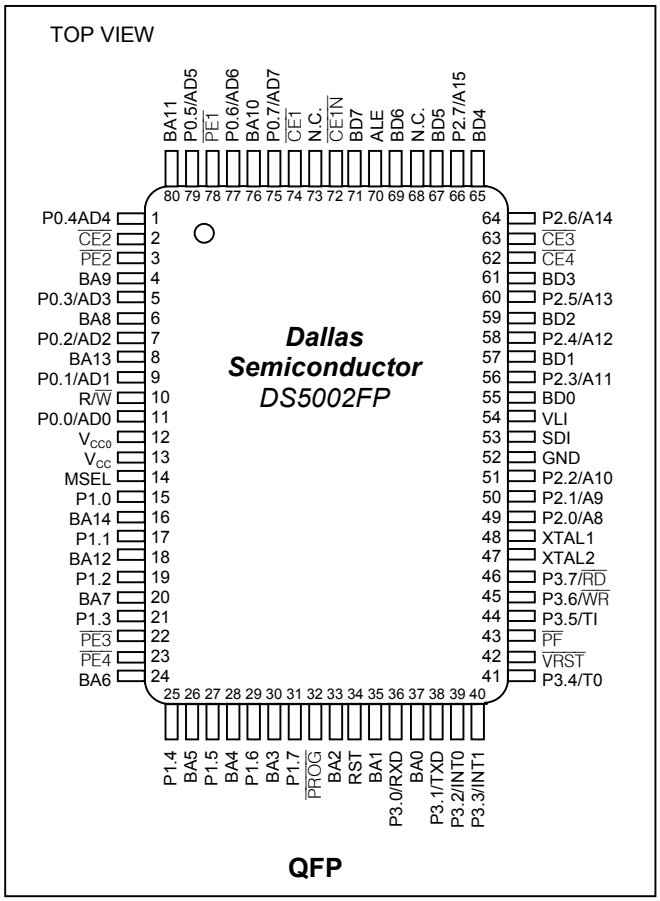
DS5002FP
Secure Microprocessor Chip

www.maxim-ic.com

GENERAL DESCRIPTION

The DS5002FP secure microprocessor chip is a secure version of the DS5001FP 128k soft microprocessor chip. In addition to the memory and I/O enhancements of the DS5001FP, the secure microprocessor chip incorporates the most sophisticated security features available in any processor. The security features of the DS5002FP include 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 memory contents. Furthermore, the "soft" nature of the DS5002FP allows frequent modification of the secure information, thereby minimizing the value of any secure information obtained by such a massive effort.

PIN CONFIGURATION



FEATURES

- 8051-Compatible Microprocessor for Secure/Sensitive Applications
  - Access 32kB, 64kB, or 128kB of NV SRAM for Program and/or Data Storage
  - 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)
  - Optional Top Coating Prevents Microprobe (DS5002FPM)
  - Improved Security Over Previous Generations Protects Memory Contents from Piracy
- Crash-Proof Operation
  - Maintains All Nonvolatile Resources for Over 10 Years in the Absence of Power
  - Power-Fail Reset
  - Early Warning Power-Fail Interrupt
  - Watchdog Timer

ORDERING INFORMATION

PART	TEMP RANGE	PIN-PACKAGE
DS5002FP-16	0°C to +70°C	80 QFP
DS5002FPM-16	0°C to +70°C	80 QFP
DS5002FP-16N	-40°C to +85°C	80 QFP
DS5002FMN-16	-40°C to +85°C	80 QFP

Selector Guide appears at end of data sheet.

Note: *Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, click here: www.maxim-ic.com/errata.*

ELECTRICAL SPECIFICATIONS

The DS5002FP adheres to all AC and DC electrical specifications published for the DS5001FP. The absolute maximum ratings and unique specifications for the DS5002FP are listed below.

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	See IPC/JEDEC J-STD-020A

This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operation sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods of time can affect reliability.

**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.*

DC CHARACTERISTICS

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

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
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, 13)		0.15	0.45	V
Output Low Voltage at I_{OL} = 3.2mA (Ports 0, ALE, BA15–0, BD7–0, R/$\overline{W}$, $\overline{CE1N}$, $\overline{CE}$ 1–4, $\overline{PE}$ 1–4, V_{RST})	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 (Ports 0, ALE, BA15–0, BD7–0, R/$\overline{W}$, $\overline{CE1N}$, $\overline{CE}$ 1–4, $\overline{PE}$ 1–4, V_{RST})	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}	0°C to +70°C			-500	µA
	I_{TL}	-40°C to +85°C (Note 12)			-600	µA
SDI Input Low Voltage	V_{ILS}	(Note 1)			0.4	V
SDI Input High Voltage	V_{IHS}	(Notes 1, 11)	2.0		V_{CCO}	V
SDI Pulldown Resistor	R_{SDI}		25		60	kΩ

DC CHARACTERISTICS (continued)

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

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Input Leakage Current (Port 0, MSEL)	I_{IL}	0.45 < V_{IN} < V_{CC}			+10	µA
RST Pulldown Resistor	R_{RE}	0°C to +70°C	40		150	kΩ
		-40°C to +85°C (Note 12)	30		180	
$\overline{VRST}$ Pullup Resistor	R_{VR}			4.7		kΩ
$\overline{PROG}$ Pullup Resistor	R_{PR}			40		kΩ
Power-Fail Warning Voltage	V_{PFW}	0°C to +70°C (Note 1)	4.25	4.37	4.5	V
		-40°C to +85°C (Notes 1, 12)	4.1	4.37	4.6	
Minimum Operating Voltage	V_{CCMIN}	0°C to +70°C (Note 1)	4.00	4.12	4.25	V
		-40°C to +85°C (Notes 1, 12)	3.85	4.09	4.25	
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
		-40°C to +85°C (Notes 3, 12)			8.0	
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{CE}$1–4, $\overline{PE}$ 1–2)	V_{CCO2}	0°C to +70°C (Notes 1, 8)	V_{LI} -0.65			V
		-40°C to +85°C (Notes 1, 8, 12)	V_{LI} -0.9			
Output Supply Current (Note 6)	I_{CCO1}	V_{CCO} = V_{CC} - 0.45V			75	mA
Lithium-Backed Quiescent Current (Note 7)	I_{LI}	0°C to +70°C		5	75	nA
		-40°C to +85°C		75	500	
Reset Trip Point in Stop Mode		BAT = 3.0V (0°C to +70°C) (Note 1)	4.0		4.25	
		BAT = 3.0V (-40°C to +85°C) (Notes 1, 12)	3.85		4.25	
		BAT = 3.3V (0°C to +70°C) (Note 1)	4.4		4.65	

AC CHARACTERISTICS

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

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SDI Pulse Reject (Note 10)	t_{SPR}	4.5V < V_{CC} < 5.5V			2	µs
		V_{CC} = 0V, V_{BAT} = 2.9V			4	
SDI Pulse Accept (Note 10)	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.) (Figure 1 and Figure 2)

#	PARAMETER	SYMBOL	CONDITIONS	MIN	MAX	UNITS
1	Oscillator Frequency	$1 / t_{CLK}$		1.0	16	MHz
2	ALE Pulse Width	t_{ALPW}		$2t_{CLK}$ - 40		ns
3	Address Valid to ALE Low	t_{AVALL}		t_{CLK} - 40		ns
4	Address Hold After ALE Low	t_{AVAAV}		t_{CLK} - 35		ns
14	$\overline{RD}$ Pulse Width	t_{RDPW}		$6t_{CLK}$ - 100		ns
15	$\overline{WR}$ Pulse Width	t_{WRPW}		$6t_{CLK}$ - 100		ns
16	$\overline{RD}$ Low to Valid Data In	t_{RDLDV}	12MHz		$5t_{CLK}$ - 165	ns
			16MHz		$5t_{CLK}$ - 105	
17	Data Hold after $\overline{RD}$ High	t_{RDHDV}		0		ns
18	Data Float after $\overline{RD}$ High	t_{RDHDZ}			$2t_{CLK}$ - 70	ns
19	ALE Low to Valid Data In	t_{ALLVD}	12MHz		$8t_{CLK}$ - 150	ns
			16MHz		$8t_{CLK}$ - 90	
20	Valid Address to Valid Data In	t_{AVDV}	12MHz		$9t_{CLK}$ - 165	ns
			16MHz		$9t_{CLK}$ - 105	
21	ALE Low to $\overline{RD}$ or $\overline{WR}$ Low	t_{ALLRDL}		$3t_{CLK}$ - 50	$3t_{CLK}$ + 50	ns
22	Address Valid to $\overline{RD}$ or $\overline{WR}$ Low	t_{AVRDL}		$4t_{CLK}$ - 130		ns
23	Data Valid to $\overline{WR}$ Going Low	t_{DVWRL}		t_{CLK} - 60		ns
24	Data Valid to $\overline{WR}$ High	t_{DVWRH}	12MHz	$7t_{CLK}$ - 150		ns
			16MHz	$7t_{CLK}$ - 90		
25	Data Valid after $\overline{WR}$ High	t_{WRHDV}		t_{CLK}-50		ns
26	$\overline{RD}$ Low to Address Float	t_{RDLAZ}			0	ns
27	$\overline{RD}$ or $\overline{WR}$ High to ALE High	t_{RDHALH}		t_{CLK} - 40	t_{CLK} + 50	ns

