 0 and 255. It is also usable as stack space for pushes, pops, calls, and returns.

Register indirect addressing is used to access the scratchpad RAM locations above 7Fh. It can also be used to reach the lower RAM (0h–7Fh) if needed. The address is supplied by the contents of the working register specified in the instruction. Thus, one instruction can be used to reach many values by altering the contents of the designated working register. Note that only R0 and R1 can be used as pointers. An example of register indirect addressing is as follows:

```
ANL A, @R0  ;Logical AND the Accumulator with
            the contents of
            ;the register pointed to by the
            value stored in R0
```

Applications

PIN Pads

Gaming Machines

Any Application Requiring Software Protection

Features

- **8051-Compatible Microprocessor for Secure/Sensitive Applications**
  - **Access 32kB, 64kB, or 128kB of Nonvolatile SRAM for Program and/or Data Storage**
  - **128 Bytes of RAM**
  - **128 Bytes of Indirect Scratchpad RAM**
  - **In-System Programming Through On-Chip Serial Port**
  - **Can Modify Its Own Program or Data Memory in the End System**
- **Firmware Security Features**
  - **Memory Stored in Encrypted Form**
  - **Encryption Using On-Chip 64-Bit Key**
  - **Automatic True Random-Key Generator**
  - **Self-Destruct Input (SDI)**
  - **Top Coating Prevents Microprobing**
  - **Protects Memory Contents from Piracy**
- **Crash-Proof Operation**
  - **Maintains All Nonvolatile Resources for Over 10 Years (at Room Temperature) in the Absence of Power**
  - **Power-Fail Reset**
  - **Early Warning Power-Fail Interrupt**
  - **Watchdog Timer**

Ordering Information

PART	TEMP RANGE	INTERNAL MICRO PROBE SHIELD	PIN-PACKAGE
DS5003FPM-16+	0°C to +70°C	Yes	80 MQFP

+Denotes a lead(Pb)-free/RoHS-compliant package.

Pin Configuration appears at end of data sheet.

Secure Microprocessor Chip

ABSOLUTE MAXIMUM RATINGS

Voltage Range on Any Pin Relative to Ground.....-0.3V to (V_{CC} + 0.5V)
Voltage Range on V_{CC} Relative to Ground .....-0.3V to +6.0V

Operating Temperature Range.....40°C to +85°C
Storage Temperature* .....-55°C to +125°C
Soldering Temperature.....Refer to the IPC/JEDEC J-STD-020 Specification.

**Storage temperature is defined as the temperature of the device when V_{CC} = 0V and V_{LI} = 0V. In this state, the contents of SRAM are not battery backed and are undefined.*

Note: The DS5003 adheres to all AC and DC electrical specifications published for the DS5002FP.

Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

DC CHARACTERISTICS

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Operating Voltage	V_{CC}	(Note 1)	V_{CCMIN}		5.5	V
Minimum Operating Voltage	V_{CCMIN}	0°C to +70°C (Note 1)	4.00	4.12	4.25	V
Power-Fail Warning Voltage	V_{PFW}	0°C to +70°C (Note 1)	4.25	4.37	4.50	V
Lithium Supply Voltage	V_{LI}	(Note 1)	2.5		4.0	V
Operating Current at 16MHz	I_{CC}	(Note 2)			36	mA
Idle-Mode Current at 12MHz	I_{IDLE}	0°C to +70°C (Note 3)			7.0	mA
Stop-Mode Current	I_{STOP}	(Note 4)			80	µA
Pin Capacitance	C_{IN}	(Note 5)			10	pF
Output Supply Voltage (V_{CCO})	V_{CCO1}	(Notes 1, 2)	V_{CC} - 0.45			V
Output Supply Battery-Backed Mode (V_{CCO}, $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$, $\overline{PE2}$)	V_{CCO2}	0°C to +70°C (Notes 1, 6)	V_{LI} - 0.65			V
Output Supply Current (Note 7)	I_{CCO1}	V_{CCO} = V_{CC} - 0.45V			75	mA
Lithium-Backed Quiescent Current (Note 8)	I_{LI}	0°C to +70°C		5	75	nA
Reset Trip Point in Stop Mode		BAT = 3.0V (0°C to +70°C) (Note 1)	4.00		4.25	V
		BAT = 3.3V (0°C to +70°C) (Note 1)	4.40		4.65	
Input Low Voltage	V_{IL}	(Note 1)	-0.3		+0.8	V
Input High Voltage	V_{IH1}	(Note 1)	2.0		V_{CC} + 0.3	V
Input High Voltage (RST, XTAL1, $\overline{PROG}$)	V_{IH2}	(Note 1)	3.5		V_{CC} + 0.3	V
Output Low Voltage at I_{OL} = 1.6mA (Ports 1, 2, 3, $\overline{PF}$)	V_{OL1}	(Notes 1, 9)		0.15	0.45	V

DC CHARACTERISTICS (continued)

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Output Low Voltage at I_{OL} = 3.2mA (P0.0–P0.7, ALE, BA0–BA14, BD0–BD7, R/$\overline{W}$, $\overline{CE1N}$, $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, $\overline{VRST}$)	V_{OL2}	(Note 1)		0.15	0.45	V
Output High Voltage at I_{OH} = -80µA (Ports 1, 2, 3)	V_{OH1}	(Note 1)	2.4	4.8		V
Output High Voltage at I_{OH} = -400µA (P0.0–P0.7, ALE, BA0–BA14, BD0–BD7, R/$\overline{W}$, $\overline{CE1N}$, $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, $\overline{VRST}$)	V_{OH2}	(Note 1)	2.4	4.8		V
Input Low Current, V_{IN} = 0.45V (Ports 1, 2, 3)	I_{IL}				-50	µA
Transition Current 1 to 0, V_{IN} = 2.0V (Ports 1, 2, 3)	I_{TL}				-500	µA
SDI Input Low Voltage	V_{ILS}	(Note 1)			0.4	V
SDI Input High Voltage	V_{IHS}	(Notes 1, 10)	2.0		V_{CCO}	V
SDI Pulldown Resistor	R_{SDI}		25		60	kΩ
Input Leakage (P0.0–P0.7, MSEL)	I_{IL}	0.45 < V_{IN} < V_{CC}			+10	µA
RST Pulldown Resistor	R_{RE}	0°C to +70°C	40		150	kΩ
$\overline{VRST}$ Pullup Resistor	R_{VR}			4.7		kΩ
$\overline{PROG}$ Pullup Resistor	R_{PR}			40		kΩ

AC CHARACTERISTICS—SDI PIN

(V_{CC} = 0V to 5V, T_A = 0°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SDI Pulse Reject (Note 11)	t_{SPR}	4.5V < V_{CC} < 5.5V			1.3	µs
		V_{CC} = 0V, V_{BAT} = 2.9V			4	
SDI Pulse Accept (Note 11)	t_{SPA}	4.5V < V_{CC} < 5.5V	10			µs
		V_{CC} = 0V, V_{BAT} = 2.9V	50			

AC CHARACTERISTICS—EXPANDED BUS-MODE TIMING SPECIFICATIONS

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figures 1, 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	MAX	UNITS
Oscillator Frequency	$1/t_{CLK}$		1.0	16.0	MHz
ALE Pulse Width	t_{ALPW}		$2t_{CLK}$ - 40		ns
Address Valid to ALE Low	t_{AVALL}		t_{CLK} - 40		ns
Address Hold After ALE Low	t_{AVAAV}		t_{CLK} - 35		ns
$\overline{RD}$ Pulse Width	t_{RDPW}		$6t_{CLK}$ - 100		ns
$\overline{WR}$ Pulse Width	t_{WRPW}		$6t_{CLK}$ - 100		ns
$\overline{RD}$ Low to Valid Data In	t_{RDLDV}	12MHz		$5t_{CLK}$ - 165	ns
		16MHz		$5t_{CLK}$ - 105	
Data Hold After $\overline{RD}$ High	t_{RDHDV}		0		ns
Data Float After $\overline{RD}$ High	t_{RDHDZ}			$2t_{CLK}$ - 70	ns
ALE Low to Valid Data In	t_{ALLVD}	12MHz		$8t_{CLK}$ - 150	ns
		16MHz		$8t_{CLK}$ - 90	
Valid Address to Valid Data In	t_{AVDV}	12MHz		$9t_{CLK}$ - 165	ns
		16MHz		$9t_{CLK}$ - 105	
ALE Low to $\overline{RD}$ or $\overline{WR}$ Low	t_{ALLRDL}		$3t_{CLK}$ - 50	$3t_{CLK}$ + 50	ns
Address Valid to $\overline{RD}$ or $\overline{WR}$ Low	t_{AVRDL}		$4t_{CLK}$ - 130		ns
Data Valid to $\overline{WR}$ Going Low	t_{DVWRL}		t_{CLK} - 60		ns
Data Valid to $\overline{WR}$ High	t_{DVWRH}	12MHz	$7t_{CLK}$ - 150		ns
		16MHz	$7t_{CLK}$ - 90		
Data Valid After $\overline{WR}$ High	t_{WRHDV}		t_{CLK} - 50		ns
$\overline{RD}$ Low to Address Float	t_{RDLAZ}			0	ns
$\overline{RD}$ or $\overline{WR}$ High to ALE High	t_{RDHALH}		t_{CLK} - 40	t_{CLK} + 50	ns

AC CHARACTERISTICS—EXTERNAL CLOCK DRIVE

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 3)

PARAMETER	SYMBOL	CONDITIONS	MIN	MAX	UNITS
External Clock High Time	t_{CLKHPW}	12MHz	20		ns
		16MHz	15		
External Clock Low Time	t_{CLKLPW}	12MHz	20		ns
		16MHz	15		
External Clock Rise Time	t_{CLKR}	12MHz		20	ns
		16MHz		15	
External Clock Fall Time	t_{CLKF}	12MHz		20	ns
		16MHz		15	

AC CHARACTERISTICS—POWER-CYCLE TIME

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 4)

PARAMETER	SYMBOL	MIN	MAX	UNITS
Slew Rate from V_{CCMIN} to V_{LI}	t_F	130		µs
Crystal Startup Time	t_{CSU}		(Note 12)	
Power-On Reset Delay	t_{POR}		21,504	t_{CLK}

AC CHARACTERISTICS—SERIAL PORT TIMING (MODE 0)

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 5)

PARAMETER	SYMBOL	MIN	MAX	UNITS
Serial Port Clock Cycle Time	t_{SPCLK}	$12t_{CLK}$		µs
Output Data Setup to Rising Clock Edge	t_{DOCH}	$10t_{CLK}$ - 133		ns
Output Data Hold After Rising Clock Edge	t_{CHDO}	$2t_{CLK}$ - 117		ns
Clock Rising Edge to Input Data Valid	t_{CHDV}		$10t_{CLK}$ - 133	ns
Input Data Hold After Rising Clock Edge	t_{CHDIV}	0		ns

AC CHARACTERISTICS—BYTE-WIDE ADDRESS/DATA BUS TIMING

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 6)

PARAMETER	SYMBOL	MIN	MAX	UNITS
Delay to Byte-Wide Address Valid from $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ Low During Op Code Fetch	t_{CE1LPA}		30	ns
Pulse Width of $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$	t_{CEPW}	$4t_{CLK}$ - 35		ns
Byte-Wide Address Hold After $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{CE1HPA}	$2t_{CLK}$ - 20		ns
Byte-Wide Data Setup to $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{OVCE1H}	$1t_{CLK}$ + 40		ns
Byte-Wide Data Hold After $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{CE1HOV}	0		ns
Byte-Wide Address Hold After $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$ High During MOVX	t_{CEHDA}	$4t_{CLK}$ - 30		ns
Delay from Byte-Wide Address Valid $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$ Low During MOVX	t_{CELDA}	$4t_{CLK}$ - 35		ns
Byte-Wide Data Setup to $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$ High During MOVX (Read)	t_{DACEH}	$1t_{CLK}$ + 40		ns
Byte-Wide Data Hold After $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$ High During MOVX (Read)	t_{CEHDV}	0		ns
Byte-Wide Address Valid to R/$\overline{W}$ Active During MOVX (Write)	t_{AVRWL}	$3t_{CLK}$ - 35		ns

