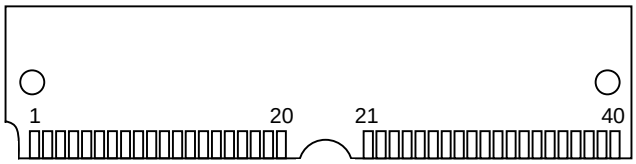
DS2252T
Secure Microcontroller Module

www.dalsemi.com

FEATURES

- 8051-compatible microcontroller for secure/sensitive applications
  - 32, 64, or 128 kbytes of nonvolatile SRAM for program and/or data storage
  - In-system programming via on-chip serial port
  - Capable of modifying 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
  - SDI (Self-Destruct Input)
  - Improved security over previous generations
  - Protects memory contents from piracy
- Crashproof operation
  - Maintains all nonvolatile resources for over 10 years in the absence of power
  - Power-fail Reset
  - Early Warning Power-fail Interrupt
  - Watchdog Timer
  - Precision reference for power monitor
- Fully 8051-compatible
  - 128 bytes scratchpad RAM
  - Two timer/counters
  - On-chip serial port
  - 32 parallel I/O port pins
- Permanently powered real time clock

PACKAGE OUTLINE



40-Pin SIMM

DESCRIPTION

The DS2252T Secure Microcontroller Module is an 8051-compatible microcontroller based on nonvolatile RAM technology. It is designed for systems that need to protect memory contents from disclosure. This includes key data, sensitive algorithms, and proprietary information of all types. Like other members of the Secure Microcontroller family, it provides full compatibility with the 8051 instruction set, timers, serial port, and parallel I/O ports. By using NV RAM instead of ROM, the user can program, then reprogram the microcontroller while in-system. This allows frequent changing of sensitive processes with minimal effort. The DS2252T provides an array of mechanisms to prevent an attacker from examining the memory. It is designed to resist all levels of threat including observation, analysis, and physical attack. As a result, a massive effort would be required to obtain any information about

memory contents. Furthermore, the “Soft” nature of the DS2252T allows frequent modification of secure information. This minimizes that value of any information that is obtained.

Using a security system based on the DS5002FP, the DS2252T protects the memory contents from disclosure. It loads program memory via its serial port and encrypts it in real time prior to storing it in SRAM. Once encrypted, the RAM contents and the program flow are unintelligible. The real data exists only inside the processor chip after being decrypted. Any attempt to discover the on-chip data, encryption keys, etc., results in its destruction. Extensive use of nonvolatile lithium-backed technology creates a microcontroller that retains data for over 10 years at room temperature, but which can be erased instantly if tampered with. The DS2252T even interfaces directly to external tamper protection hardware.