Figure 1. Expanded Data Memory Read Cycle

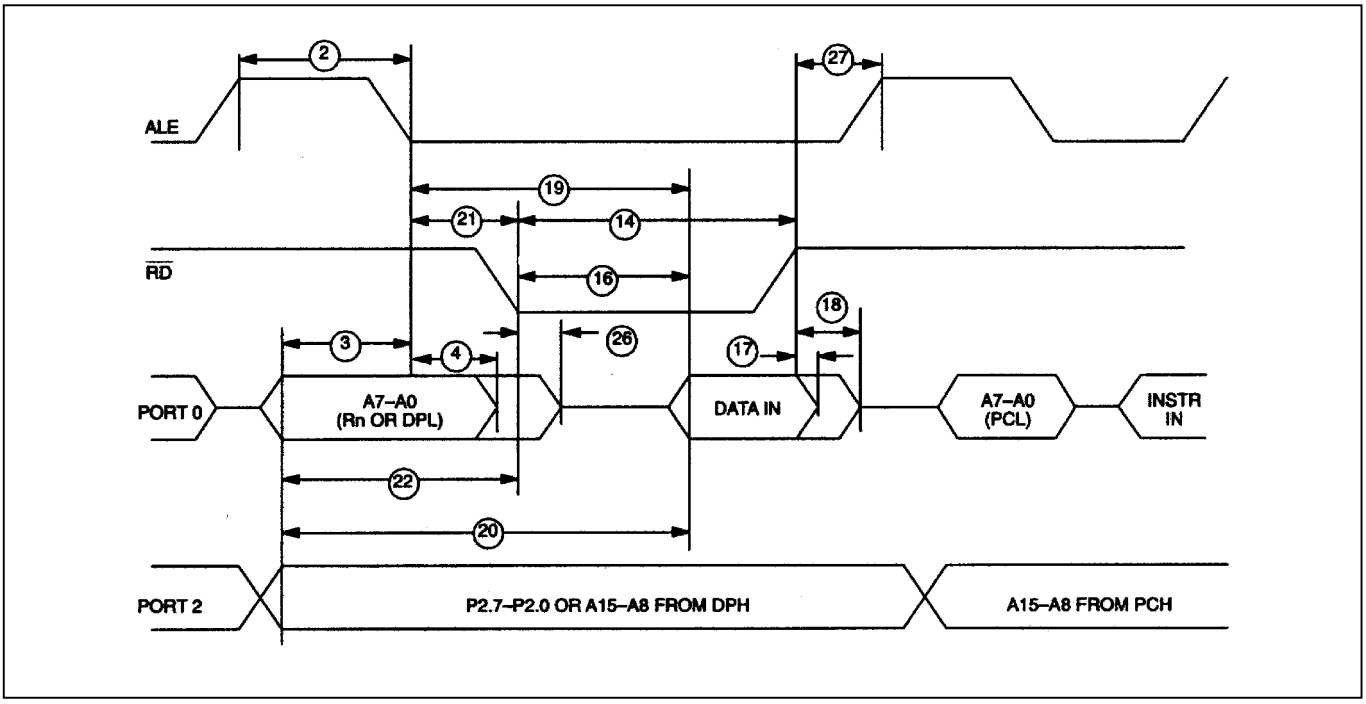
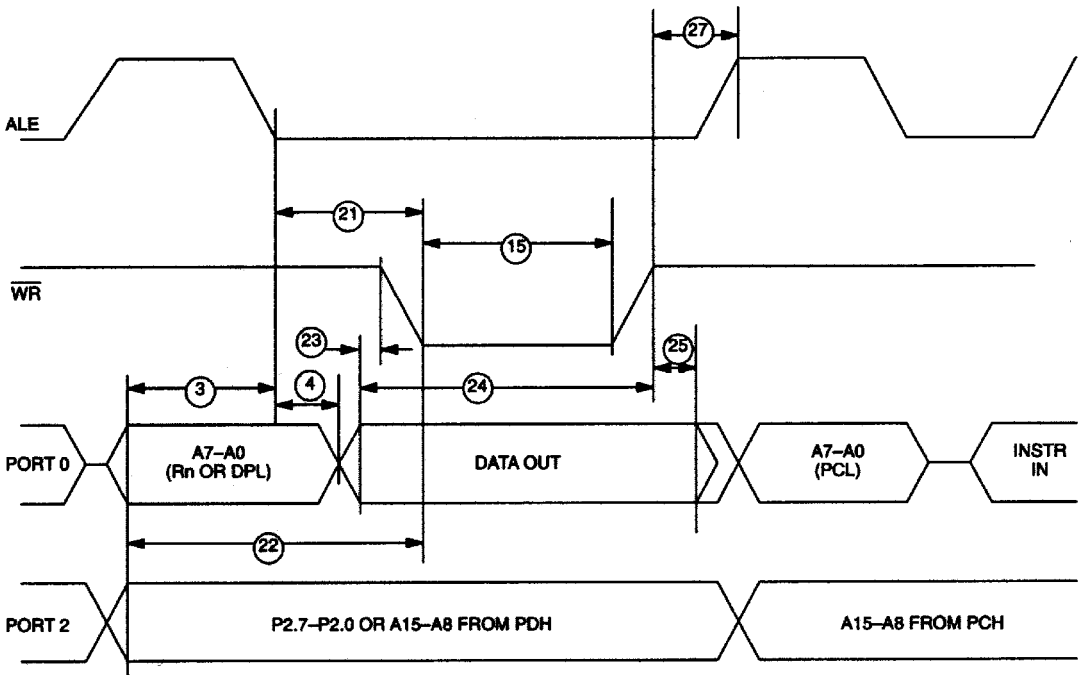


Figure 2. Expanded Data Memory Write Cycle

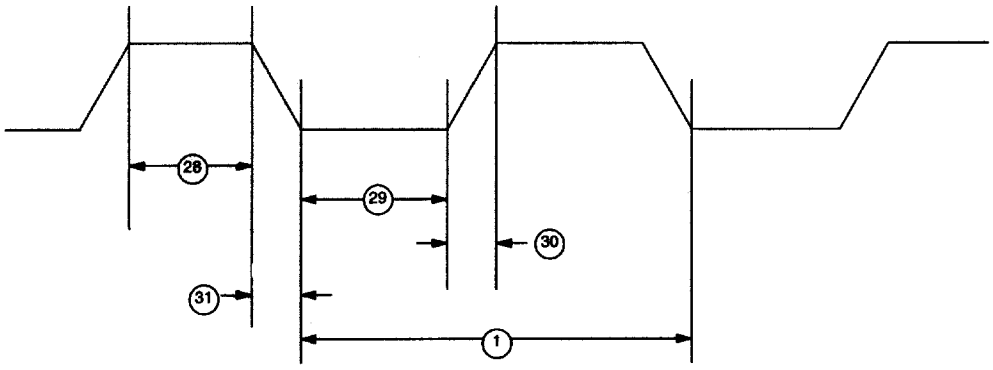


AC CHARACTERISTICS—EXTERNAL CLOCK DRIVE

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

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

Figure 3. External Clock Timing

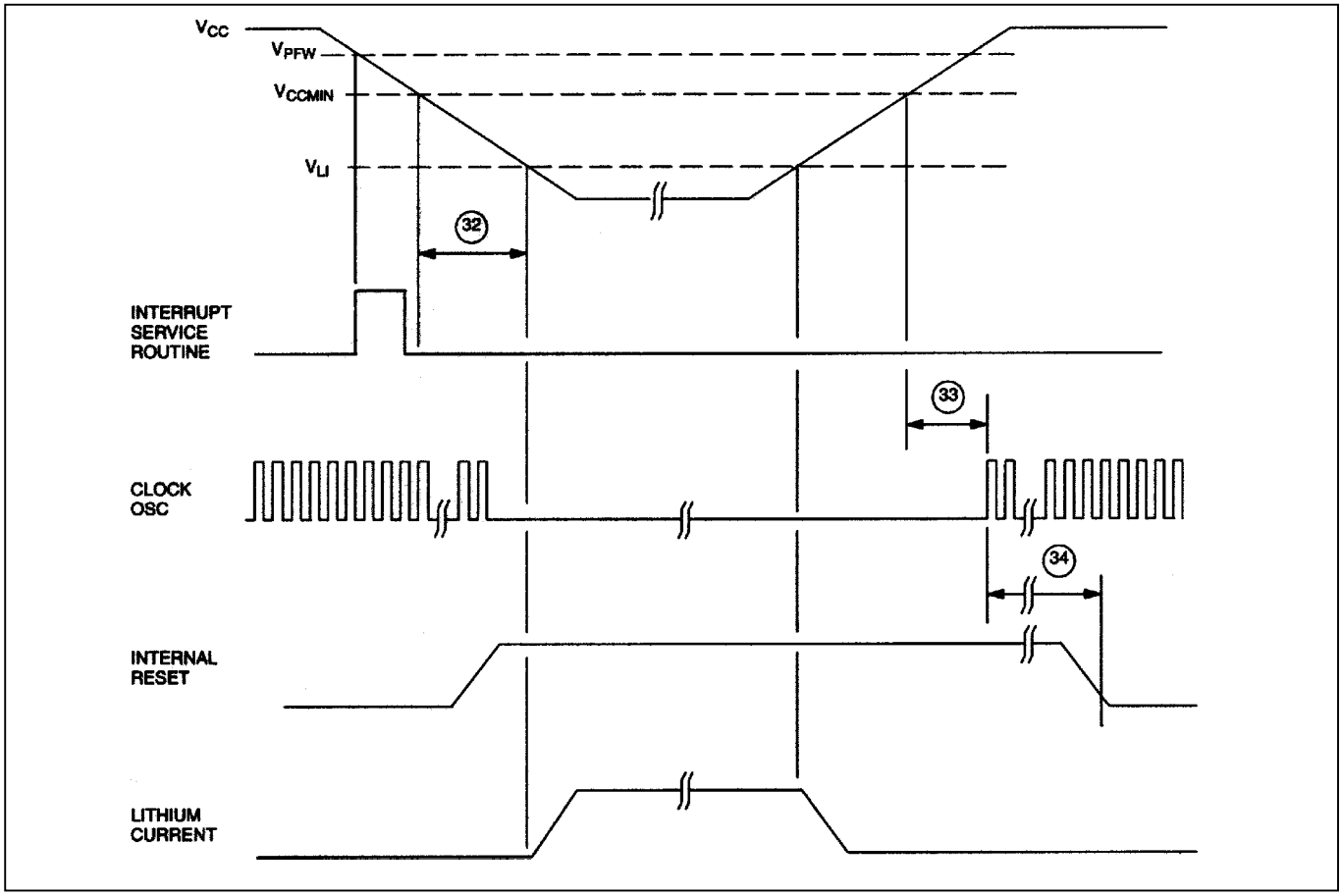


AC CHARACTERISTICS—POWER CYCLE TIME

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

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
32	Slew Rate from V_{CCMIN} to V_{LI}	t_F	130		µs
33	Crystal Startup Time	t_{CSU}		(Note 9)	
34	Power-on Reset Delay	t_{POR}		21504	t_{CLK}