AC CHARACTERISTICS—BYTE-WIDE ADDRESS/DATA BUS TIMING (continued)

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 6)

PARAMETER	SYMBOL	MIN	MAX	UNITS
Delay from R/$\overline{W}$ Low to Valid Data Out During MOVX (Write)	t_{RWLDV}	20		ns
Valid Data Out Hold Time from $\overline{CE1}$–$\overline{CE4}$, $\overline{PE1}$–$\overline{PE4}$, or $\overline{CE1N}$ High	t_{CEHDV}	$1t_{CLK}$ - 15		ns
Valid Data Out Hold Time from R/$\overline{W}$ High	t_{RWHDV}	0		ns
Write Pulse Width (R/$\overline{W}$ Low Time)	t_{RWLPW}	$6t_{CLK}$ - 20		ns

RPC AC CHARACTERISTICS—DBB READ

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 7)

PARAMETER	SYMBOL	MIN	MAX	UNITS
$\overline{CS}$, A0 Setup to $\overline{RD}$	t_{AR}	0		ns
$\overline{CS}$, A0 Hold After $\overline{RD}$	t_{RA}	0		ns
$\overline{RD}$ Pulse Width	t_{RR}	160		ns
$\overline{CS}$, A0 to Data Out Delay	t_{AD}		130	ns
$\overline{RD}$ to Data Out Delay	t_{RD}	0	130	ns
$\overline{RD}$ to Data Float Delay	t_{RDZ}		85	ns

RPC AC CHARACTERISTICS—DBB WRITE

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.) (Figure 7)

PARAMETER	SYMBOL	MIN	MAX	UNITS
$\overline{CS}$, A0 Setup to $\overline{WR}$	t_{AW}	0		ns
$\overline{CS}$ Hold After $\overline{WR}$	t_{WA}	0		ns
A0 Hold After $\overline{WR}$	t_{WA}	20		ns
$\overline{WR}$ Pulse Width	t_{WW}	160		ns
Data Setup to $\overline{WR}$	t_{DW}	130		ns
Data Hold After $\overline{WR}$	t_{WD}	20		ns

AC CHARACTERISTICS—DMA

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.)

PARAMETER	SYMBOL	MIN	MAX	UNITS
$\overline{DACK}$ to $\overline{WR}$ or $\overline{RD}$	t_{ACC}	0		ns
$\overline{RD}$ or $\overline{WR}$ to $\overline{DACK}$	t_{CAC}	0		ns
$\overline{DACK}$ to Data Valid	t_{ACD}	0	130	ns
$\overline{RD}$ or $\overline{WR}$ to DRQ Cleared	t_{CRQ}		110	ns

AC CHARACTERISTICS—$\overline{PROG}$

(V_{CC} = 5V ±10%, T_A = 0°C to +70°C.)

PARAMETER	SYMBOL	MIN	MAX	UNITS
$\overline{PROG}$ Low to Active	t_{PRA}	48		Clocks
$\overline{PROG}$ High to Inactive	t_{PRI}	48		Clocks

Note 1: All voltages are referenced to ground.
Note 2: Maximum operating I_{CC} is measured with all output pins disconnected; XTAL1 driven with t_{CLKR}, t_{CLKF} = 10ns, V_{IL} = 0.5V; XTAL2 disconnected; RST = Port 0 = V_{CC}, MSEL = V_{SS}.
Note 3: Idle mode, I_{IDLE}, is measured with all output pins disconnected; XTAL1 driven with t_{CLKR}, t_{CLKF} = 10ns, V_{IL} = 0.5V; XTAL2 disconnected; Port 0 = V_{CC}, RST = MSEL = V_{SS}.
Note 4: Stop mode, I_{STOP}, is measured with all output pins disconnected; Port 0 = V_{CC}; XTAL2 not connected; RST = MSEL = XTAL1 = V_{SS}.
Note 5: Pin capacitance is measured with a test frequency: 1MHz, T_A = +25°C. This specification is characterized but not production tested.
Note 6: V_{CCO2} is measured with $V_{CC} < V_{LI}$ and a maximum load of 10µA on V_{CCO}.
Note 7: I_{CCO1} is the maximum average operating current that can be drawn from V_{CCO} in normal operation.
Note 8: I_{LI} is the current drawn from the V_{LI} input when V_{CC} = 0V and V_{CCO} is disconnected. Battery-backed mode is 2.5V ≤ V_{BAT} ≤ 4.0; $V_{CC} \le V_{BAT}$; V_{SDI} should be ≤ V_{ILS} for I_{BAT} max.
Note 9: $\overline{PF}$ pin operation is specified with $V_{BAT} \ge 3.0V$.
Note 10: V_{IHS} minimum is 2.0V or V_{CCO}, whichever is lower.
Note 11: SDI is deglitched to prevent accidental destruction. The pulse must be longer than t_{SPR} to pass the deglitcher, but SDI is not guaranteed unless it is longer than t_{SPA}.
Note 12: Crystal startup time is the time required to get the mass of the crystal into vibrational motion from the time that power is first applied to the circuit until the first clock pulse is produced by the on-chip oscillator. The user should check with the crystal vendor for a worst-case specification on this time.