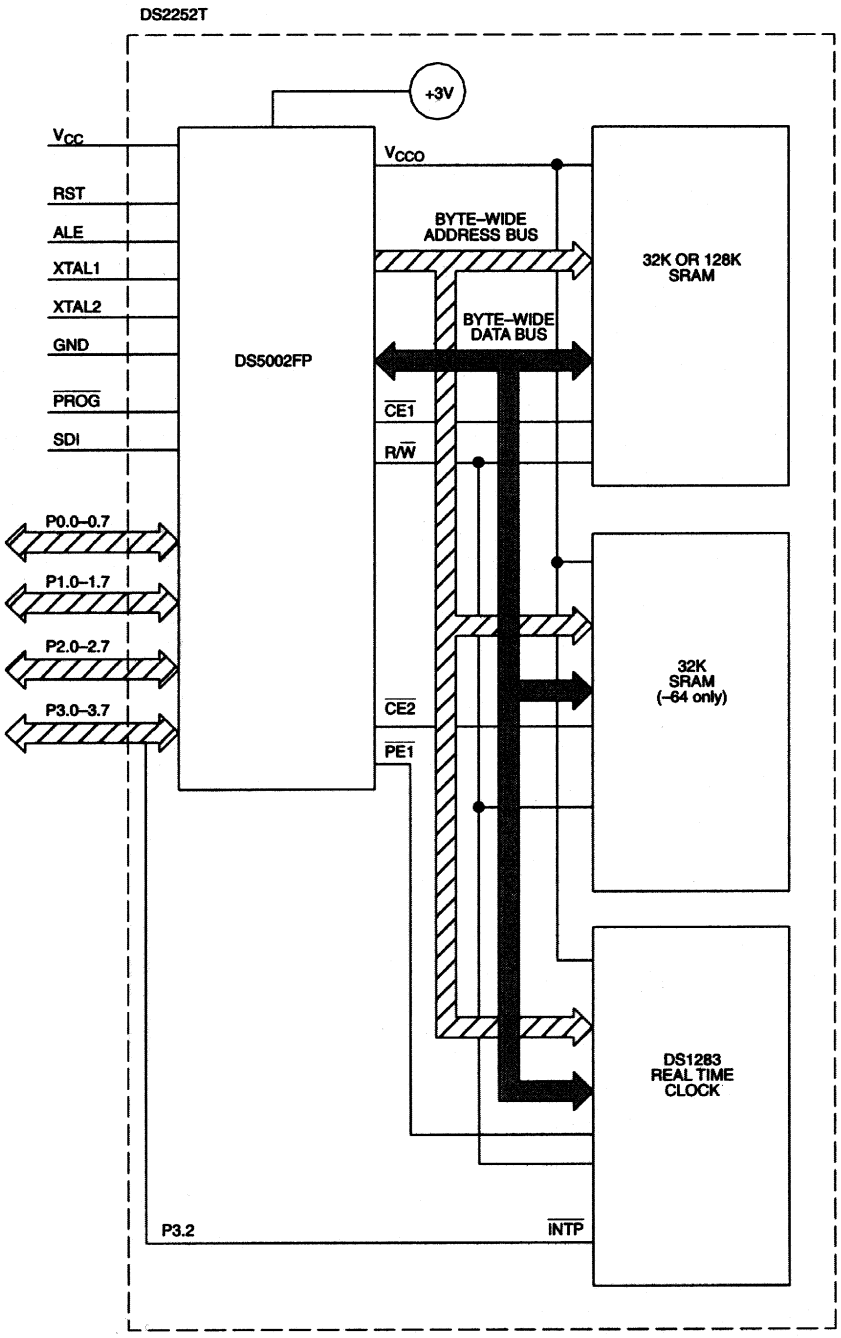
The DS2252T provides a permanently powered real time lock with interrupts for time stamp and date. It keeps time to one hundredth of a second using its onboard 32 kHz crystal.

Like other Secure Microcontrollers in the family, the DS2252T provides crashproof operation in portable systems or systems with unreliable power. These features include the ability to save the operating state, Power-fail Reset, Power-fail Interrupt, and Watchdog Timer. All nonvolatile memory and resources are maintained for over 10 years at room temperature in the absence of power.

A user loads programs into the DS2252T via its on-chip Serial Bootstrap Loader. This function supervises the loading of software into NV RAM, validates it, then becomes transparent to the user. It also manages the loading of new encryption keys automatically. Software is stored in onboard CMOS SRAM. Using its internal Partitioning, the DS2252T can divide a common RAM into user selectable program and data segments. This Partition can be selected at program loading time, but can be modified anytime later. The microcontroller will decode memory access to the SRAM, access memory via its Byte-wide bus and write-protect the memory portion designated as program (ROM).

A detailed summary of the security features is provided in the User’s Guide section of the Secure Microcontroller data book. An overview is also available in the DS5002FP data sheet.