Figure 4. Power Cycle Timing

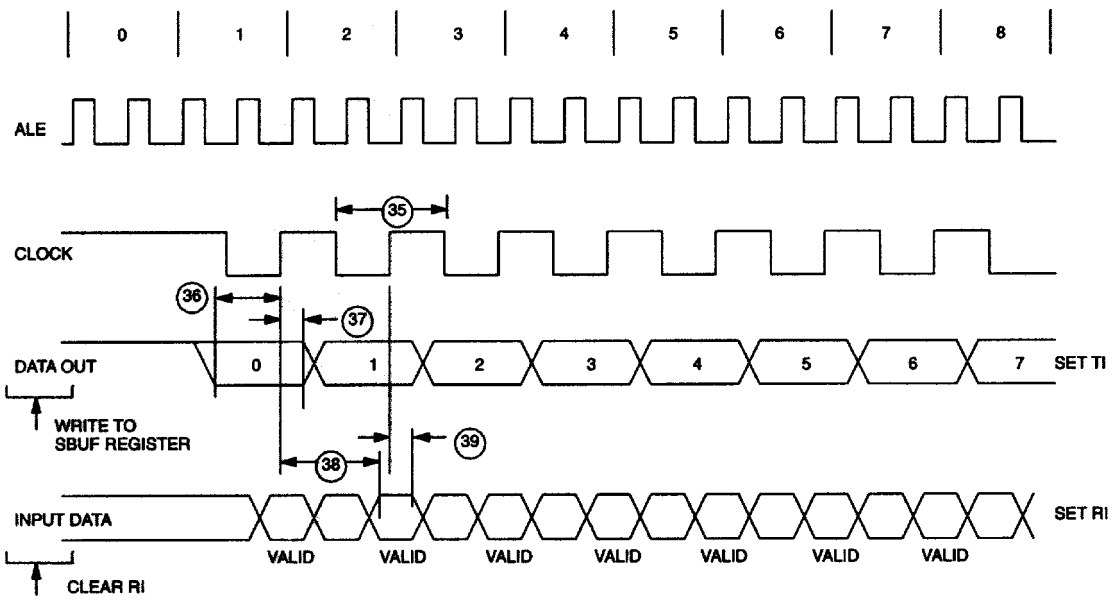


AC CHARACTERISTICS—SERIAL PORT TIMING, MODE 0

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

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

Figure 5. Serial Port Timing, Mode 0

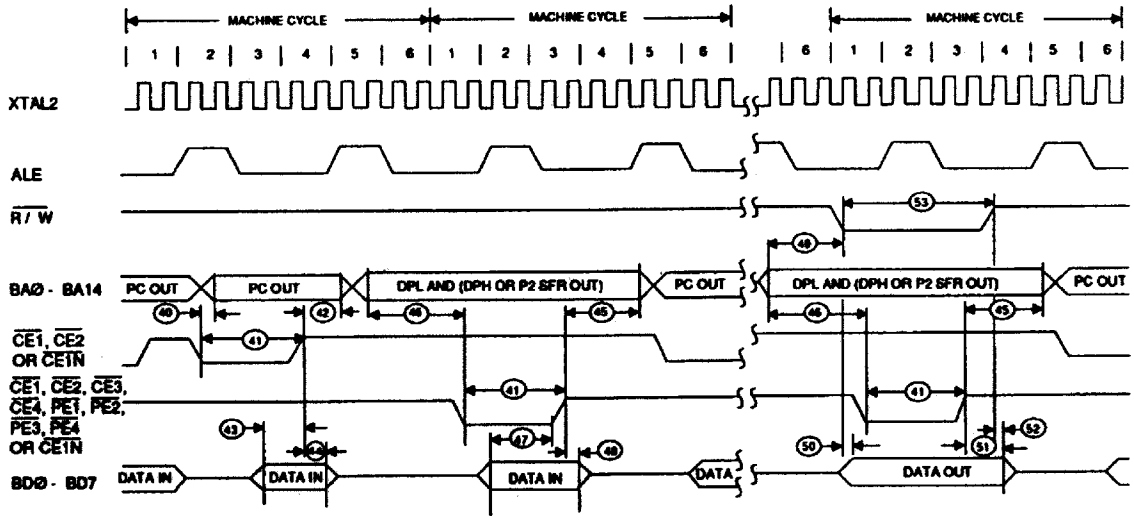


AC CHARACTERISTICS—BYTE-WIDE ADDRESS/DATA BUS TIMING

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

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
40	Delay to Byte-Wide Address Valid from $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ Low During Op Code Fetch	t_{CE1LPA}		30	ns
41	Pulse Width of $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$	t_{CEPW}	$4t_{CLK}$ - 35		ns
42	Byte-Wide Address Hold After $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{CE1HPA}	$2t_{CLK}$ - 20		ns
43	Byte-Wide Data Setup to $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{OVCE1H}	$1t_{CLK}$ + 40		ns
44	Byte-Wide Data Hold After $\overline{CE1}$, $\overline{CE2}$, or $\overline{CE1N}$ High During Op Code Fetch	t_{CE1HOV}	0		ns
45	Byte-Wide Address Hold After $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$ High During MOVX	t_{CEHDA}	$4t_{CLK}$ - 30		ns
46	Delay from Byte-Wide Address Valid $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$ Low During MOVX	t_{CELDA}	$4t_{CLK}$ - 35		ns
47	Byte-Wide Data Setup to $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$ High During MOVX (Read)	t_{DACEH}	$1t_{CLK}$ + 40		ns
48	Byte-Wide Data Hold After $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$ High During MOVX (Read)	t_{CEHDV}	0		ns
49	Byte-Wide Address Valid to R/$\overline{W}$ Active During MOVX (Write)	t_{AVRWL}	$3t_{CLK}$ - 35		ns
50	Delay from R/$\overline{W}$ Low to Valid Data Out During MOVX (Write)	t_{RWLDV}	20		ns
51	Valid Data Out Hold Time from $\overline{CE}$1–4, $\overline{PE}$1–4, or $\overline{CE1N}$ High	t_{CEHDV}	$1t_{CLK}$ - 15		ns
52	Valid Data Out Hold Time from R/$\overline{W}$ High	t_{RWHDV}	0		ns
53	Write Pulse Width (R/$\overline{W}$ Low Time)	t_{RWLPW}	$6t_{CLK}$ - 20		ns

Figure 6. Byte-Wide Bus Timing



RPC AC CHARACTERISTICS, DBB READ

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

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
54	$\overline{CS}$, A_0 Setup to $\overline{RD}$	t_{AR}	0		ns
55	$\overline{CS}$, A_0 Hold After $\overline{RD}$	t_{RA}	0		ns
56	$\overline{RD}$ Pulse Width	t_{RR}	160		ns
57	$\overline{CS}$, A_0 to Data Out Delay	t_{AD}		130	ns
58	$\overline{RD}$ to Data Out Delay	t_{RD}	0	130	ns
59	$\overline{RD}$ 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
60	$\overline{CS}$, A_0 Setup to $\overline{WR}$	t_{AW}	0		ns
61A	$\overline{CS}$, Hold After $\overline{WR}$	t_{WA}	0		ns
61B	A_0, Hold After $\overline{WR}$	t_{WA}	20		ns
62	$\overline{WR}$ Pulse Width	t_{WW}	160		ns
63	Data Setup to $\overline{WR}$	t_{DW}	130		ns
64	Data Hold After $\overline{WR}$	t_{WD}	20		ns

AC CHARACTERISTICS, DMA

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

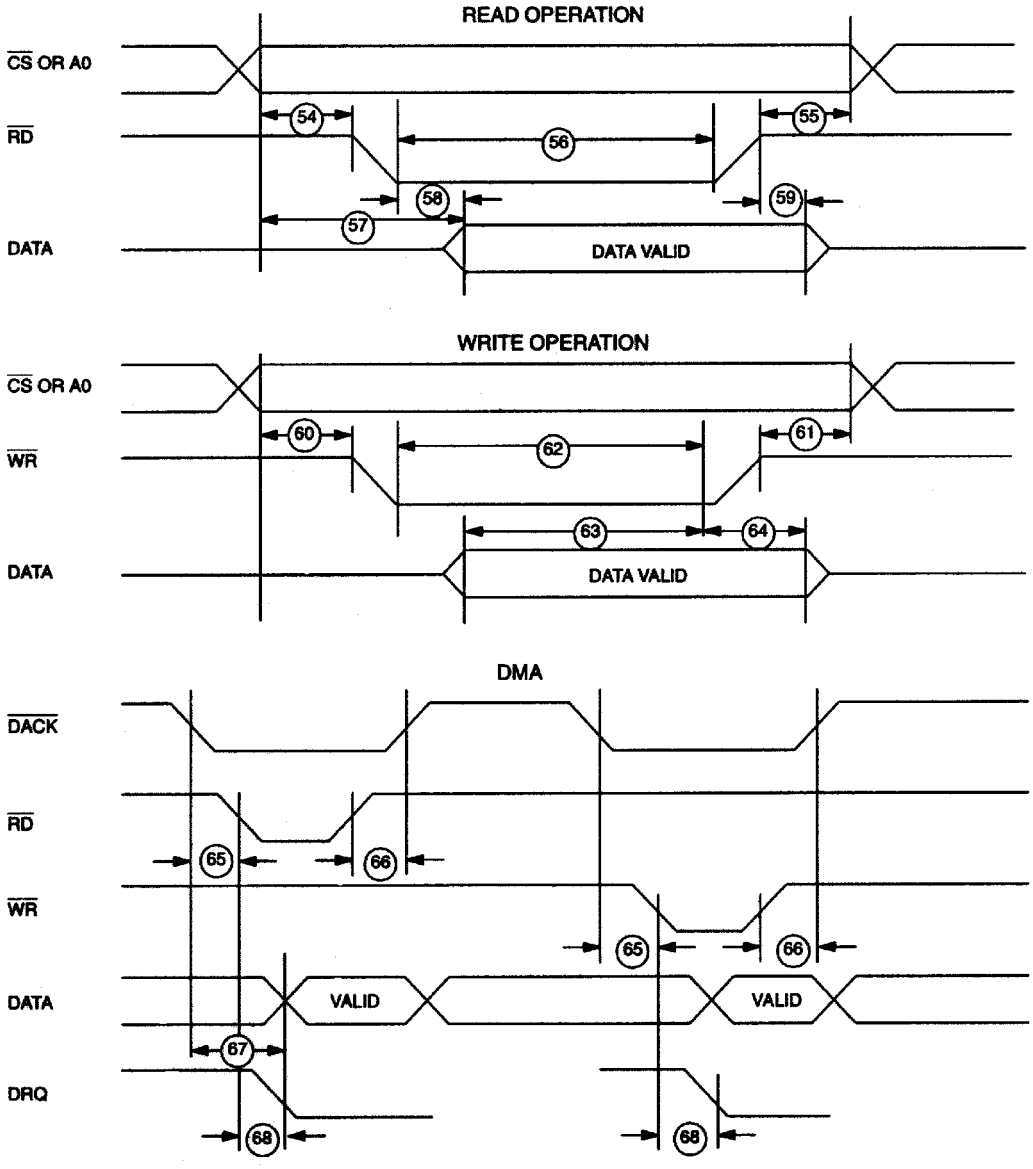
#	PARAMETER	SYMBOL	MIN	MAX	UNITS
65	$\overline{DACK}$ to $\overline{WR}$ or $\overline{RD}$	t_{ACC}	0		ns
66	$\overline{RD}$ or $\overline{WR}$ to $\overline{DACK}$	t_{CAC}	0		ns
67	$\overline{DACK}$ to Data Valid	t_{ACD}	0	130	ns
68	$\overline{RD}$ or $\overline{WR}$ to DRQ Cleared	t_{CRQ}		110	ns