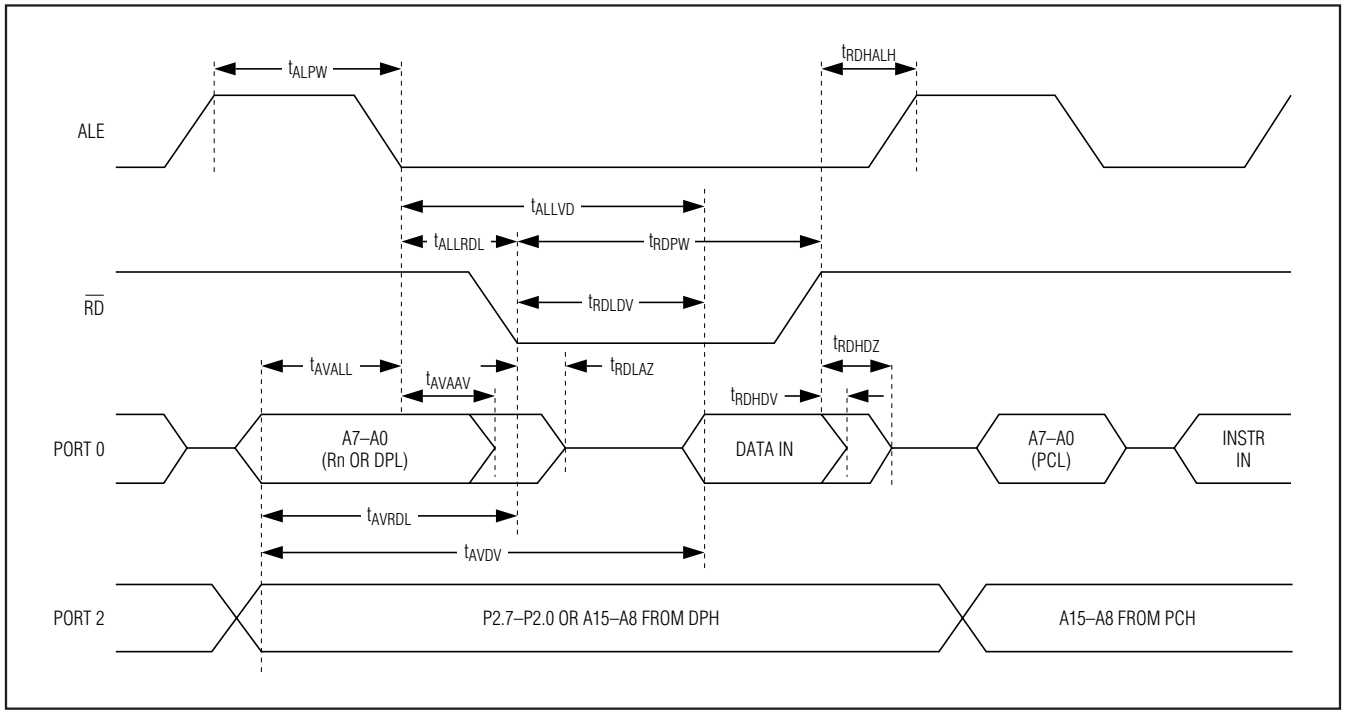


Figure 1. Expanded Data Memory Read Cycle

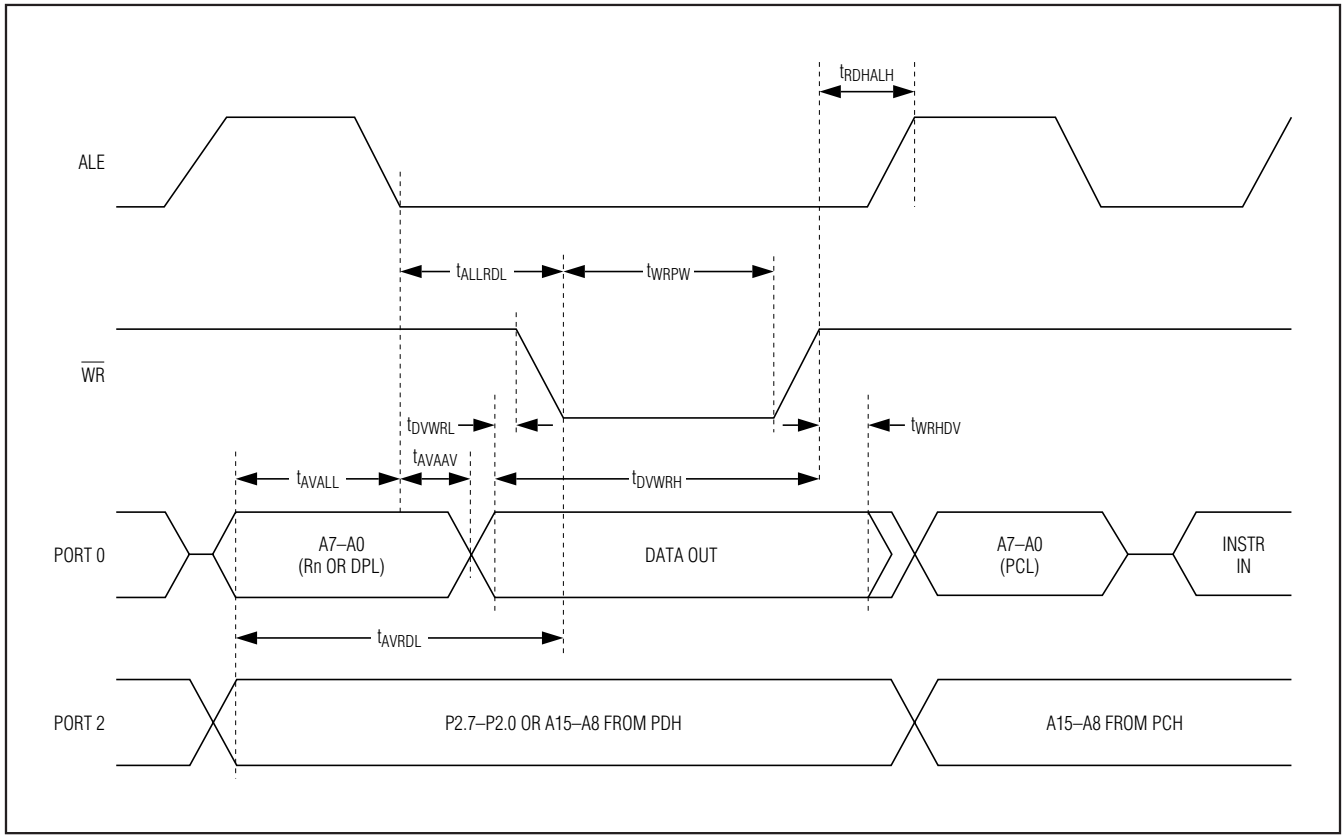


Figure 2. Expanded Data Memory Write Cycle

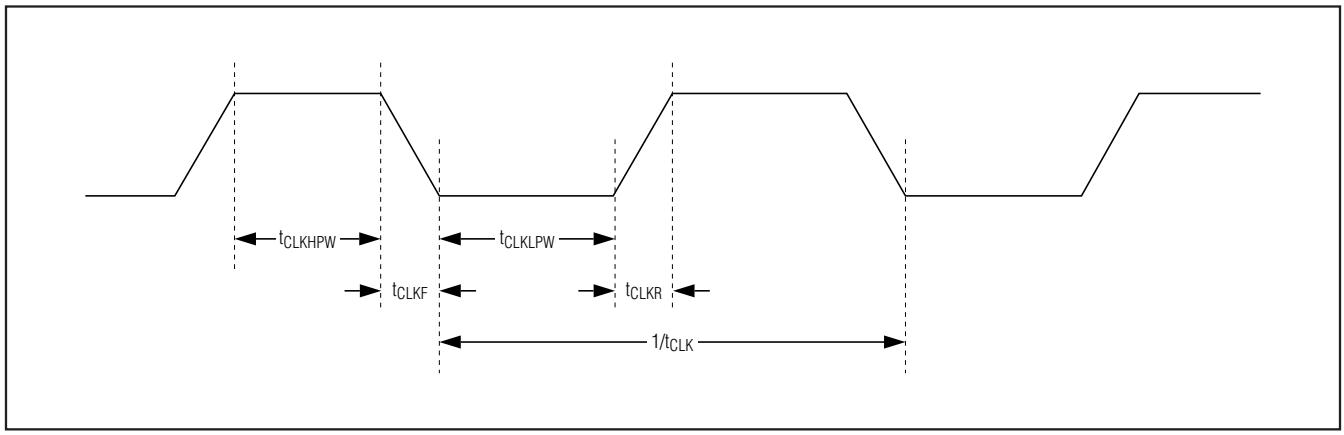


Figure 3. External Clock Timing

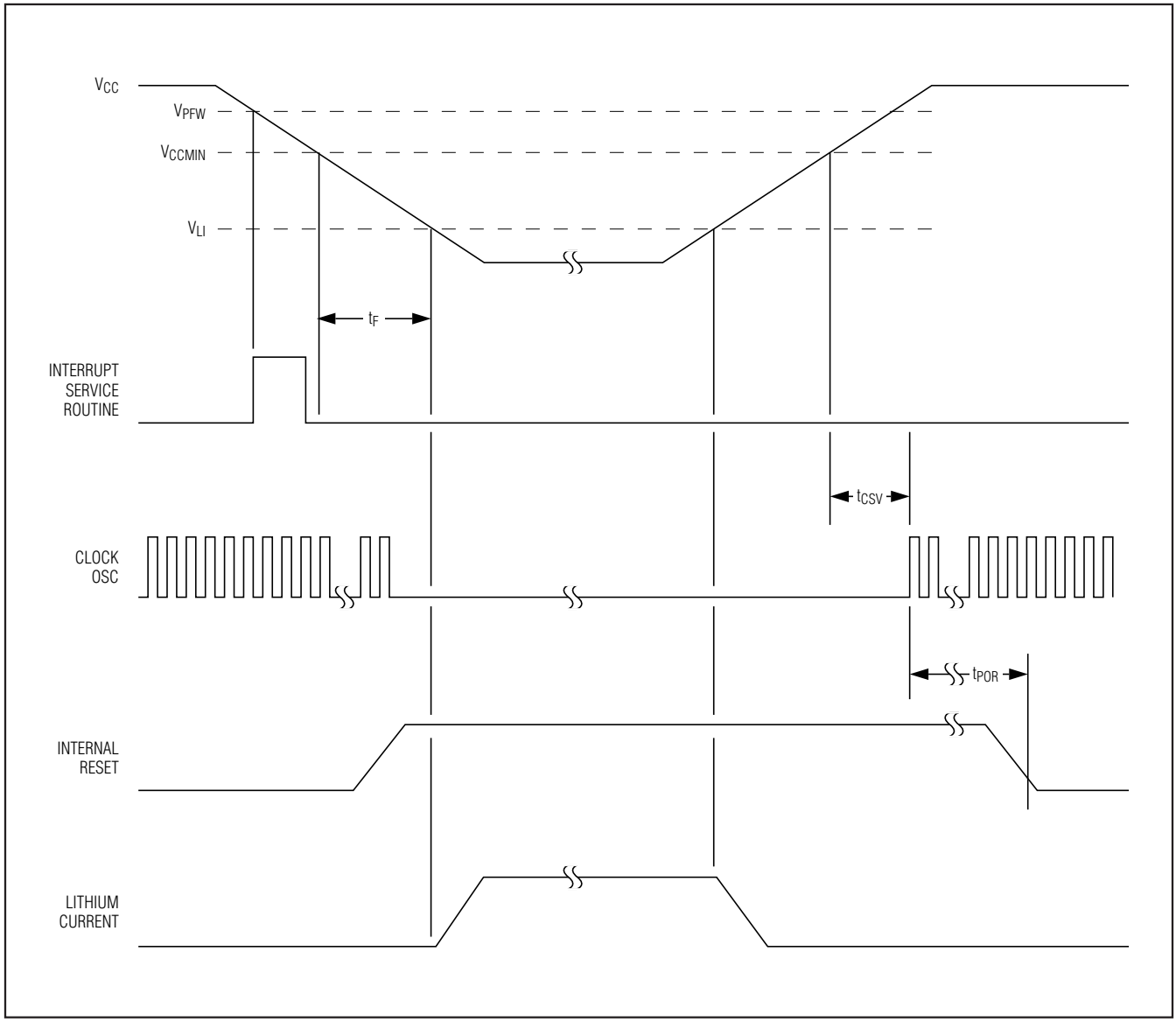


Figure 4. Power-Cycle Timing

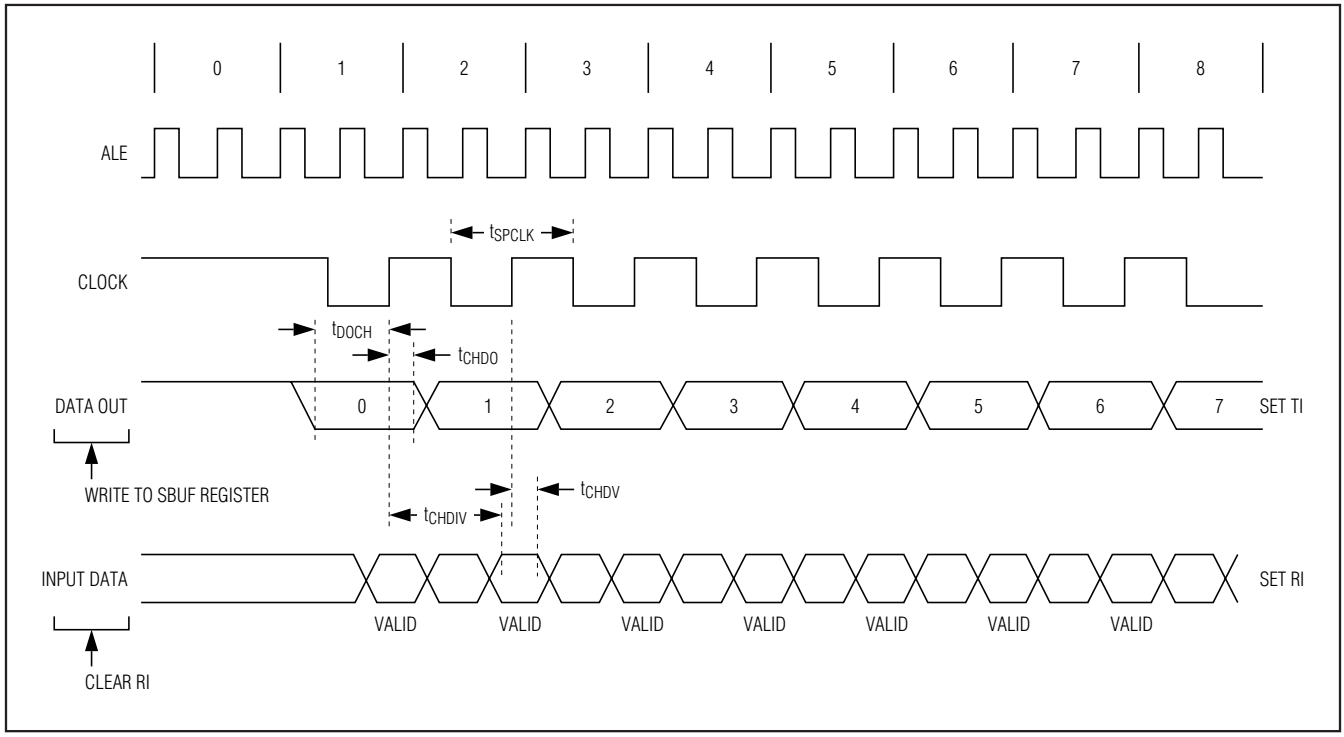


Figure 5. Serial Port Timing (Mode 0)