DS2252T BLOCK DIAGRAM Figure 1



PIN ASSIGNMENT

1	P1.0	11	P1.5	21	P3.1 TXD	31	P3.6 $\overline{WR}$
2	V_{CC}	12	P0.4	22	ALE	32	P2.4
3	P1.1	13	P1.6	23	P3.2 $\overline{INT0}$	33	P3.7 $\overline{RD}$
4	P0.0	14	P0.5	24	$\overline{PROG}$	34	P2.3
5	P1.2	15	P1.7	25	P3.3 $\overline{INT1}$	35	XTAL2
6	P0.1	16	P0.6	26	P2.7	36	P2.2
7	P1.3	17	RST	27	P3.4 T0	37	XTAL1
8	P0.2	18	P0.7	28	P2.6	38	P2.1
9	P1.4	19	P3.0 RXD	29	P3.5 T1	39	GND
10	P0.3	20	SDI	30	P2.5	40	P2.0

PIN DESCRIPTION

PIN	DESCRIPTION
4, 6, 8, 10, 12, 14, 16, 18	**P0.0 - P0.7.** General purpose I/O Port 0. This port is open-drain and can not 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.
1, 3, 5, 7, 9, 11, 13, 15	**P1.0 - P1.7.** General purpose I/O Port 1.
40, 38, 36, 34, 32, 30, 28, 26	**P2.0 - P2.7.** General purpose I/O Port 2. Also serves as the MSB of the Expanded Address bus.
19	**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.
21	**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.
23	**P3.2 $\overline{INT0}$.** General purpose I/O port pin 3.2. Also serves as the active low External Interrupt 0. This pin is also connected to the $\overline{INTP}$ output of the DS1283 Real Time Clock.
25	**P3.3 $\overline{INT1}$.** General purpose I/O port pin 3.3. Also serves as the active low External Interrupt 1.
27	**P3.4 T0.** General purpose I/O port pin 3.4. Also serves as the Timer 0 input.
29	**P3.5 T1.** General purpose I/O port pin 3.5. Also serves as the Timer 1 input.
31	**P3.6 $\overline{WR}$.** General purpose I/O port pin. Also serves as the write strobe for Expanded bus operation.
33	**P3.7 $\overline{RD}$.** General purpose I/O port pin. Also serves as the read strobe for Expanded bus operation.
17	**RST -** Active high reset input. A logic 1 applied to this pin will activate a reset state. This pin is pulled down internally, can be left unconnected if not used. An RC power-on reset circuit is not needed and is NOT recommended.

PIN	DESCRIPTION
22	**ALE -** Address Latch Enable. Used to de-multiplex the multiplexed Expanded Address/Data bus on Port 0. This pin is normally connected to the clock input on a ’373 type transparent latch.
35, 37	**XTAL2, XTAL1.** Used to connect an external crystal to the internal oscillator. XTAL1 is the input to an inverting amplifier and XTAL2 is the output.
39	**GND -** Logic ground.
2	**V_{CC} - +5V**.
24	$\overline{\textbf{PROG}}$ **-** 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 microcontroller will enter Bootstrap loading on power up. This signal is pulled up internally.
20	**SDI –** Self-Destruct Input. A logic 1 applied to this input causes a hardware unlock. This involves the destruction of Encryption Keys, Vector RAM, and the momentary removal of power from V_{CCO}. This pin should be grounded if not used.