AC CHARACTERISTICS, $\overline{PROG}$

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

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
69	$\overline{PROG}$ Low to Active	t_{PRA}	48		CLKS
70	$\overline{PROG}$ High to Inactive	t_{PRI}	48		CLKS

Figure 7. RPC Timing Mode



All parameters apply to both commercial and industrial temperature operation unless otherwise noted.

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} = 10 ns, V_{IL} = 0.5V; XTAL2 disconnected; RST = PORT0 = 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; PORT0 = V_{CC}, RST = MSEL = V_{SS}.
Note 4: Stop mode I_{STOP} is measured with all output pins disconnected; PORT0 = 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.
Note 6: I_{CCO1} is the maximum average operating current that can be drawn from V_{CCO} in normal operation.
Note 7: I_{LI} is the current drawn from V_{LI} input when V_{CC} = 0V and V_{CCO} is disconnected. Battery-backed mode is 2.5V ≤ V_{BAT} ≤ 4.0; V_{CC} ≤ V_{BAT}; V_{SDI} should be ≤ V_{ILS} for I_{BAT} max.
Note 8: V_{CCO2} is measured with V_{CC} < V_{LI}, and a maximum load of 10 µA on V_{CCO}.
Note 9: 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.
Note 10: 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 11: V_{IHS} minimum is 2.0V or V_{CCO}, whichever is lower.
Note 12: This parameter applies to industrial temperature operation.
Note 13: $\overline{PF}$ pin operation is specified with V_{BAT} ≥ 3.0V.

PIN DESCRIPTION

PIN	NAME	FUNCTION
11, 9, 7, 5, 1, 79, 77, 75	P0.0–P0.7	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.
15, 17, 19, 21, 25, 27, 29, 31	P1.0–P1.7	General-Purpose I/O Port 1
49, 50, 51, 56, 58, 60, 64, 66	P2.0–P2.7	General-Purpose I/O Port 2. Also serves as the MSB of the expanded address bus.
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 $\overline{\text{INT0}}$	General-Purpose I/O Port Pin 3.2. Also serves as the active-low external interrupt 0.
40	P3.3 $\overline{\text{INT1}}$	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 $\overline{\text{WR}}$	General-Purpose I/O Port Pin. Also serves as the write strobe for Expanded bus operation.
46	P3.7 $\overline{\text{RD}}$	General-Purpose I/O Port Pin. Also serves as the read strobe for Expanded bus operation.
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.
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.
47, 48	XTAL2, XTAL1	XTAL1, XTAL 2. Used to connect an external crystal to the internal oscillator. XTAL1 is the input to an inverting amplifier and XTAL2 is the output.
52	GND	Logic Ground
13	V_{CC}	V_{CC} - +5V
12	V_{CCO}	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}, the V_{CCO} switches to the V_{LI} source. V_{CCO} should be connected to the V_{CC} pin of an SRAM.
54	VLI	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.
16, 8, 18, 80, 76, 4, 6, 20, 24, 26, 28, 30, 33, 35, 37	BA14–0	Byte-Wide Address Bus Bits 14–0. This bus is combined with the nonmultiplexed data bus (BD7–0) to access NV SRAM. Decoding is performed using $\overline{\text{CE1}}$ through $\overline{\text{CE4}}$. Therefore, BA15 is not actually needed. Read/write access is controlled by R/$\overline{\text{W}}$. BA14–0 connect directly to an 8k, 32k, or 128k SRAM. If an 8k RAM is used, BA13 and BA14 are unconnected. If a 128k SRAM is used, the micro converts $\overline{\text{CE2}}$ and $\overline{\text{CE3}}$ to serve as A16 and A15, respectively.
71, 69, 67, 65, 61, 59, 57, 55	BD7–0	Byte-Wide Data Bus Bits 7–0. This 8-bit bidirectional bus is combined with the nonmultiplexed address bus (BA14–0) to access NV SRAM. Decoding is performed on $\overline{\text{CE1}}$ and $\overline{\text{CE2}}$. Read/write access is controlled by R/$\overline{\text{W}}$. D7–0 connect directly to an SRAM, and optionally to a real-time clock or other peripheral.
10	R/$\overline{\text{W}}$	Read/Write. 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	$\overline{\text{CE1}}$	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. $\overline{\text{CE1}}$ is lithium-backed. It remains in a logic-high inactive state when V_{CC} falls below V_{LI}.
2	$\overline{\text{CE2}}$	Chip Enable 2. This chip enable is provided to access a second 32k block of memory. It connects to the chip-enable input of one SRAM. When MSEL = 0, the micro converts $\overline{\text{CE2}}$ into A16 for a 128k x 8 SRAM. $\overline{\text{CE2}}$ is lithium-backed and remains at a logic high when V_{CC} falls below V_{LI}.
63	$\overline{\text{CE3}}$	Chip Enable 3. This chip enable is provided to access a third 32k block of memory. It connects to the chip enable input of one SRAM. When MSEL = 0, the micro converts $\overline{\text{CE3}}$

PIN	NAME	FUNCTION
		into A15 for a 128k x 8 SRAM. $\overline{CE3}$ is lithium-backed and remains at a logic high when V_{CC} falls below V_{LI}.
62	$\overline{CE4}$	Chip Enable 4. This chip enable is provided to access a fourth 32k 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	$\overline{PE1}$	Peripheral Enable 1. Accesses data memory between addresses 0000h and 3FFFh when the PES bit is set to a logic 1. Commonly used to chip enable a byte-wide real-time clock such as the DS1283. $\overline{PE1}$ is lithium-backed and will remain at a logic high when V_{CC} falls below V_{LI}. Connect $\overline{PE1}$ to battery-backed functions only.
3	$\overline{PE2}$	Peripheral Enable 2. Accesses data memory between addresses 4000h and 7FFFh when the PES bit is set to a logic 1. $\overline{PE2}$ is lithium-backed and will remain at a logic high when V_{CC} falls below V_{LI}. Connect $\overline{PE2}$ to battery-backed functions only.
22	$\overline{PE3}$	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 will need additional circuitry to maintain the chip enable in an inactive state when $V_{CC} < V_{LI}$.
23	$\overline{PE4}$	Peripheral Enable 4. Accesses data memory between addresses C000h and FFFFh when the PES bit is set to a 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 will need additional circuitry to maintain the chip enable in an inactive state when $V_{CC} < V_{LI}$.
32	$\overline{PROG}$	Invokes the bootstrap loader on a falling edge. This signal should be debounced so that only one edge is detected. If connected to ground, the micro enters bootstrap loading on power-up. This signal is pulled up internally.
42	$\overline{VRST}$	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 micro is in a reset state. When this occurs, the DS5002FP drives this pin to a logic 0. Because the micro 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	$\overline{PF}$	This output goes to a logic 0 to indicate that the micro has switched to lithium backup. This corresponds to $V_{CC} < V_{LI}$. Because the micro 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 non-battery-backed functions.
14	MSEL	Memory Select. This signal controls the memory size selection. When MSEL = +5V, the DS5002FP expects to use 32k x 8 SRAMs. When MSEL = 0V, the DS5002FP expects to use a 128k x 8 SRAM. MSEL must be connected regardless of partition, mode, etc.
53	SDI	Self-Destruct Input. An active high on this pin causes an unlock procedure. This results in the destruction of Vector RAM, Encryption Keys, and the loss of power from V_{CCO}. This pin should be grounded if not used.
72	$\overline{CE1N}$	This is a non-battery-backed version of $\overline{CE1}$. It is not generally useful since the DS5002FP cannot be used with EPROM due to its encryption.
73	N.C.	No Connect

DETAILED DESCRIPTION

The DS5002FP implements a security system that is an improved version of its predecessor, the DS5000FP. Like the DS5000FP, the DS5002FP loads and executes application software in encrypted form. Up to 128kB of standard SRAM can be accessed by its byte-wide bus. This RAM is converted by the DS5002FP into lithium-backed nonvolatile storage for program and data. Data is maintained for over 10 years at room temperature with a very small lithium cell. As a result, the contents of the RAM 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 RAM useless.