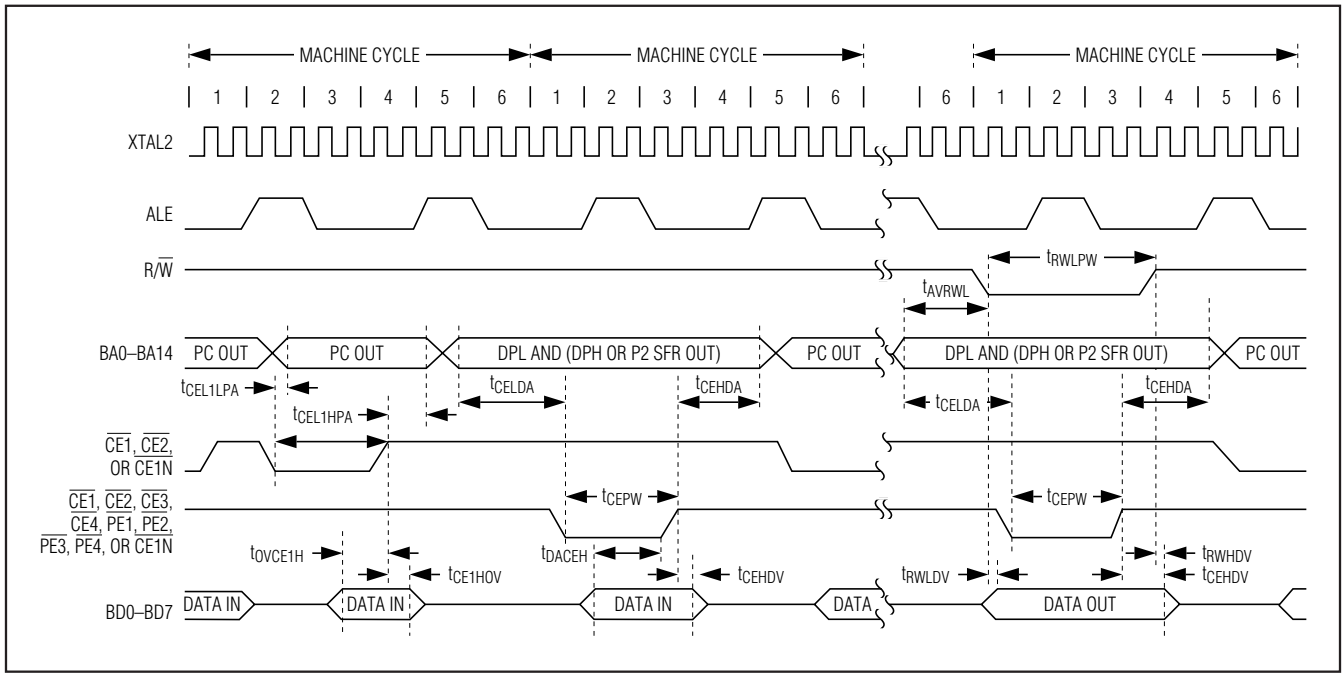


Figure 6. Byte-Wide Bus Timing

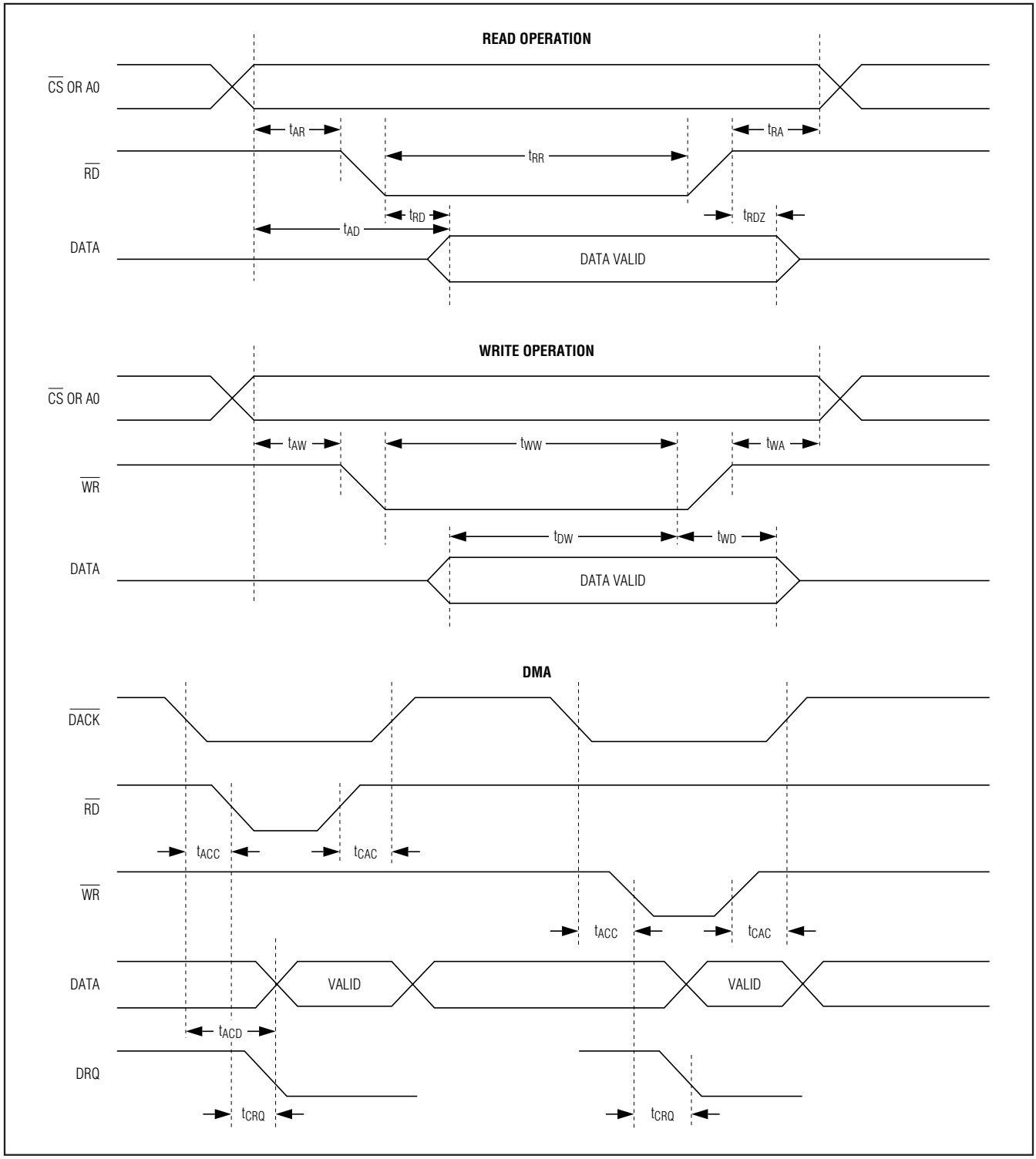


Figure 7. RPC Timing Mode

Pin Description

PIN	NAME	FUNCTION
		POWER PINS
13	V_{CC}	**Power Supply, +5V**
12	V_{CCO}	**V_{CC} Output.** This is switched between V_{CC} and V_{LI} by internal circuits based on the level of V_{CC}. When power is above the lithium input, power is drawn from V_{CC}. The lithium cell remains isolated from a load. When V_{CC} is below V_{LI}, V_{CCO} switches to the V_{LI} source. V_{CCO} should be connected to the V_{CC} pin of an SRAM.
54	V_{LI}	**Lithium Voltage Input.** Connect to a lithium cell greater than V_{LIMIN} and no greater than V_{LIMAX} as shown in the electrical specifications. Nominal value is +3V.
52	GND	**Logic Ground**
		GENERAL-PURPOSE I/O PINS
11	P0.0/AD0	**General-Purpose I/O Port 0.** This port is open drain and cannot drive a logic 1. It requires external pullups. Port 0 is also the multiplexed expanded address/data bus. When used in this mode, it does not require pullups.
9	P0.1/AD1	
7	P0.2/AD2	
5	P0.3/AD3	
1	P0.4/AD4	
79	P0.5/AD5	
77	P0.6/AD6	
75	P0.7/AD7	
15	P1.0	**General-Purpose I/O Port 1**
17	P1.1	
19	P1.2	
21	P1.3	
25	P1.4	
27	P1.5	
29	P1.6	
31	P1.7	
49	P2.0/A8	**General-Purpose I/O Port 2.** Also serves as the MSB of the expanded address bus.
50	P2.1/A9	
51	P2.2/A10	
56	P2.3/A11	
58	P2.4/A12	
60	P2.5/A13	
64	P2.6/A14	
66	P2.7/A15	
36	P3.0/RXD	**General-Purpose I/O Port Pin 3.0.** Also serves as the receive signal for the on-board UART. This pin should not be connected directly to a PC COM port.
38	P3.1/TXD	**General-Purpose I/O Port Pin 3.1.** Also serves as the transmit signal for the on-board UART. This pin should not be connected directly to a PC COM port.
39	P3.2/$\overline{INT0}$	**General-Purpose I/O Port Pin 3.2.** Also serves as the active-low external interrupt 0.
40	P3.3/$\overline{INT1}$	**General-Purpose I/O Port Pin 3.3.** Also serves as the active-low external interrupt 1.
41	P3.4/T0	**General-Purpose I/O Port Pin 3.4.** Also serves as the timer 0 input.
44	P3.5/T1	**General-Purpose I/O Port Pin 3.5.** Also serves as the timer 1 input.
45	P3.6/$\overline{WR}$	**General-Purpose I/O Port Pin 3.6.** Also serves as the write strobe for expanded bus operation.
46	P3.7/$\overline{RD}$	**General-Purpose I/O Port Pin 3.7.** Also serves as the read strobe for expanded bus operation.

Pin Description (continued)

PIN	NAME	FUNCTION
		BYTE-WIDE BUS INTERFACE PINS
37	BA0	**Byte-Wide Address Bus Bits 14–0.** This bus is combined with the nonmultiplexed data bus (BD7–BD0) to access external SRAM. Decoding is performed using $\overline{CE1}$–$\overline{CE4}$. Therefore, BA15 is not actually needed. Read/write access is controlled by R/$\overline{W}$. BA14–BA0 connect directly to an 8kB, 32kB, or 128kB SRAM. If an 8kB SRAM is used, BA13 and BA14 are unconnected. If a 128kB SRAM is used, the microcontroller converts $\overline{CE2}$ and $\overline{CE3}$ to serve as A16 and A15, respectively.
35	BA1	
33	BA2	
30	BA3	
28	BA4	
26	BA5	
24	BA6	
20	BA7	
6	BA8	
4	BA9	
76	BA10	
80	BA11	
18	BA12	
8	BA13	
16	BA14	
55	BD0	**Byte-Wide Data Bus Bits 7–0.** This 8-bit bidirectional bus is combined with the nonmultiplexed address bus (BA14–BA0) to access external SRAM. Decoding is performed on $\overline{CE1}$ and $\overline{CE2}$. Read/write access is controlled by R/$\overline{W}$. D7–D0 connect directly to an SRAM and optionally to a real-time clock or other peripheral.
57	BD1	
59	BD2	
61	BD3	
65	BD4	
67	BD5	
69	BD6	
71	BD7	
70	ALE	**Address Latch Enable.** Used to demultiplex the multiplexed expanded address/data bus on port 0. This pin is normally connected to the clock input on a ’373 type transparent latch.
10	R/$\overline{W}$	**Read/Write (Active Low).** This signal provides the write enable to the SRAMs on the byte-wide bus. It is controlled by the memory map and partition. The blocks selected as program (ROM) are write protected.
74	$\overline{CE1}$	**Active-Low Chip-Enable 1.** This is the primary decoded chip enable for memory access on the byte-wide bus. It connects to the chip-enable input of one SRAM. $\overline{CE1}$ is lithium-backed. It remains in a logic-high inactive state when V_{CC} falls below V_{LI}.
72	$\overline{CE1N}$	**Nonbattery-Backed Version of CE1.** It is not generally useful because the DS5003 cannot be used with EPROM due to its encryption.
2	$\overline{CE2}$	**Active-Low Chip-Enable 2.** This chip enable is provided to access a second 32kB block of memory. It connects to the chip-enable input of one SRAM. When MSEL = 0, the microcontroller converts $\overline{CE2}$ into A16 for a 128kB x 8 SRAM. $\overline{CE2}$ is lithium-backed and remains at a logic-high when V_{CC} falls below V_{LI}.
63	$\overline{CE3}$	**Active-Low Chip-Enable 3.** This chip enable is provided to access a third 32kB block of memory. It connects to the chip-enable input of one SRAM. When MSEL = 0, the microcontroller converts $\overline{CE3}$ into A15 for a 128kB x 8 SRAM. $\overline{CE3}$ is lithium backed and remains at a logic-high when V_{CC} falls below V_{LI}.