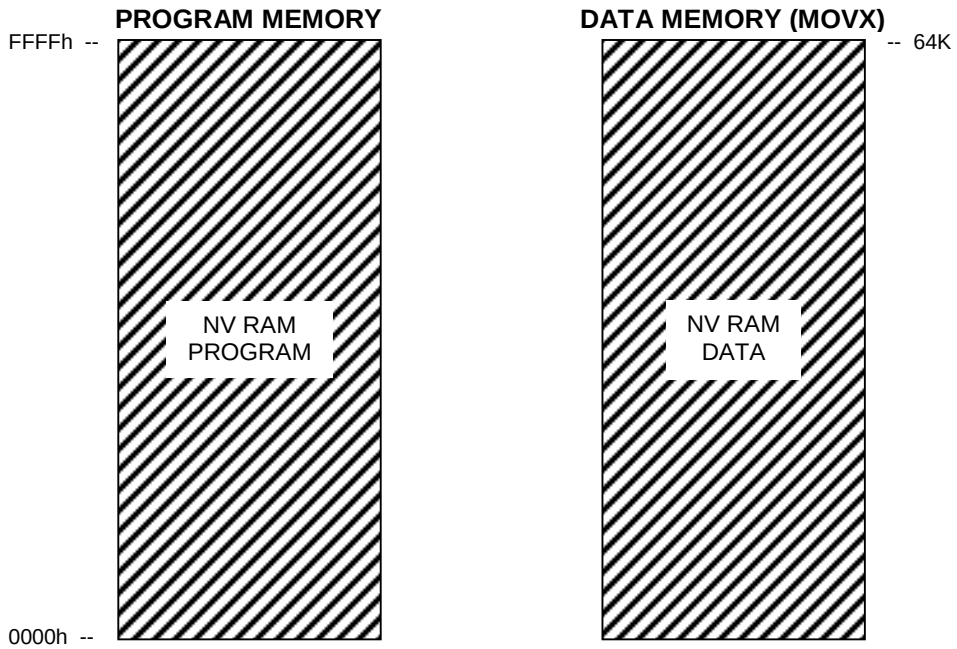
INSTRUCTION SET

The DS2252T 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 DS2252T. A complete description of the instruction set and operation are provided in the User’s Guide section of the Secure Microcontroller Data Book.

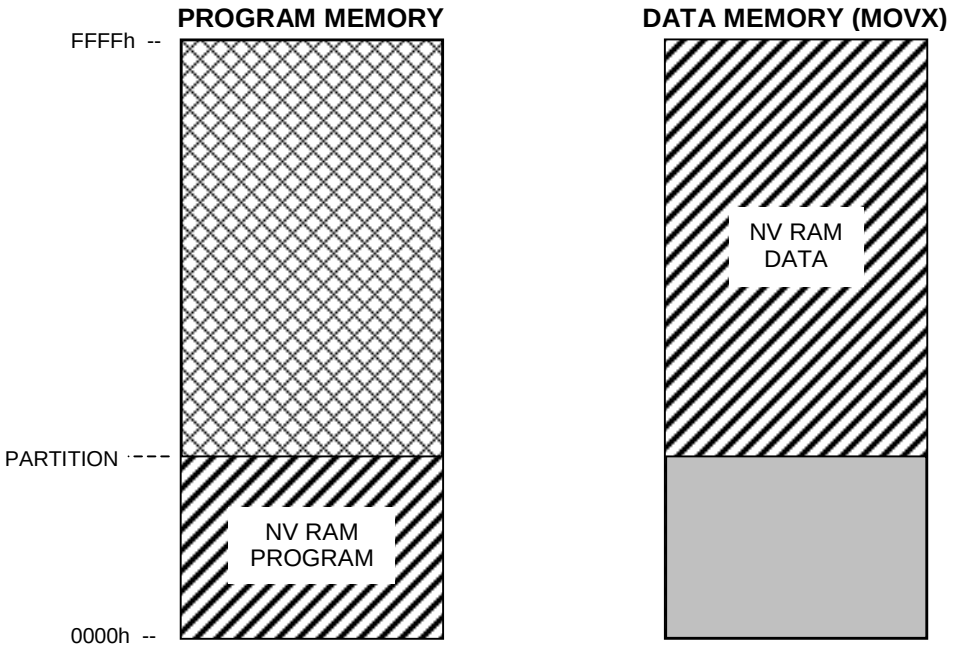
MEMORY ORGANIZATION

Figure 2 illustrates the memory map accessed by the DS2252T. The entire 64k of program and 64k of data are available to the Byte-wide bus. This preserves the I/O ports for application use. An alternate configuration allows dynamic Partitioning of a 64k space as shown in Figure 3. Any data area not mapped into the NV RAM is reached via the Expanded bus on Ports 0 and 2. Off-board program memory is not available for security reasons. Selecting PES=1 provides access to the Real Time Clock as shown in Figure 4. These selections are made using Special Function Registers. The memory map and its controls are covered in detail in the User’s Guide section of the Secure Microcontroller Data Book.