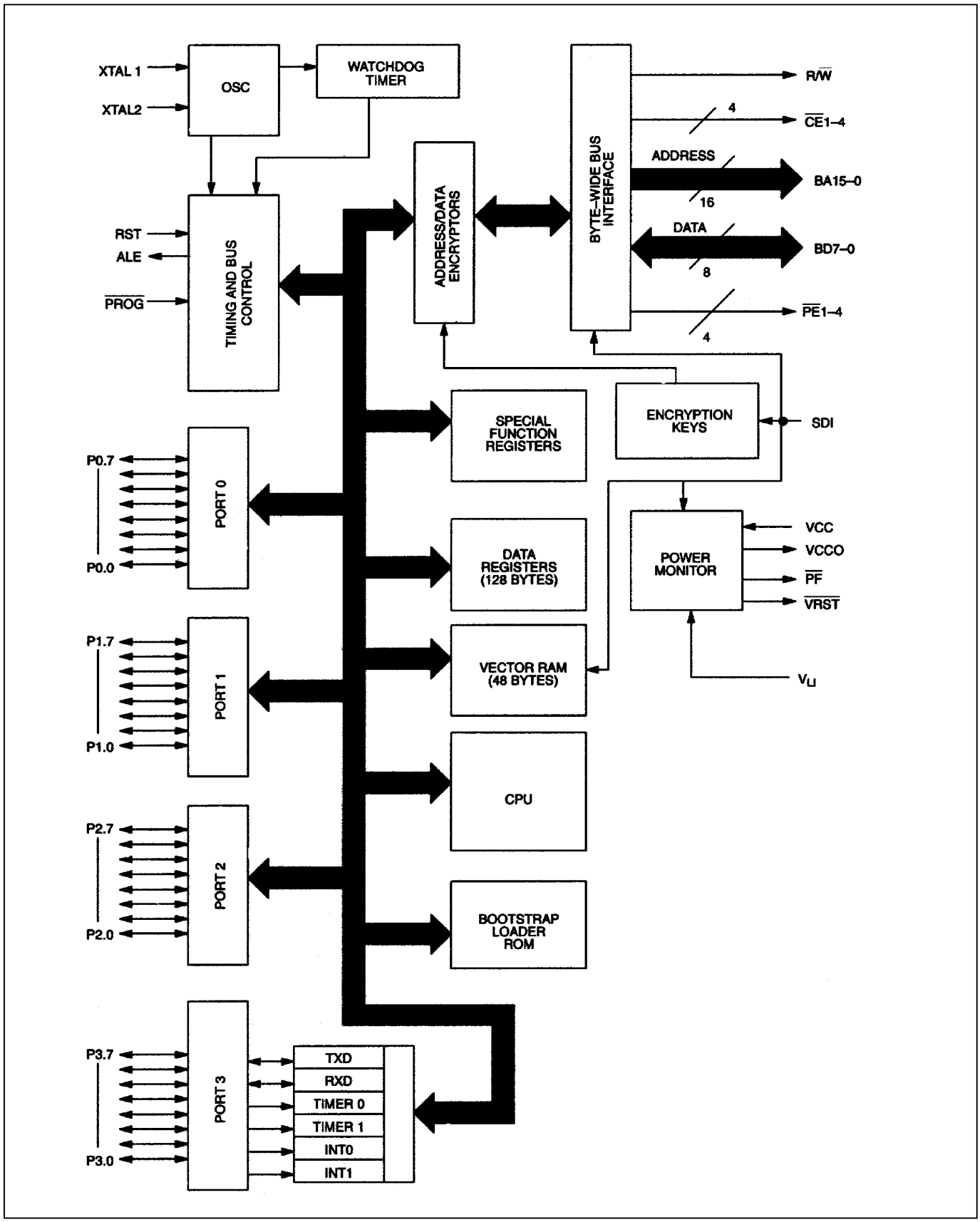
The secure microprocessor chip offers a number of major enhancements to the software security implemented in the previous generation DS5000FP. First, the DS5002FP provides a stronger software encryption algorithm that incorporates elements of DES encryption. Second, the encryption is based on a 64-bit key word, as compared to the DS5000FP's 40-bit key. Third, the key can only be loaded from an on-chip true random-number generator. As a result, the true key value is never known by the user. Fourth, 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 RAM area. Fifth, an optional top-coating of the die prevents access of information using microprobing techniques. Finally, customer-specific versions of the DS5002FP are available that incorporate a one-of-a-kind encryption algorithm.

When implemented as a part of a secure system design, a system based on the DS5002FP can typically provide a level of security that requires more time and resources to defeat than it is worth to unauthorized individuals who have reason to try. For a user who wants a preconstructed module using the DS5002FP, RAM, lithium cell, and a real-time clock, the DS2252T is available and described in a separate data sheet.

BLOCK DIAGRAM

Figure 8 is a block diagram illustrating the internal architecture of the DS5002FP. The DS5002FP is a secure implementation of the DS5001FP 128k soft microprocessor chip. As a result, it operates in an identical fashion to the DS5001FP, except where indicated. See the DS5001FP data sheet for operating details.

Figure 8. Block Diagram



SECURE OPERATION OVERVIEW

The DS5002FP 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 NV RAM. Loading an application program in this manner is performed by the bootstrap loader using the general sequence described below:

1) Clear security lock.
2) Set memory map configuration as for DS5001FP
3) Load application software
4) Set security lock
5) Exit loader

Loading of application software into the program/data RAM is performed while the DS5002FP is in its bootstrap load mode. Loading is only possible when the security lock is clear. If the security lock has previously set, then it must be cleared by issuing the "Z" command from the bootstrap loader. Resetting the security lock instantly clears the previous key word and the contents of the Vector RAM. In addition, the bootstrap ROM writes 0's into the first 32k of external RAM.

The user's application software is loaded into external CMOS SRAM by the "L" command in "scrambled" form through on-chip encryptor circuits. Each external RAM 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 RAM memory. The contents of the program/data RAM are also encrypted. Each byte in RAM 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 RAM is dependent on an on-chip 64-bit key word. The key is loaded 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 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 RAM contents results in the erasure of the key word as well as the RAM contents.

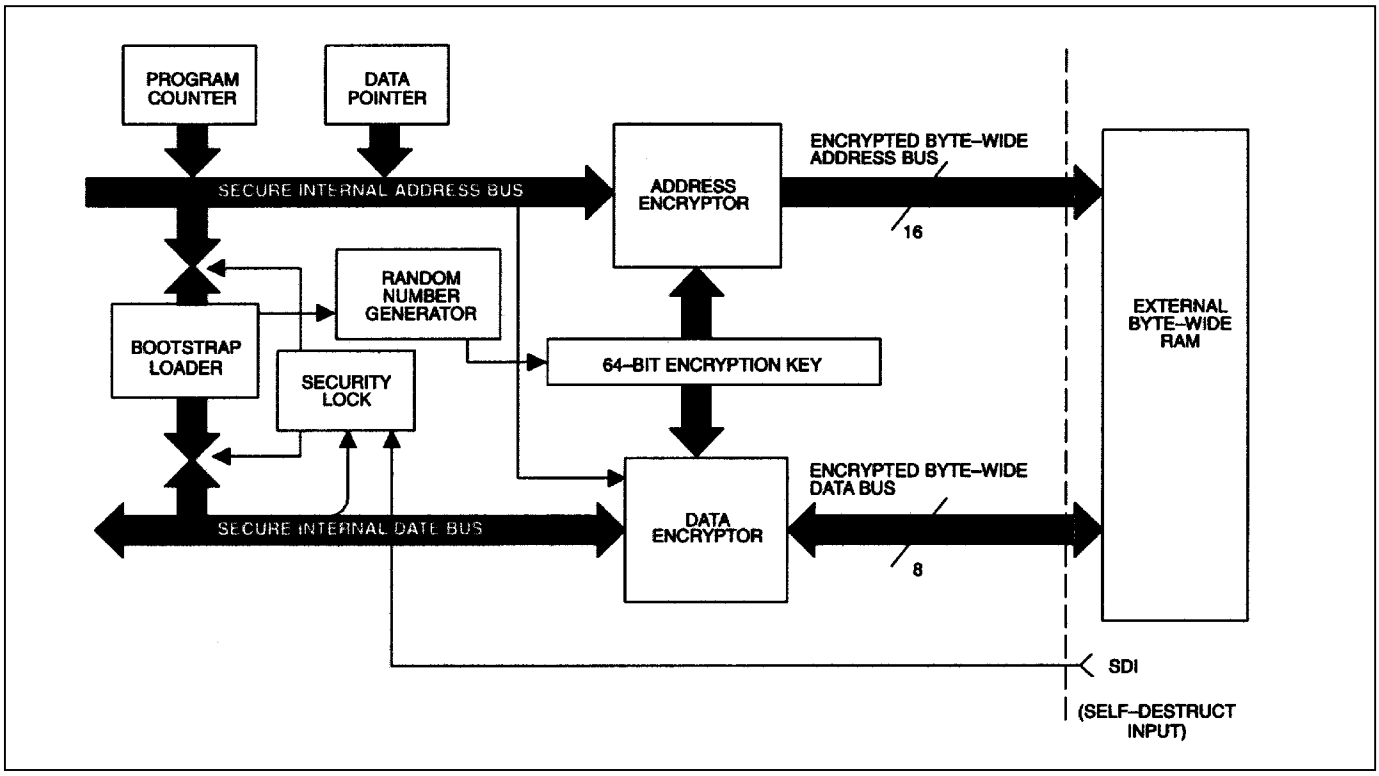
During execution of the application software, logical addresses on the DS5002FP that are generated from the program counter or data pointer registers are encrypted before they are presented on the byte-wide address bus. Op codes and data are read back and decrypted before they are operated on by the CPU. Similarly, data values written to the external nonvolatile RAM 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 as compared to the non-encrypted DS5001FP or 8051 running at the same clock rate. As a result, operation of the encryptor circuitry is transparent to the application software.

Unlike the DS5000FP, the DS5002FP chip's security feature is always enabled.

SECURITY CIRCUITRY

The on-chip functions associated with the DS5002FP's software security feature are depicted in Figure 9. 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 which is contained in the Encryption Key registers. Both the encryptors operate during loading of the application software and also during its execution.

Figure 9. Security Circuitry



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 RAM. 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 RAM 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 RAM. The encryption algorithm is repeatable, such that for a given data value, encryption key value, and logical address the encrypted byte will always be 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.

When the application software is executed, the internal CPU of the DS5002FP operates as normal. Logical addresses are calculated for op code fetch cycles and also data read and write operations. The DS5002FP has the ability to 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, it is also encrypted when it is written to the external program/data RAM, and is restored to its original value when it is read back.