Pin Description (continued)

PIN	NAME	FUNCTION
62	$\overline{CE4}$	**Active-Low Chip-Enable 4.** This chip enable is provided to access a fourth 32kB block of memory. It connects to the chip-enable input of one SRAM. When MSEL = 0, this signal is unused. $\overline{CE4}$ is lithium-backed and remains at a logic-high when V_{CC} falls below V_{LI}.
78	$\overline{PE1}$	**Active-Low Peripheral Enable 1.** Accesses data memory between addresses 0000h and 3FFFh when the PES bit is set to logic 1. Commonly used to chip enable a byte-wide real-time clock such as the DS1283. $\overline{PE1}$ is lithium backed and remains at a logic-high when V_{CC} falls below V_{LI}. Connect $\overline{PE1}$ to battery-backed circuitry only.
3	$\overline{PE2}$	**Active-Low Peripheral Enable 2.** Accesses data memory between addresses 4000h and 7FFFh when the PES bit is set to logic 1. $\overline{PE2}$ is lithium backed and remains at a logic-high when V_{CC} falls below V_{LI}. Connect $\overline{PE2}$ to battery-backed circuitry only.
22	$\overline{PE3}$	**Active-Low Peripheral Enable 3.** Accesses data memory between addresses 8000h and BFFFh when the PES bit is set to a logic 1. $\overline{PE3}$ is not lithium backed and can be connected to any type of peripheral function. If connected to a battery-backed chip, it needs additional circuitry to maintain the chip enable in an inactive state when $V_{CC} < V_{LI}$.
23	$\overline{PE4}$	**Active-Low Peripheral Enable 4.** Accesses data memory between addresses C000h and FFFFh when the PES bit is set to logic 1. $\overline{PE4}$ is not lithium backed and can be connected to any type of peripheral function. If connected to a battery-backed chip, it needs additional circuitry to maintain the chip enable in an inactive state when $V_{CC} < V_{LI}$.
14	MSEL	**Memory Select.** This signal controls the memory size selection. When MSEL = +5V, the DS5003 expects to use 32kB x 8 SRAMs. When MSEL = 0V, the DS5003 expects to use a 128kB x 8 SRAM. MSEL must be connected regardless of partition, mode, etc.
CLOCK PINS		
47, 48	XTAL2, XTAL1	**Crystal Connections.** Used to connect an external crystal to the internal oscillator. XTAL1 is the input to an inverting amplifier and XTAL2 is the output.
RESET, STATUS, AND SELF-DESTRUCT PINS		
34	RST	**Active-High Reset Input.** A logic 1 applied to this pin activates a reset state. This pin is pulled down internally so this pin can be left unconnected if not used. An RC power-on reset circuit is not needed and is not recommended.
32	$\overline{PROG}$	**Invokes the Bootstrap Loader on Falling Edge.** This signal should be debounced so that only one edge is detected. If connected to ground, the microcontroller enters bootstrap loading on power-up. This signal is pulled up internally.
42	$\overline{VRST}$	**Reset State Active Due to Low V_{CC}.** This I/O pin (open drain with internal pullup) indicates that the power supply (V_{CC}) has fallen below the V_{CCMIN} level and the microcontroller is in a reset state. When this occurs, the DS5003 drives this pin to logic 0. Because the microcontroller is lithium backed, this signal is guaranteed even when V_{CC} = 0V. Because it is an I/O pin, it also forces a reset if pulled low externally. This allows multiple parts to synchronize their power-down resets.
43	$\overline{PF}$	**Lithium Backup Active.** This output goes to a logic 0 to indicate that the microcontroller has switched to lithium backup. This corresponds to $V_{CC} < V_{LI}$. Because the microcontroller is lithium backed, this signal is guaranteed even when V_{CC} = 0V. The normal application of this signal is to control lithium-powered current to isolate battery-backed functions from nonbattery-backed functions.
53	SDI	**Self-Destruct Input.** An active high on this pin causes an unlock procedure. This results in the destruction of vector SRAM, encryption keys, and the loss of power from V_{CCO}. This pin should be grounded if not used.
MISCELLANEOUS PINS		
68, 73	N.C.	**No Connection**

Detailed Description

The DS5003 implements a security system that loads and executes application software in encrypted form. Up to 128kB of standard SRAM (64kB program + 64kB data) can be accessed by its byte-wide bus. This SRAM is converted by the DS5003 into lithium-backed nonvolatile storage for program and data. Data can be maintained for up to 10 years at room temperature with a very small lithium cell. As a result, the contents of the SRAM and the execution of the software appear unintelligible to the outside observer. The encryption algorithm uses an internally stored and protected key. Any attempt to discover the key value results in its erasure, rendering the encrypted contents of the SRAM useless.

The secure microprocessor chip provides a strong software-encryption algorithm that incorporates elements of DES encryption. The encryption is based on a 64-bit key word, and the key can only be loaded from an on-chip true random-number generator. As a result, the user never knows the true key value. A self-destruct input (SDI) pin is provided to interface to external tamper-detection circuitry. With or without the presence of V_{CC}, activation of the SDI pin has the same effect as resetting the security lock: immediate erasure of the key word and the 48-byte vector SRAM area. In addition, an optional top coating of the die prevents access of information using microprobing techniques.

When implemented as a part of an overall secure system design, a system based on the DS5003 can typically provide a level of security that requires more time and resources to defeat than necessary for unauthorized individuals who have reason to try.

Figure 8 is a block diagram illustrating the internal architecture of the DS5003. The DS5003 operates in an identical fashion to the DS5002FP, except where noted in text.

Secure Operation Overview

The DS5003 incorporates encryption of the activity on its byte-wide address/data bus to prevent unauthorized access to the program and data information contained in the external SRAM. Loading an application program in this manner is performed by the bootstrap loader using the general sequence described as follows:

1) Activate bootstrap loader by asserting the $\overline{PROG}$ pin low for at least 48 clocks.
2) Clear security lock.
3) Set memory map configuration. These settings are identical to those used for DS5002FP-based designs.
4) Load application software.
5) Set security lock.
6) Exit loader by taking the $\overline{PROG}$ pin high again.

Loading of application software into the program/data SRAM is performed while the DS5003 is in its bootstrap load mode. Loading is only possible when the security lock is clear. If the security lock was previously set, it must be cleared by issuing the U command from the bootstrap loader. Clearing the security lock instantly clears the previous key word and the contents of the vector SRAM. In addition, the bootstrap ROM writes zeros into the first 32kB of external SRAM.

The user's application software is loaded into user-supplied external SRAM by the L command in "scrambled" form through on-chip encryptor circuits. Each external SRAM address is an encrypted representation of an on-chip logical address. Thus, the sequential instructions of an ordinary program or data table are stored nonsequentially in SRAM memory. The contents of the program/data SRAM are also encrypted. Each byte in SRAM is encrypted by a key- and address-dependent encryptor circuit such that identical bytes are stored as different values in different memory locations.

The encryption of the program/data SRAM is dependent on an on-chip 64-bit key word. The key is automatically generated by the ROM firmware just prior to the time that the application software is loaded, and is retained as nonvolatile information in the absence of V_{CC} by the lithium-backup circuits. After the application software loading is complete, the key is protected by setting the on-chip security lock, which is also retained as nonvolatile information in the absence of V_{CC}. Any attempt to tamper with the key word and, thereby, gain access to the true program/data SRAM contents results in the erasure of the key word as well as the SRAM contents.

During execution of the application software, logical addresses on the DS5003 that are generated from the program counter or data pointer registers are encrypted before they are presented on the byte-wide address bus. Op codes and data are read back and decrypted before they are operated on by the CPU. Similarly, data values written to the external NV SRAM storage during program execution are encrypted before they are presented on the byte-wide data bus during the write operation. This encryption/decryption process is performed in real time such that no execution time is lost, so the operation of the encryptor circuitry is transparent to the application software.

The DS5003's security features are always enabled.

Secure Microprocessor Chip

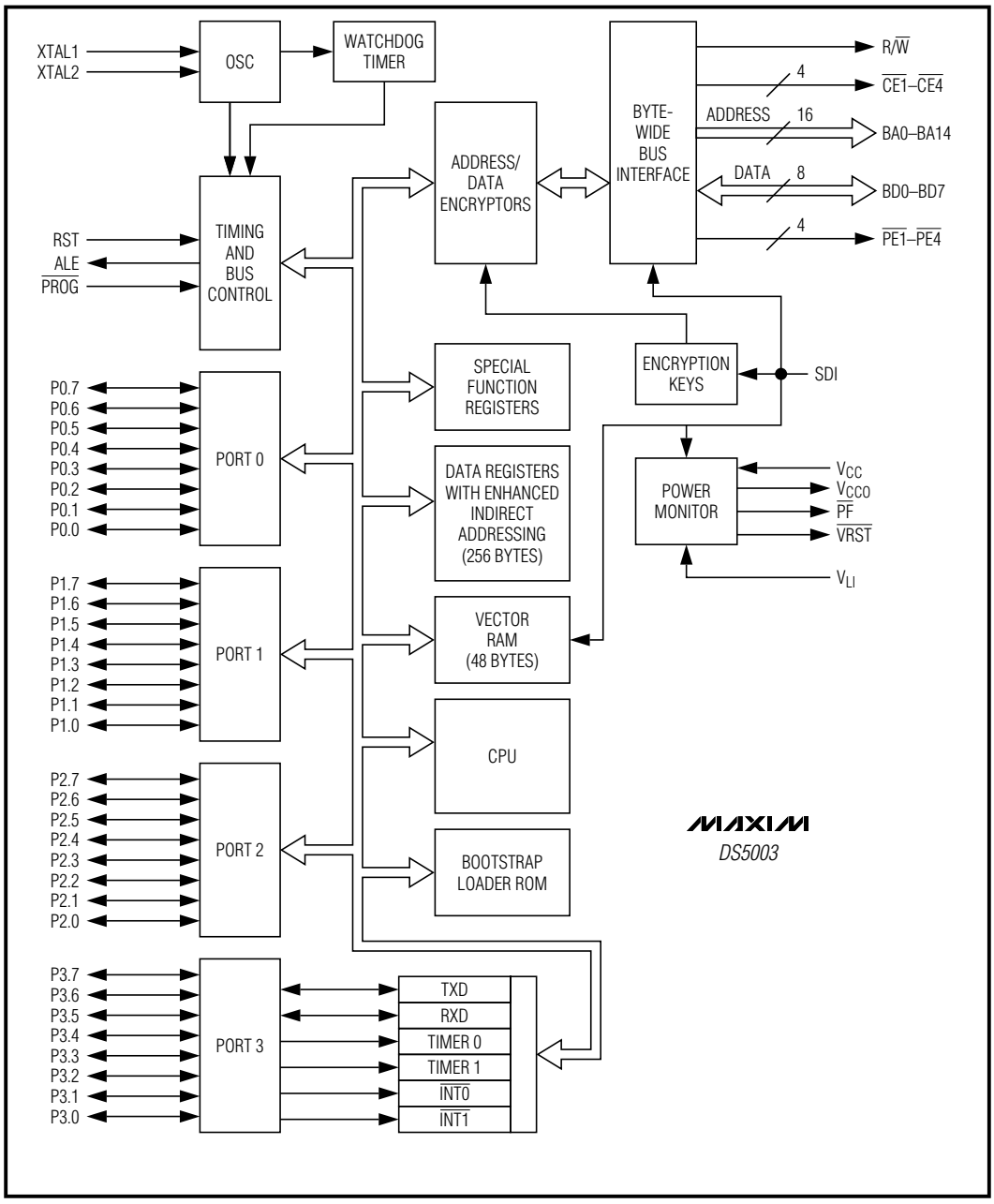


Figure 8. Block Diagram

Security Circuitry

Figure 9 shows the on-chip functions associated with the DS5003's software security feature. Encryption logic consists of an address encryptor and a data encryptor. Although each encryptor uses its own algorithm for encrypting data, both depend on the 64-bit key word that is contained in the encryption key registers. Both the encryptors operate during loading of the application software and also during its execution.

The address encryptor translates each logical address, i.e., the normal sequence of addresses that are generated in the logical flow of program execution, into an encrypted address (or physical address) at which the byte is actually stored. Each time a logical address is generated, either during program loading or during program execution, the address encryptor circuitry uses the value of the 64-bit key word and of the address itself to form the physical address, which are presented on the address lines of the SRAM. The encryption algorithm is such that there is one and only one physical address for every possible logical address. The address encryptor operates over the entire memory range, which is configured during bootstrap loading for access on the byte-wide bus.

As bootstrap loading of the application software is performed, the data encryptor logic transforms the op code, operand, or data byte at any given memory location into an encrypted representation. As each byte is read back to the CPU during program execution, the internal data encryptor restores it to its original value. When a byte is written to the external nonvolatile program/data SRAM during program execution, that byte is stored in encrypted form as well. The data encryption logic uses the value of the 64-bit key, the logical address to which the data is being written, and the value of the data itself to form the encrypted data, which is written to the nonvolatile program/data SRAM. The encryption algorithm is repeatable, such that for a given data value, encryption key value, and logical address the encrypted byte is always the same. However, there are many possible encrypted data values for each possible true-data value due to the algorithm's dependency on the values of the logical address and encryption key.

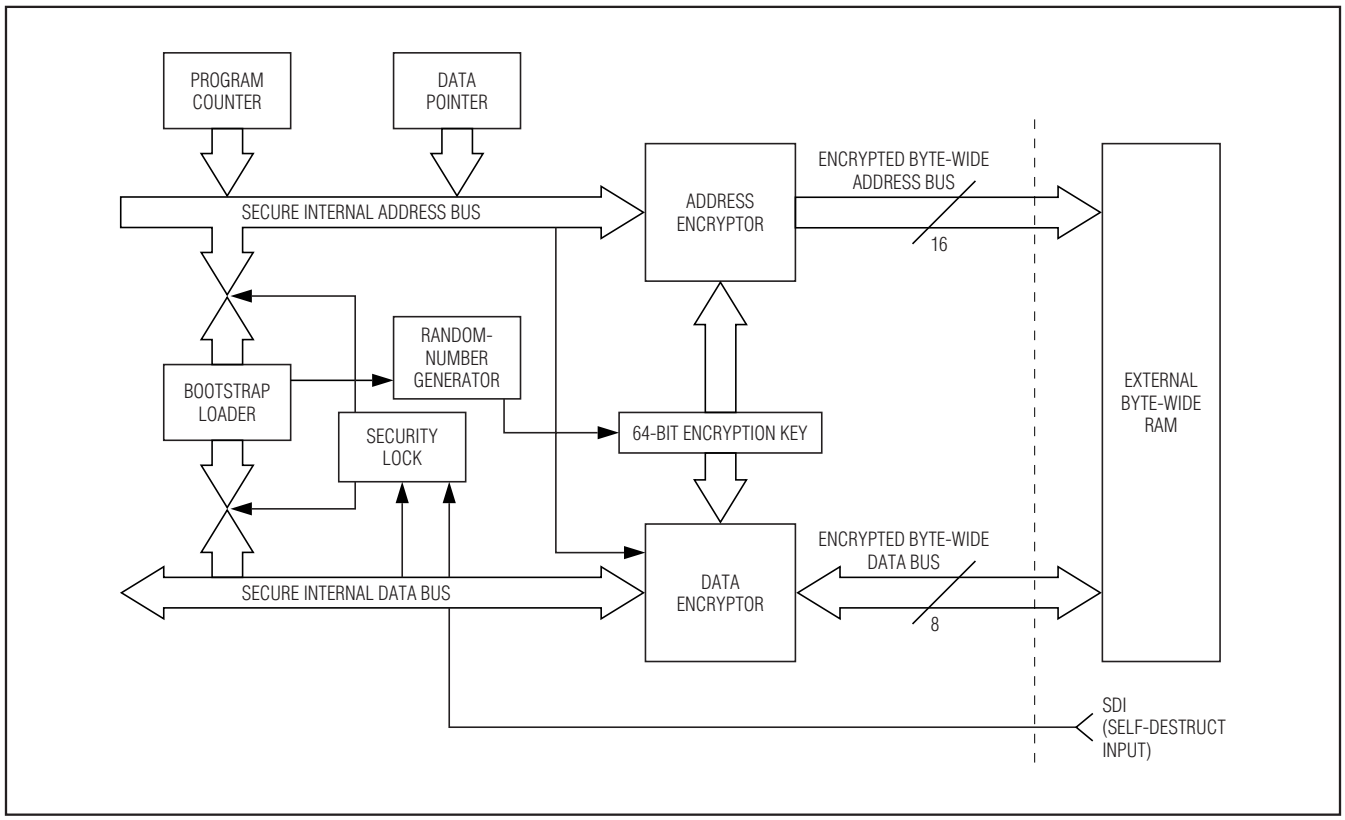


Figure 9. Security Circuitry

Secure Microprocessor Chip

When the application software is executed, the DS5003's internal CPU operates as normal. Logical addresses are calculated for op code fetch cycles and also data read and write operations. The DS5003 can perform address encryption on logical addresses as they are generated internally during the normal course of program execution. In a similar fashion, data is manipulated by the CPU in its true representation. However, data is also encrypted when it is written to the external program/data SRAM, and is restored to its original value when it is read back.

When an application program is stored in the previously described format, it is virtually impossible to disassemble op codes or to convert data back into its true representation. Address encryption has the effect that the op codes and data are not stored in the contiguous form in which they were assembled, but rather in seemingly random locations in memory. This effect makes it virtually impossible to determine the normal flow of the program. As an added protection measure, the address encryptor also generates dummy read-access cycles whenever time is available during program execution.

Dummy Read Cycles

Like the DS5002FP, the DS5003 generates a dummy read-access cycle to nonsequential addresses in external SRAM memory whenever time is available during program execution. This action further complicates the task of determining the normal flow of program execution. During these pseudorandom dummy cycles, the SRAM is read to all appearances, but the data is not used internally. Through the use of a repeatable exchange of dummy and true read cycles, it is impossible to distinguish a dummy cycle from a real one.

Encryption Algorithm

The DS5003 incorporates a proprietary hardware algorithm that performs the scrambling of address and data on the byte-wide bus to the SRAM. Improvements include the following:

- 64-bit encryption key (protected by the security lock function).
- Incorporation of DES-like operations to provide a greater degree of nonlinearity.
- Customizable encryption.

Encryption Key

As previously described, the on-chip 64-bit encryption key is the basis of both the address and data encryptor circuits. When the loader is given certain commands, the key is generated from an on-chip hardware random-number generator. This action is performed just prior to actually loading the code into the external SRAM. This scheme prevents characterization of the encryption algorithm by continuously loading new, known keys. It also frees the user from the burden of protecting the key selection process.

The random-number generator circuit uses the asynchronous frequency differences of two internal ring oscillators and the processor master clock (determined by XTAL1 and XTAL2). As a result, a true random number is produced.

Vector RAM

A 48-byte vector RAM area is incorporated on-chip, and is used to contain the reset and interrupt vector code in the DS5003. It is included in the architecture to help ensure the security of the application program.

If reset and interrupt vector locations were accessed from the external nonvolatile program/data RAM during the execution of the program, it would be possible to determine the encrypted value of known addresses. This could be done by forcing an interrupt or reset condition and observing the resulting addresses on the byte-wide address/data bus. For example, it is known that when a hardware reset is applied, the logical program address is forced to location 0000h and code is executed starting from this location. It would then be possible to determine the encrypted value (or physical address) of the logical address value 0000h by observing the address presented to the external SRAM following a hardware reset. Interrupt vector address relationships could be determined in a similar fashion. By using the on-chip vector RAM to contain the interrupt and reset vectors, it is impossible to observe such relationships. The vector RAM eliminates the unlikely possibility that an application program could be deciphered by observing vector address relationships. Note that the dummy accesses mentioned are conducted while fetching from vector RAM.

The vector RAM is automatically loaded with the user's reset and interrupt vectors from the Intel hex file during bootstrap loading.

Security Lock

Once the application program has been loaded into the DS5003's external and vector RAM, the security lock can be enabled by issuing the Z command in the bootstrap loader. While the security lock is set, no further access to program/data information is possible by the on-chip ROM. Access is prevented by both the bootstrap loader firmware and the DS5003 encryptor circuits.

Access to the SRAM can only be regained by clearing the security lock by the U command in the bootstrap

loader. This action triggers several events that defeat tampering. First, the encryption key is instantaneously erased. Without the encryption key, the DS5003 can no longer decrypt the contents of the SRAM. Therefore, the application software can no longer be correctly executed, nor can it be read back in its true form by the bootstrap loader. Second, the vector RAM area is also instantaneously erased, so that the reset and vector information is lost. Third, the bootstrap loader firmware sequentially erases the encrypted SRAM area. Lastly, the loader creates and loads a new random key.

The security lock bit is constructed using a multiple-bit latch that is interlaced for self-destruction in the event of tampering. The lock is designed to set up a "domino effect" such that erasure of the bit results in an unstoppable sequence of events that clears critical data including encryption key and vector RAM. In addition, this bit is protected from probing by the top-coating feature.

Self-Destruct Input (SDI)

The self-destruct input (SDI) pin is an active-high input that is used to reset the security lock in response to a variety of user-defined external events. The SDI input is intended to be used with external tamper-detection circuitry. It can be activated with or without operating power applied to the V_{CC} pin. Activation of the SDI pin instantly resets the security lock and causes the same sequence of events previously described for this action. In addition, power is momentarily removed from the byte-wide bus interface including the V_{CC} pin, resulting in the loss of data in external SRAM.

Top-Layer Coating

The DS5003M is provided with a special top-layer coating that is designed to prevent a probe attack. This coating is implemented with second-layer metal added through special processing of the microcontroller die. This additional layer is not a simple sheet of metal, but rather a complex layout that is interwoven with power and ground, which are in turn connected to logic for the encryption key and the security lock. As a result, any attempt to remove the layer or probe through it results in the erasure of the security lock and/or the loss of encryption key bits.

Bootstrap Loading

Initial loading of application software into the DS5003 is performed by firmware within the on-chip bootstrap loader communicating with a PC by the on-chip serial port. Table 1 summarizes the commands accepted by the bootstrap loader.

When the bootstrap loader is invoked, portions of the 256-byte scratchpad RAM area are automatically overwritten with zeros and then used for variable storage for the bootstrap firmware. Also, a set of 8 bytes is generated using the random-number generator circuitry and saved as a potential word for the 64-bit encryption key.

Any read or write operation to the DS5003's external program/data SRAM can only take place if the security lock bit is in a cleared state. Therefore, the first step in loading a program should be the clearing of the security lock bit through the U command.

Table 1. Serial Bootstrap Loader Commands

COMMAND	FUNCTION
C	Return CRC-16 of the program/data SRAM.
D	Dump RAM memory specified by MSL bit as Intel hex format.
F	Fill program/data SRAM.
G	Get data from P0, P1, P2, and P3.
L	Load Intel hex file.
N	Set freshness seal—all program and data is lost.
P	Put data into P0, P1, P2, and P3.
R	Read status of SFRs (MCON, RPCTL, MSL).
T	Trace (echo) incoming Intel hex code.
U	Clear security lock.
V	Verify program/data memory with incoming Intel hex data.
W	Write special function registers (MCON, RPCTL, MSL).
Z	Set security lock.

Execution of certain bootstrap loader commands result in the loading of the newly generated 64-bit random number into the encryption key word. These commands are as follows:

Fill	F
Load	L
Dump	D
Verify	V
CRC	C

Execution of the Fill and Load commands load the encrypted data into SRAM using encryption keys from the newly generated key word. The subsequent execution of the Dump command *within the same bootstrap session* causes the contents of the encrypted SRAM to

be read out and transmitted back to the host PC in decrypted form. Similarly, execution of the Verify command *within the same bootstrap session* causes the incoming absolute hex data to be compared against the true contents of the encrypted SRAM, and the CRC command returns the CRC value calculated from the true contents of the encrypted SRAM. As long as any of these commands are executed *within the same bootstrap session*, the loaded key value remains the same and the contents of the encrypted program/data SRAM can be read or written normally and freely until the security lock bit is set.

When the security lock bit is set using the Z command, no further access to the true SRAM contents is possible using any bootstrap command or by any other means.

A more extensive explanation of the serial loader operation can be found in the *Secure Microcontroller User's Guide* (**www.maxim-ic.com/SecureUG**).

Instruction Set

The DS5003 executes an instruction set that is object-code compatible with the industry-standard 8051 microcontroller. As a result, software development packages such as assemblers and compilers that have been written for the 8051 are compatible with the DS5003. A complete description of the instruction set and operation is provided in the *Secure Microcontroller User's Guide*.