When an application program is stored in the format described above, 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 in itself 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 DS5000FP, the DS5002FP generates a “dummy” read access cycle to non-sequential addresses in external RAM memory whenever time is available during program execution. This action has the affect of further complicating the task of determining the normal flow of program execution. During these pseudorandom dummy cycles, the RAM 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 DS5002FP incorporates a proprietary algorithm implemented in hardware, which performs the scrambling of address and data on the byte-wide bus to the SRAM. This algorithm has been greatly strengthened with respect to its DS5000FP predecessor. Improvements include:

1) 64-bit encryption key
2) Incorporation of DES-like operations to provide a greater degree of nonlinearity
3) Customizable encryption

The encryption circuitry uses a 64-bit key value (compared to the DS5000FP’s 40-bit key), which is stored on the DS5002FP die and protected by the Security Lock function described below. In addition, the algorithm has been strengthened to incorporate certain operations used in DES encryption, so that the encryption of both the addresses and data is highly nonlinear. Unlike the DS5000FP, the encryption circuitry in the DS5002FP is always enabled.

Dallas Semiconductor can customize the encryption circuitry by laser programming the die to insure that a unique encryption algorithm is delivered to the customer. In addition, the customer-specific version can be branded as specified by the customer. Please contact Dallas Semiconductor for ordering information of customer-specific versions.

ENCRYPTION KEY

As described above, the on-chip 64-bit encryption key is the basis of both the address and data encryptor circuits. The DS5002FP provides a key management system, which is greatly improved over the DS5000FP. The DS5002FP does not give the user the ability to select a key. Instead, when the loader is given certain commands, the key is set based on the value read from an on-chip hardware random number generator. This action is performed just prior to actually loading the code into the external RAM. 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 oscillator 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 DS5002FP. It is included in the architecture to help insure 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, then 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 RAM 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. Although it is very unlikely that an application program could be deciphered by observing vector address relationships, the vector RAM eliminates this possibility. Note that the dummy accesses mentioned above are conducted while fetching from vector RAM.

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

SECURITY LOCK

Once the application program has been loaded into the DS5002FP's NV 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 DS5002FP encryptor circuits.

Access to the NV RAM can only be regained by clearing the security lock by the "U" command in the bootstrap loader. This action triggers several events, which defeat tampering. First, the encryption key is instantaneously erased. Without the encryption key, the DS5002FP is no longer able to decrypt the contents of the RAM. 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 RAM area. Lastly, the loader creates and loads a new random key.

The Security Lock bit itself is constructed using a multiple-bit latch which is interlaced for self-destruct in the event of tampering. The lock is designed to set-up a "domino-effect" such that erasure of the bit will result 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 mentioned below.

SELF-DESTRUCT INPUT

The self-destruct input (SDI) pin is an active-high input that is used to reset the security lock in response to an external event. 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 described above for this action. In addition, power is momentarily removed from the byte-wide bus interface including the V_{CCO} pin, resulting in the loss of data in external RAM.

TOP LAYER COATING

The DS5002FPM 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 DS5002FP is performed by firmware within the on-chip bootstrap loader communicating with a PC by the on-chip serial port in a manner that is almost identical to that for the DS5001FP. The user should consult the DS5001FP data sheet as a basis of operational characteristics of this firmware. Certain differences in loading procedure exist in order to support the security feature. These differences are documented below. Table 1 summarizes the commands accepted by the bootstrap loader.

When the bootstrap loader is invoked, portions of the 128-byte scratchpad RAM area are automatically overwritten with 0's, and then used for variable storage for the bootstrap firmware. Also, a set of 8 bytes are generated using the random number generator circuitry and are saved as a potential word for the 64-bit encryption key.

Any read or write operation to the DS5002FP'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 NV RAM
D	Dump Intel Hex file
F	Fill program/data NV RAM
G	Get data from P1, P2, and P3
I	N/A on the DS5002FP
L	Load Intel Hex file
M	Toggle modem available bit
N	Set freshness seal—all program and data is lost
P	Put data into P0, P1, P2, and P3
R	Read status of NV SFRs (MCON, RPCTL, MSL, CALIB)
T	Trace (echo) incoming Intel Hex code
U	Clear Security Lock
V	Verify program/data NV RAM with incoming Intel Hex data
W	Write special function registers (MCON, RPCTL, MSL, CALIB)
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 result in the data loaded into the NV RAM in an encrypted form determined by the value of the newly generated key word. The subsequent execution of the Dump command *within the same bootstrap session* causes the contents of the encrypted RAM 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 RAM, and the CRC command returns the CRC value calculated from the true contents of the encrypted RAM. As long as any of the above commands are executed *within the same bootstrap session*, the loaded key value remains the same, and the contents of the encrypted program/data NV RAM 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 RAM contents is possible using any bootstrap command or by any other means.

INSTRUCTION SET

The DS5002FP 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 DS5002FP. A complete description of the instruction set and operation are provided in the *Secure Microcontroller User's Guide*.

Also note that the DS5002FP is embodied in the DS2252T module. The DS2252T combines the DS5002FP with between 32k and 128k of SRAM, a lithium cell, and a real-time clock. This is packaged in a 40-pin SIMM module.

MEMORY ORGANIZATION

Figure 10 illustrates the memory map accessed by the DS5002FP. The entire 64k of program and 64k 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 NV RAM is reached by the expanded bus on ports 0 and 2. An alternate configuration allows dynamic partitioning of a 64k space as shown in Figure 11. Selecting PES = 1 provides another 64k 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 10. Memory Map in Nonpartitionable Mode (PM = 1)

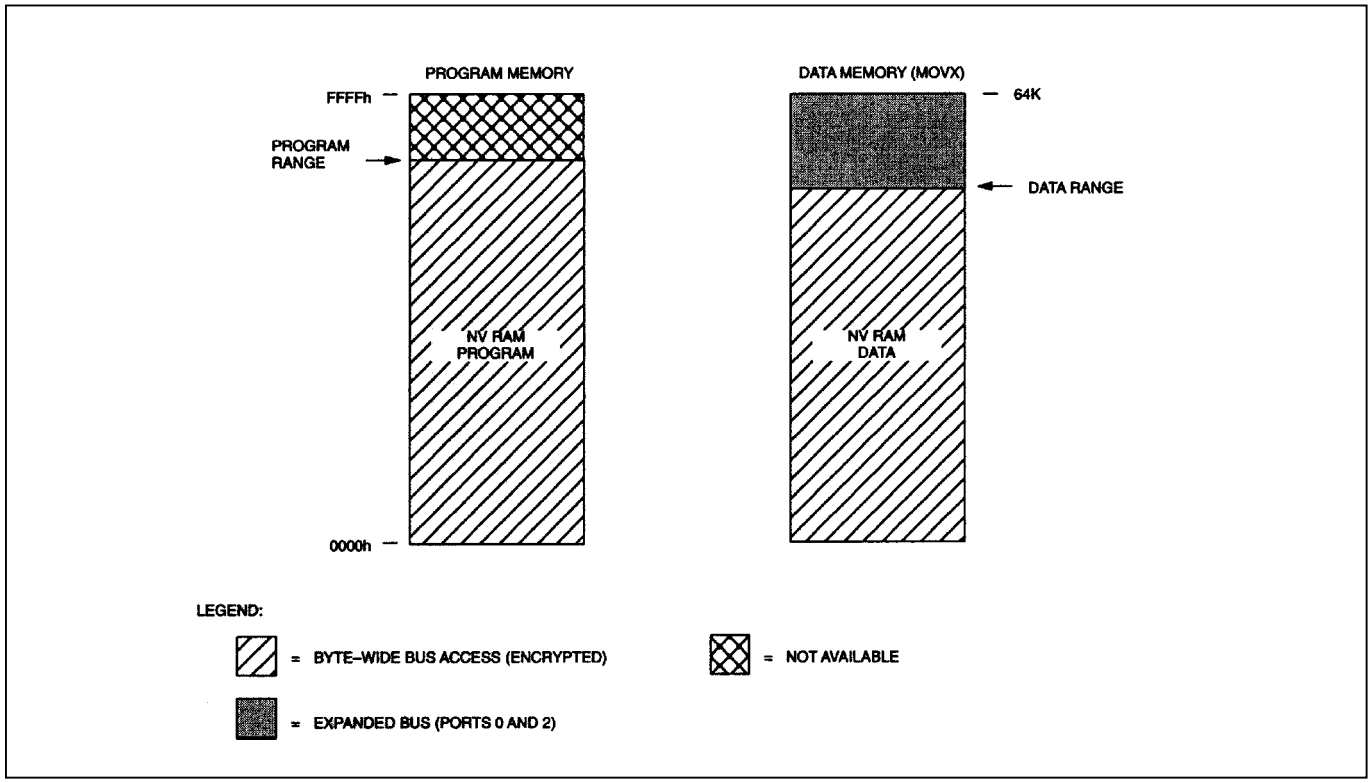


Figure 11. Memory Map In Partitionable Mode (PM = 0)