Memory Organization

Figure 10 illustrates the memory map accessed by the DS5003. The entire 64kB of program and 64kB of data are potentially available to the byte-wide bus. This preserves the I/O ports for application use. The user controls the portion of memory that is actually mapped to the byte-wide bus by selecting the program range and data range. Any area not mapped into the SRAM is

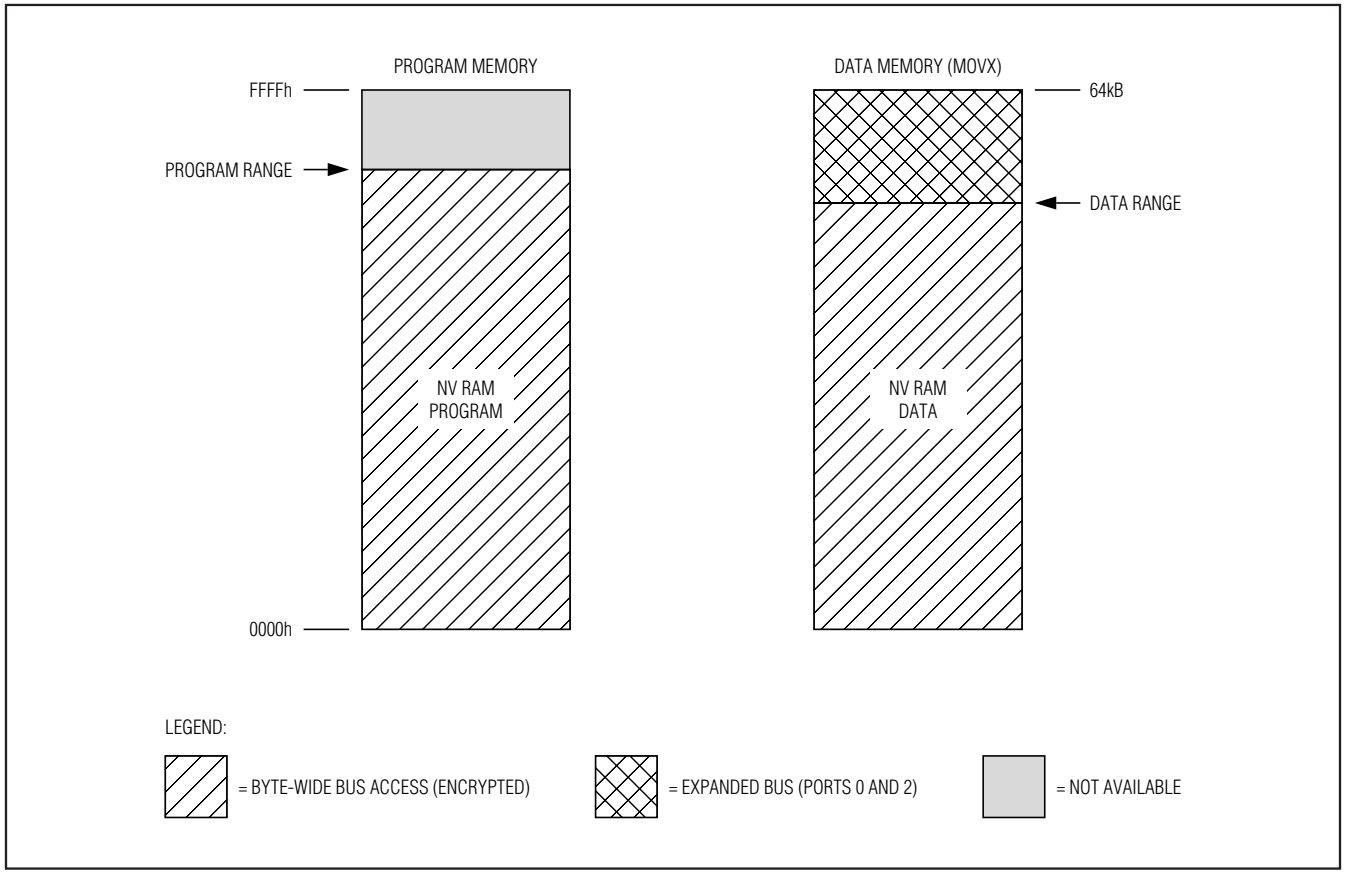


Figure 10. Memory Map in Nonpartitionable Mode (PM = 1)

reached by the expanded bus on ports 0 and 2. An alternate configuration allows dynamic partitioning of a 64kB space as shown in Figure 11. Selecting PES = 1 provides another 64kB of potential data storage or memory-mapped peripheral space as shown in Figure 12. These selections are made using special function registers. The memory map and its controls are covered in detail in the *Secure Microcontroller User's Guide*.

Figure 13 illustrates a typical memory connection for a system using a 128kB SRAM. Note that in this configuration, both program and data are stored in a common SRAM chip. Figure 14 shows a similar system with using two 32kB SRAMs. The byte-wide address bus connects to the SRAM address lines. The bidirectional byte-wide data bus connects the data I/O lines of the SRAM.

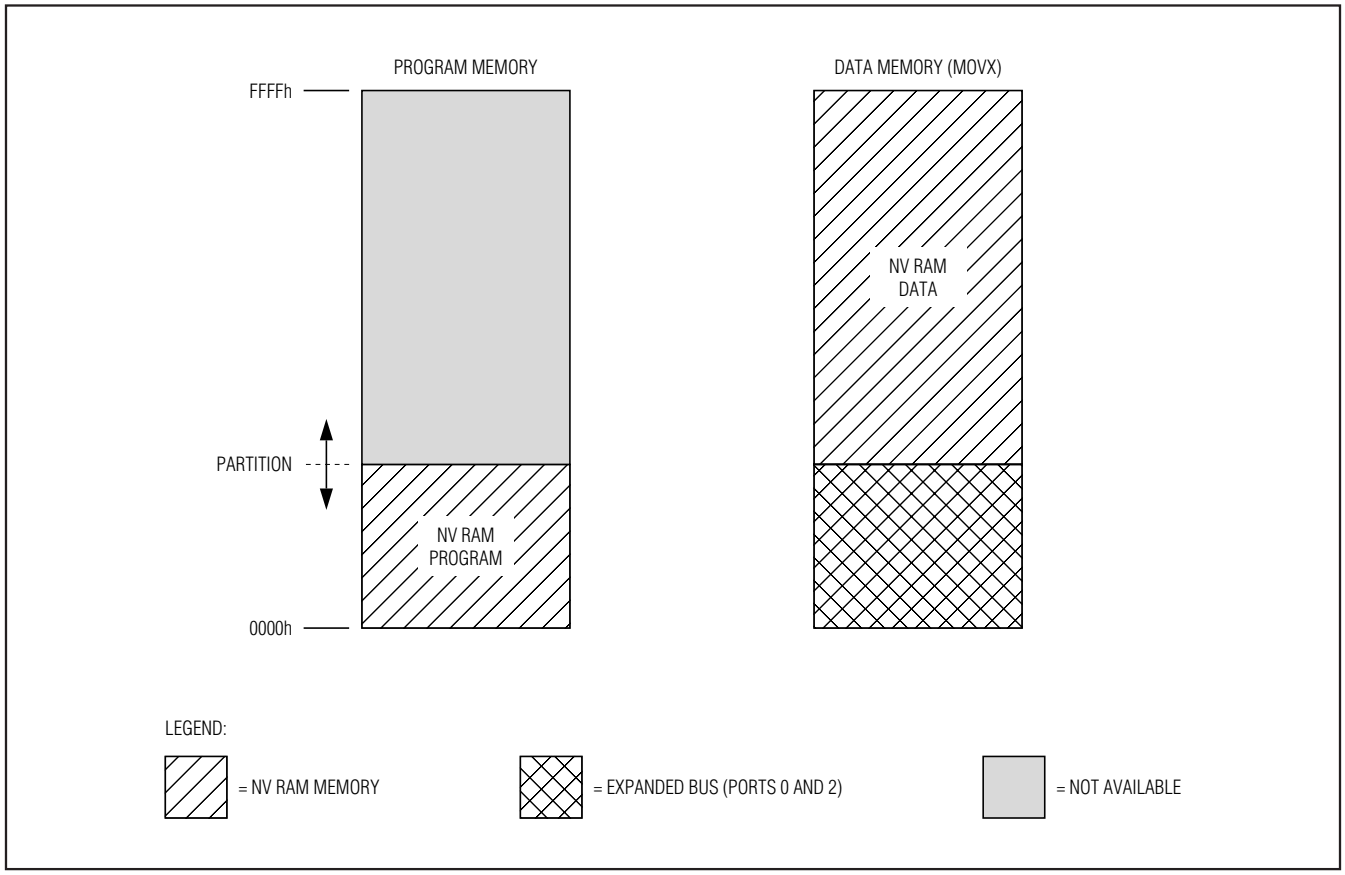


Figure 11. Memory Map in Partitionable Mode (PM = 0)