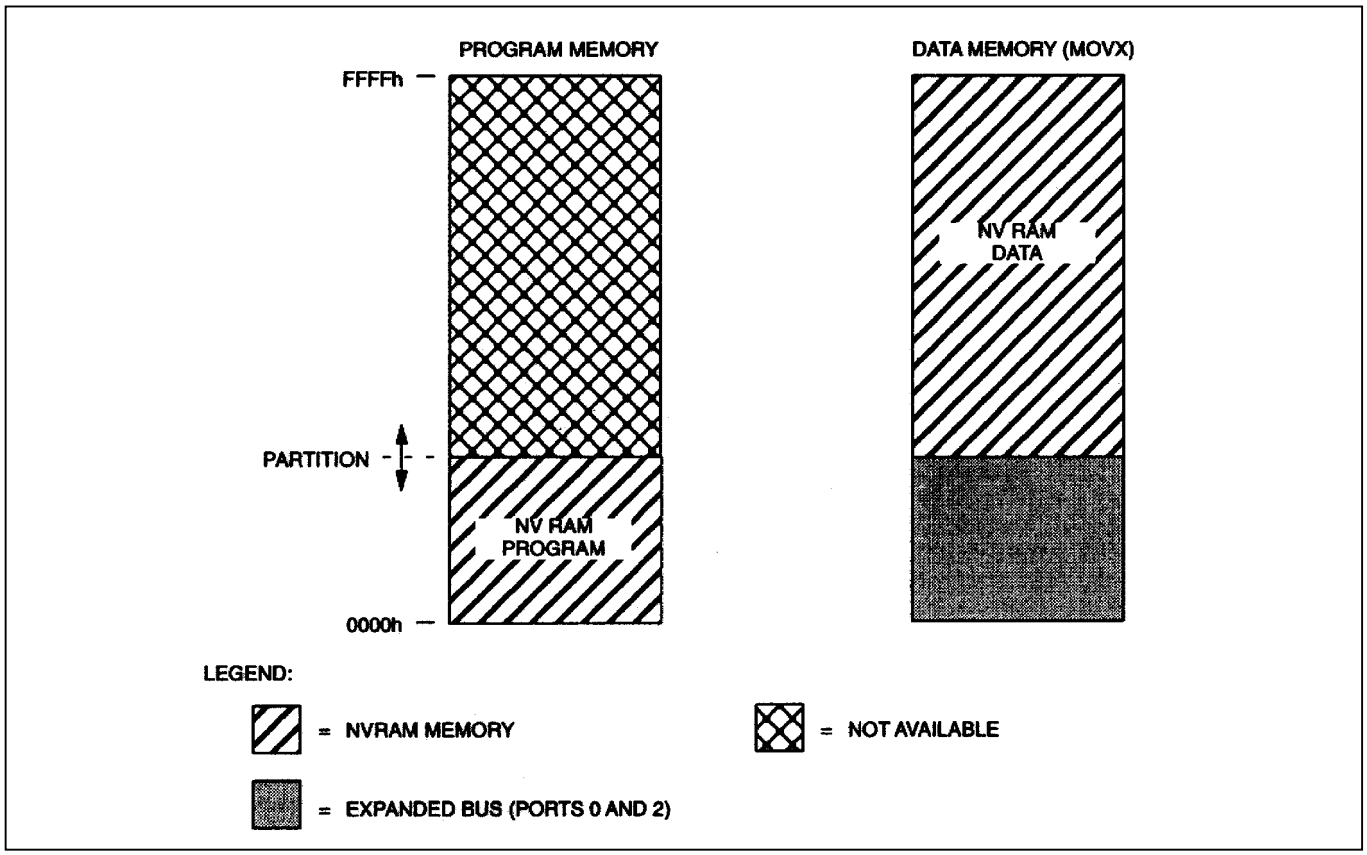


Figure 12. Memory Map with PES = 1

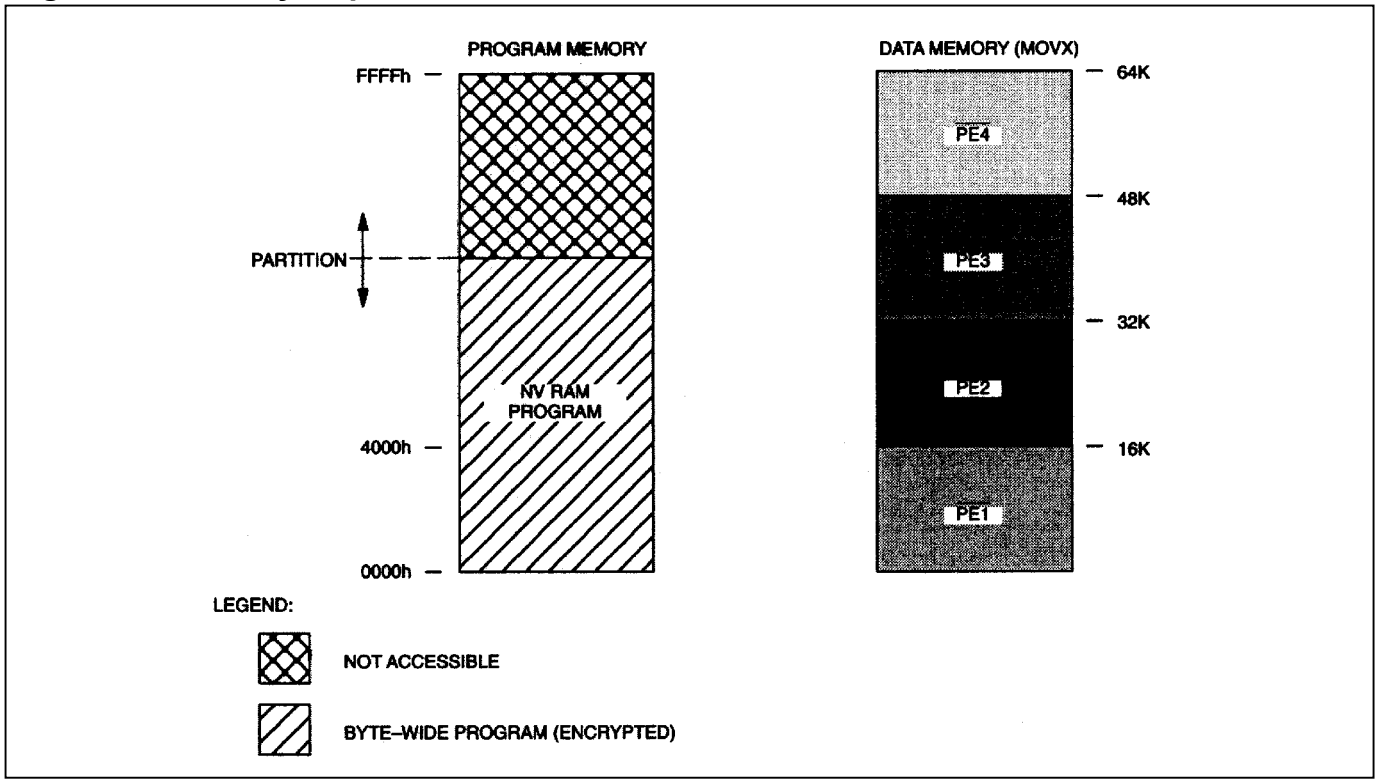


Figure 13 illustrates a typical memory connection for a system using a 128kB SRAM. Note that in this configuration, both program and data are stored in a common RAM chip. Figure 14 shows a similar system with using two 32kB SRAMs. The byte-wide address bus connects to the SRAM address lines. The bidirectional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

Figure 13. Connection to 128k x 8 SRAM

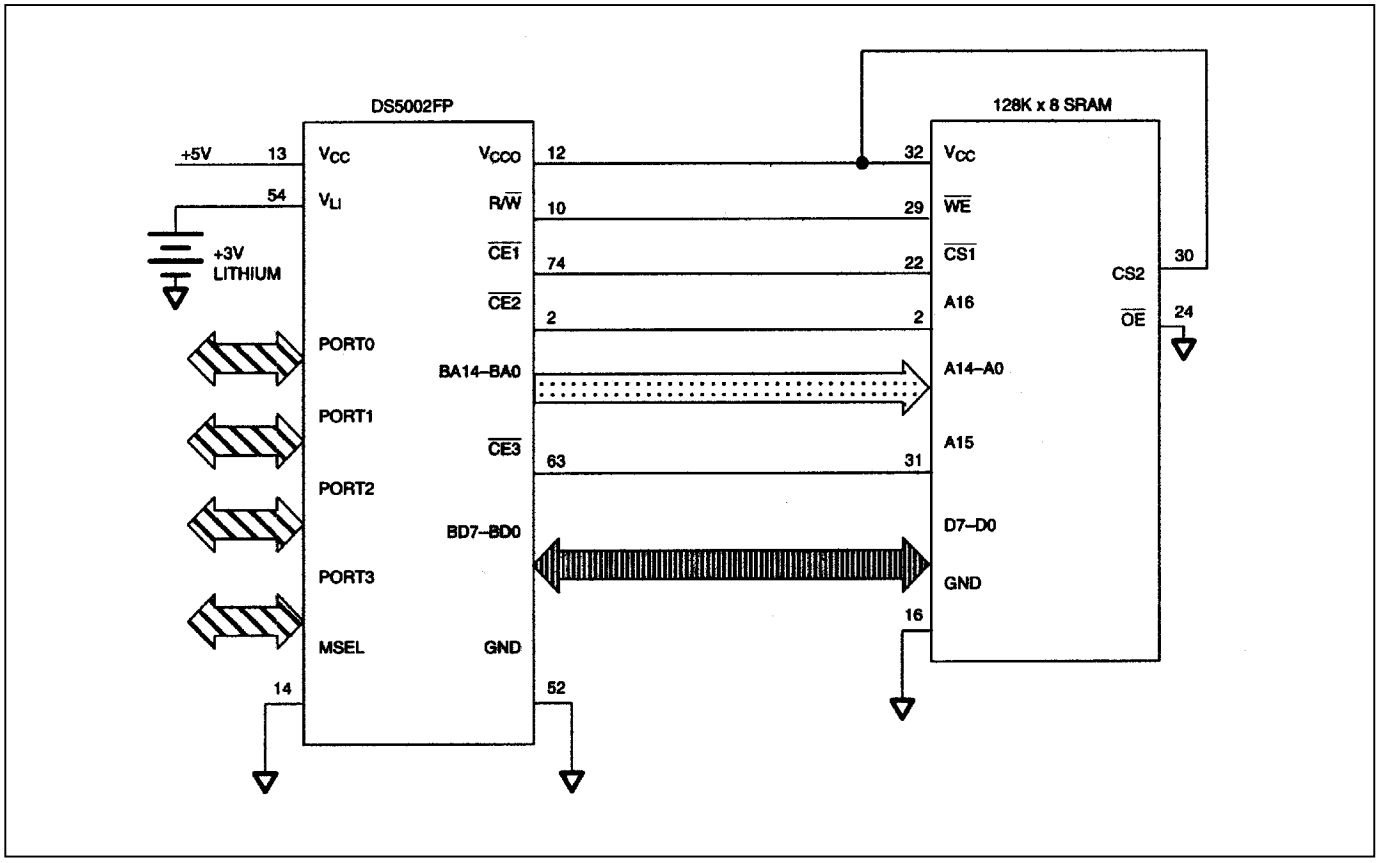
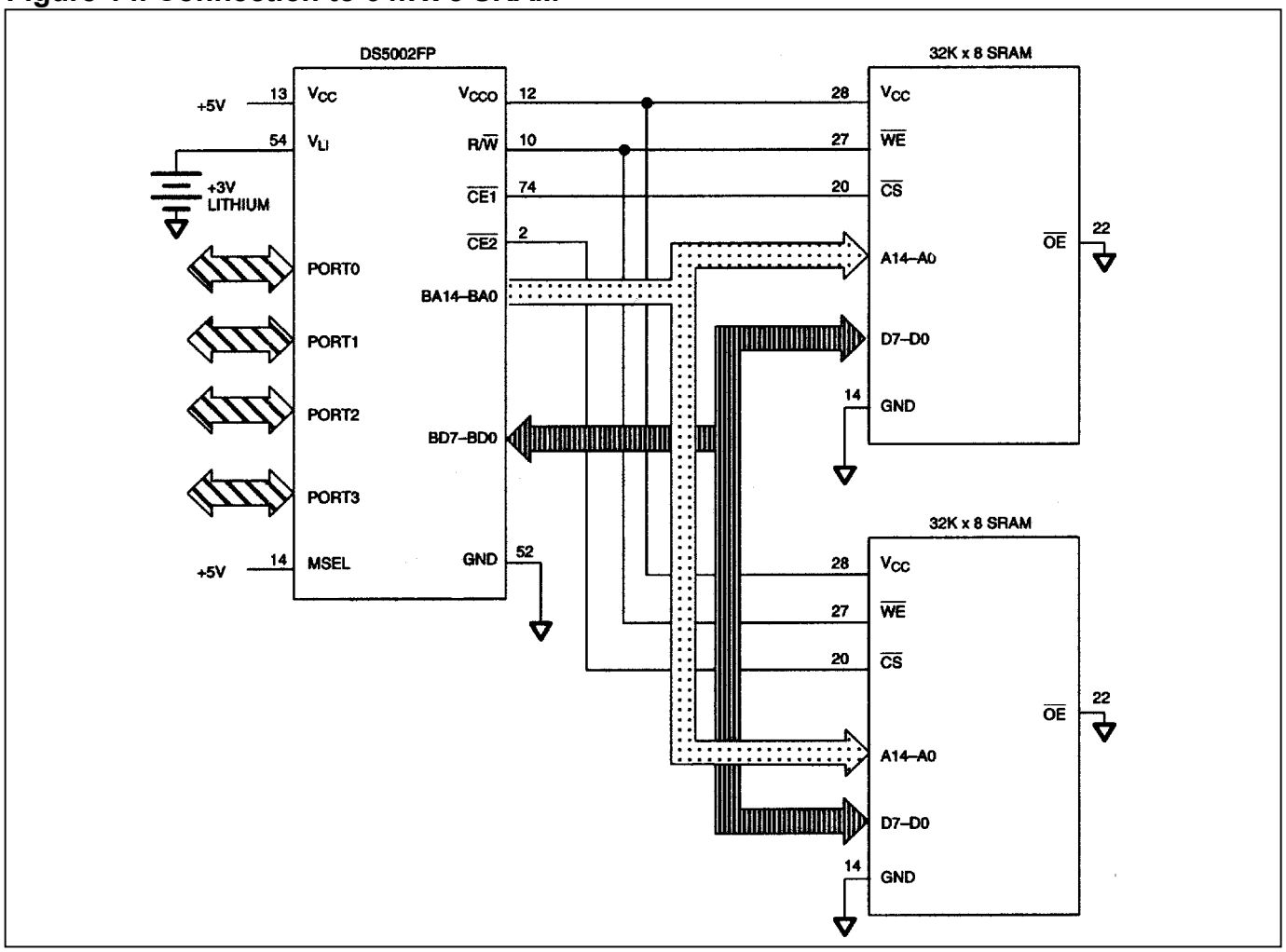