Secure Microprocessor Chip

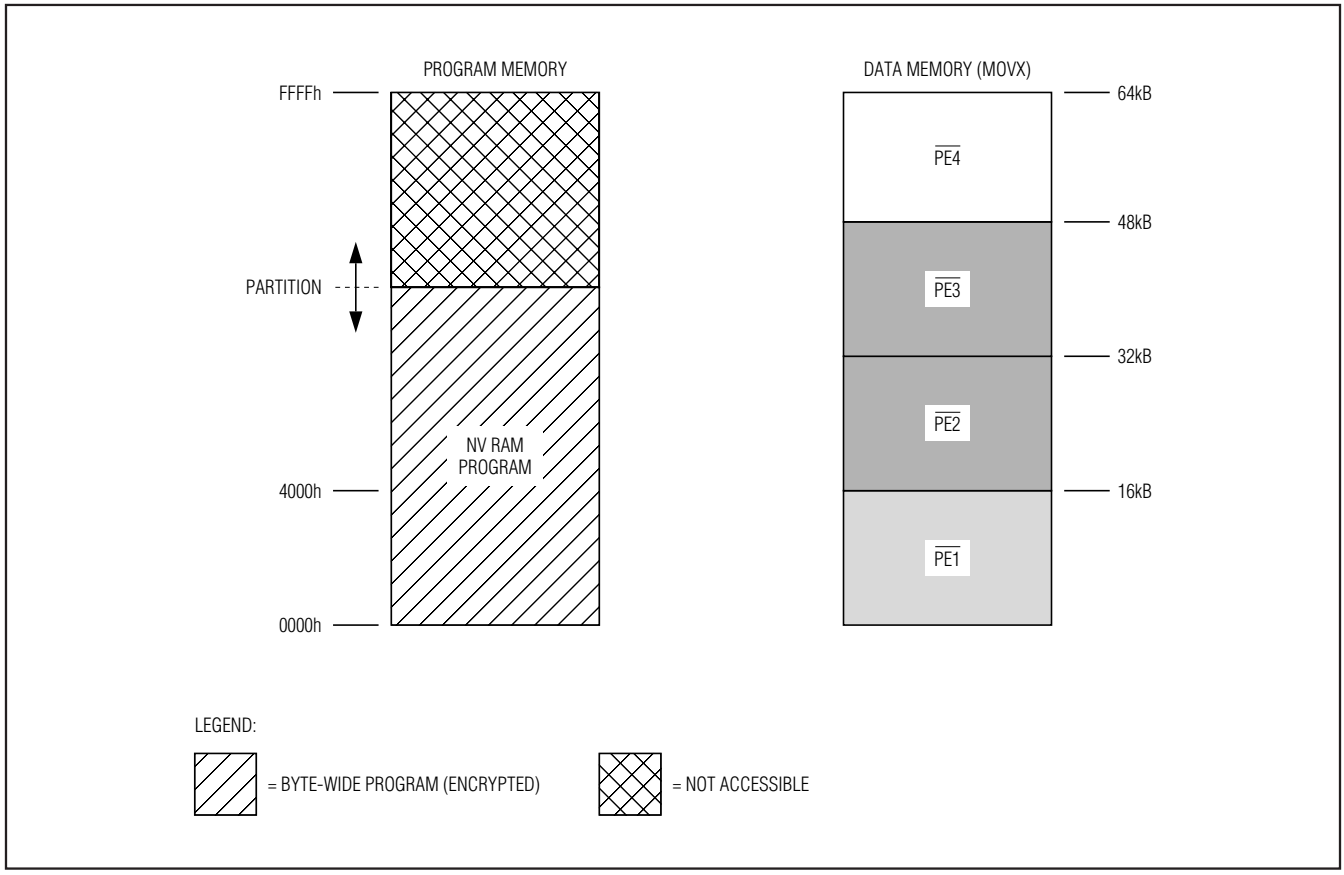


Figure 12. Memory Map with PES = 1

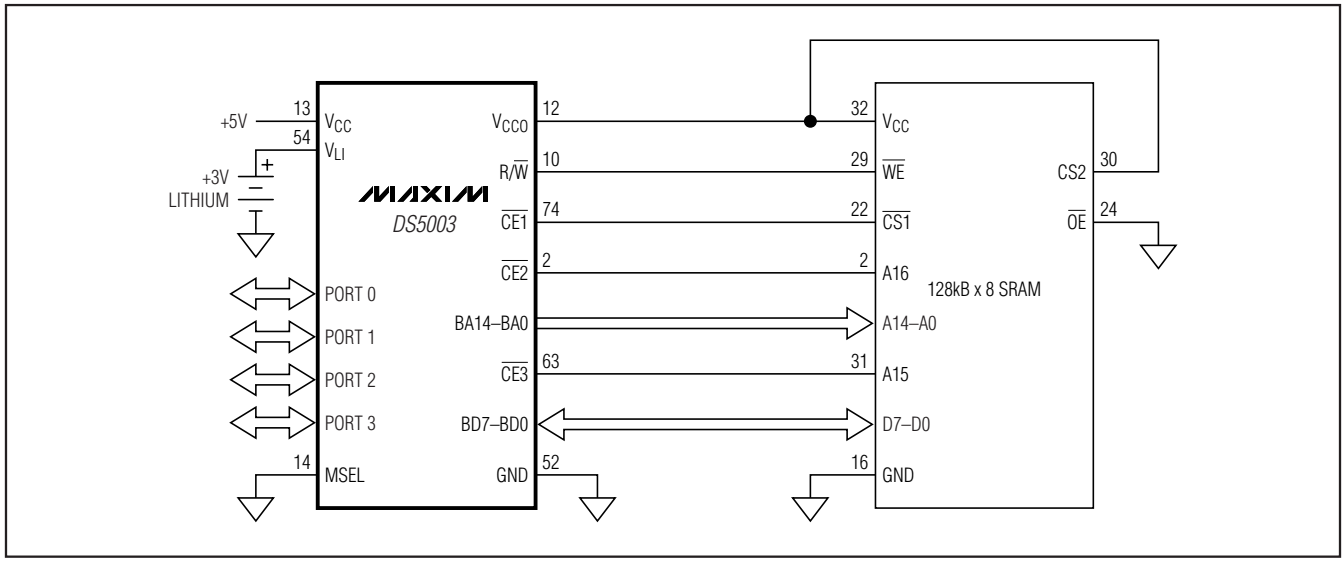


Figure 13. Connection to 128kB x 8 SRAM

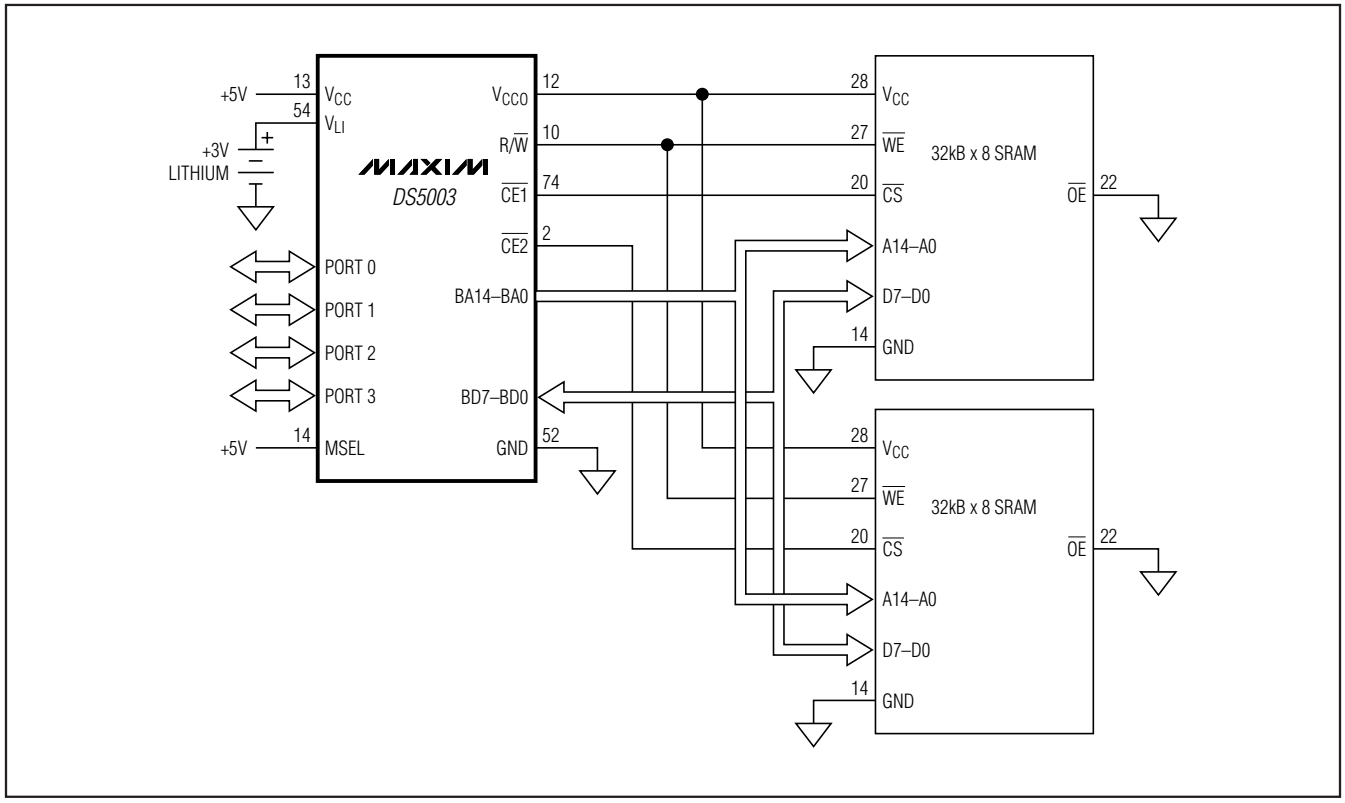


Figure 14. Connection to 64kB x 8 SRAM

Power Management

The DS5003 monitors V_{CC} to provide power-fail reset, early warning power-fail interrupt, and switchover to lithium backup. It uses an internal bandgap reference in determining the switch points. These are called V_{PFW}, V_{CCMIN}, and V_{LI}, respectively. When V_{CC} drops below V_{PFW}, the DS5003 performs an interrupt and vectors to location 2Bh if the power-fail warning was enabled. Full processor operation continues regardless. When power falls further to V_{CCMIN}, the DS5003 invokes a reset state. No further code execution is performed unless power rises back above V_{CCMIN}. All decoded chip enables and the R/$\overline{W}$ signal go to an inactive (logic 1) state. V_{CC} is still the power source at this time. When V_{CC} drops further to below V_{LI}, internal circuitry switches to the lithium cell for power. The majority of internal circuits are disabled and the remaining nonvolatile states are retained. Any devices connected to V_{CCO} are powered by the lithium cell at this time. V_{CCO} is at the lithium battery voltage minus approximately 0.45V (less a diode drop), depending on the load. Low-power SRAMs should be used for this reason. When using the DS5003, the user must select the appropriate battery to match the SRAM data-retention current and the desired backup lifetime. Note that the lithium cell is only loaded when $V_{CC} < V_{LI}$. The *Secure Microcontroller User's Guide* has more information on this topic. The trip points V_{CCMIN} and V_{PFW} are listed in the electrical specifications.

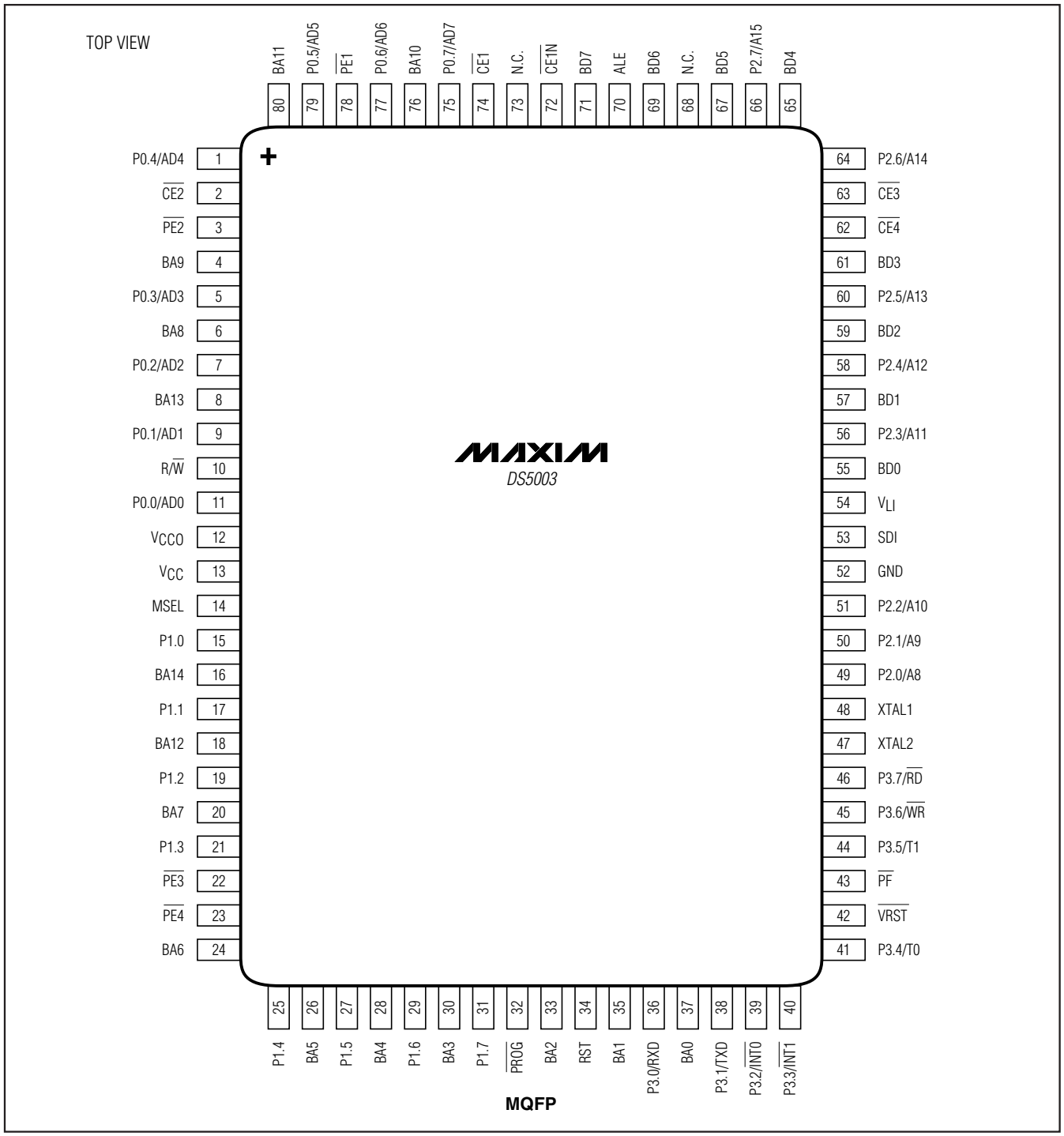
Package Information

For the latest package outline information and land patterns, go to **www.maxim-ic.com/packages**.

PACKAGE TYPE	PACKAGE CODE	DOCUMENT NO.
80 MQFP	M80+2	**21-0271**

Secure Microprocessor Chip

Pin Configuration



MQFP