Figure 14. Connection to 64k x 8 SRAM



POWER MANAGEMENT

The DS5002FP 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 DS5002FP will perform an interrupt vector to location 2Bh if the power-fail warning was enabled. Full processor operation continues regardless. When power falls further to V_{CCMIN}, the DS5002FP 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 switch to the lithium cell for power. The majority of internal circuits will be disabled and the remaining nonvolatile states will be retained. Any devices connected V_{CCO} will be powered by the lithium cell at this time. V_{CCO} is at the lithium battery voltage minus approximately 0.45V (less a diode drop). This drop varies depending on the load. Low-power SRAMs should be used for this reason. When using the DS5002FP, the user must select the appropriate battery to match the RAM 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.

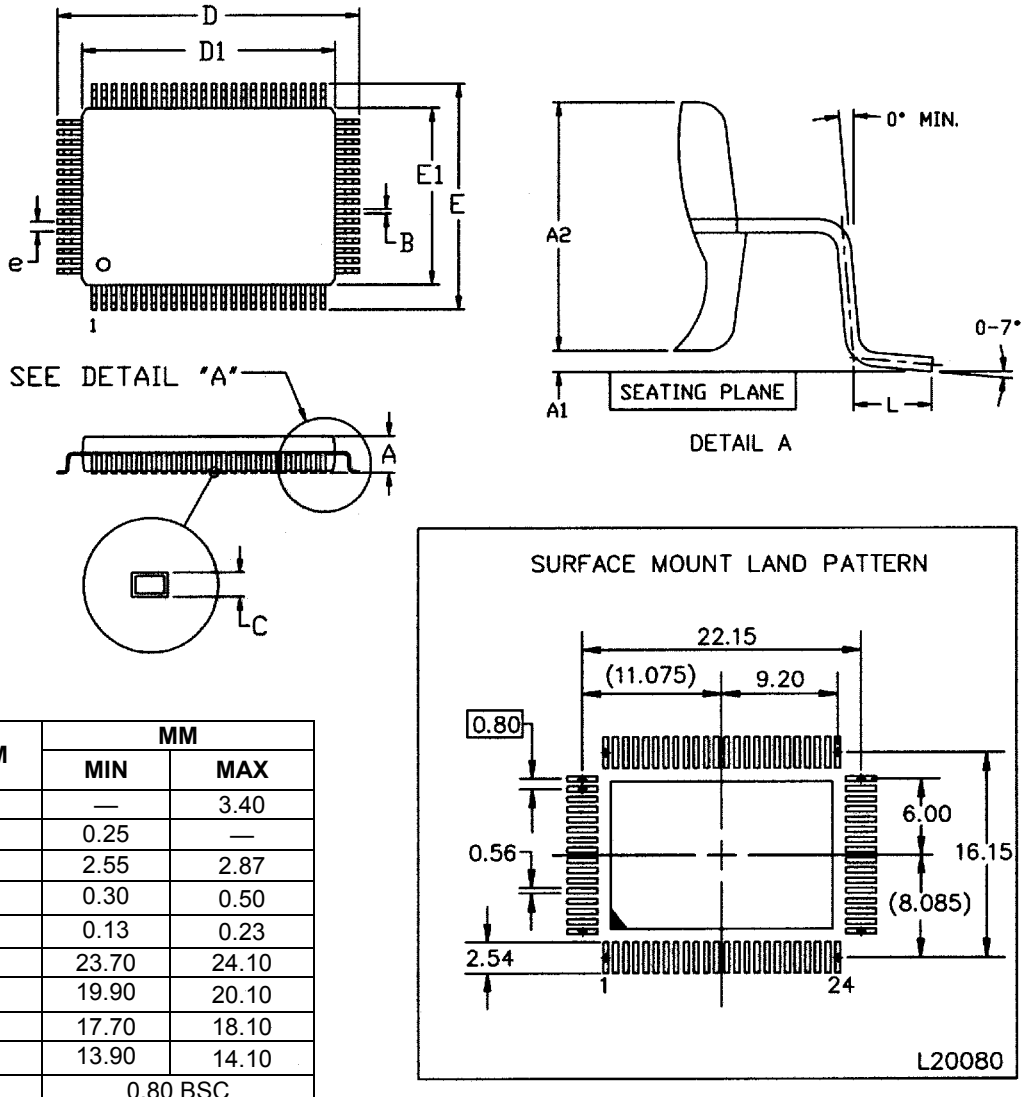
SELECTOR GUIDE

PART	TEMP RANGE	MAX CLOCK SPEED (MHz)	PIN-PACKAGE
DS5002FP-16	0°C to +70°C	16	80 QFP
DS5002FPM-16	0°C to +70°C**	16	80 QFP
DS5002FP-16N	-40°C to +85°C**	16	80 QFP
DS5002FMN-16	-40°C to +85°C	16	80 QFP

** *Internal Microprobe Shield*

PACKAGE INFORMATION

(The package drawing(s) in this data sheet may not reflect the most current specifications. For the latest package outline information, go to **www.maxim-ic.com/DallasPackInfo**.)



DIM	MM	
	MIN	MAX
A	—	3.40
A1	0.25	—
A2	2.55	2.87
B	0.30	0.50
C	0.13	0.23
D	23.70	24.10
D1	19.90	20.10
E	17.70	18.10
E1	13.90	14.10
e	0.80 BSC	
L	0.65	0.95

56-G4005-001

REVISION HISTORY

REVISION	DESCRIPTION
112795	Original release.
073096	Change V_{CC02} specification from V_{LI} - 0.5 to V_{LI} - 0.65 (PCN F62501). Update mechanical specifications.
111996	Change V_{CC01} from V_{CC} - 0.3 to V_{CC} - 0.35.
061297	$\overline{PF}$ signal moved from V_{OL2} test specification to V_{OL1}. PCN No. (D72502). AC characteristics for battery-backed SDI pulse specification added.
051499	Reduced absolute maximum voltage to V_{CC} + 0.5V. Added note clarifying storage temperature specification is for nonbattery-backed state. Deleted I_{BAT} specification (Duplicate of I_{LI} specification). Changed RRE min (industrial temp range) from 40kΩ to 30kΩ. Changed V_{PFW} max (industrial temp range) from 4.5V to 4.6V. Added industrial specification for I_{LI}. Reduced t_{CE1HOV} and t_{CEHDV} from 10ns to 0ns.
052599	Minor revisions and approval.
062102	Update V_{CCO} and I_{CCO1} specifications to reflect 0.45V internal voltage drop instead of 0.35V.
100102	Ordering information updated.
030403	Reset Trip Point in Stop Mode (DC Characteristics) with BAT = 3.0V was changed to 3.3V (original issue was 3.3V).