DS2252T MEMORY MAP IN NON-PARTITIONABLE MODE (PM=1) Figure 2



DS2252T MEMORY MAP IN PARTITIONABLE (PM=0) Figure 3



NOTE: PARTITIONABLE MODE IS NOT SUPPORTED ON THE 128KB VERSION OF THE DS2252T.

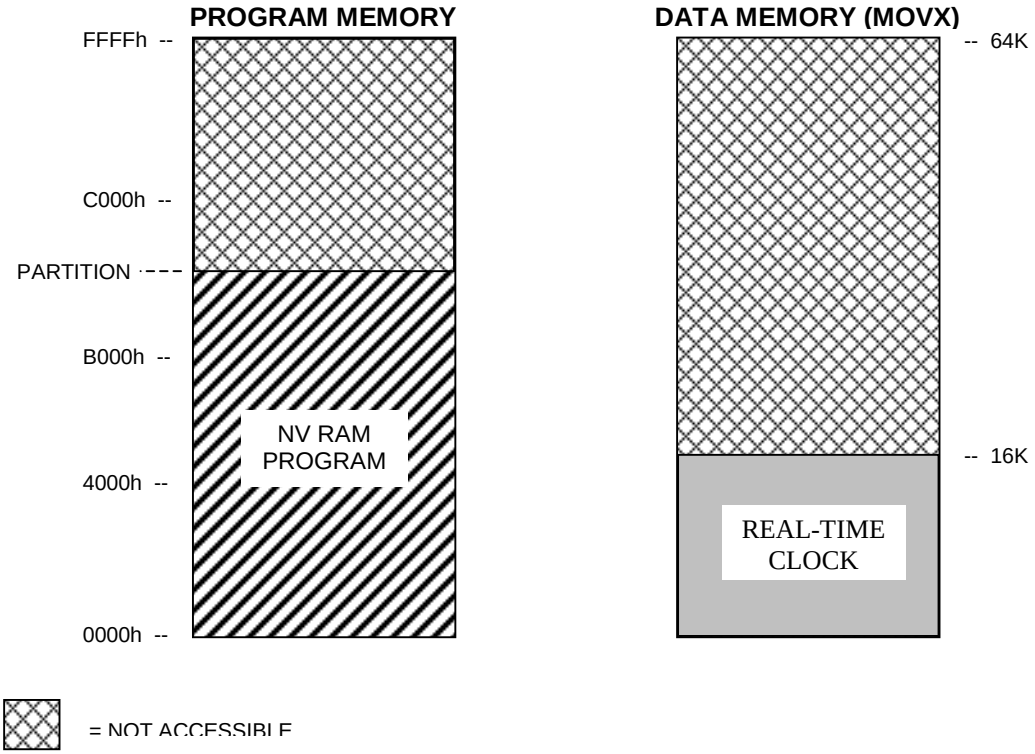
LEGEND:

= NV RAM MEMORY

= NOT AVAILABLE

= EXPANDED BUS (PORTS 0 AND 2)

DS2252T MEMORY MAP WITH (PES=1) Figure 4



POWER MANAGEMENT

The DS2252T monitors V_{CC} to provide Power-fail Reset, early warning Power-fail Interrupt, and switch-over to lithium backup. It uses an internal band-gap 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 DS2252T will perform an interrupt vector to location 2Bh if the power-fail warning is enabled. Full processor operation continues regardless. When power falls further to V_{CCMIN}, the DS2252T invokes a reset state. No further code execution will be 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 will switch to the built-in lithium cell for power. The majority of internal circuits will be disabled and the remaining nonvolatile states will be retained. The User's Guide has more information on this topic. The trip points V_{CCMIN} and V_{PFW} are listed in the electrical specifications.

ABSOLUTE MAXIMUM RATINGS*

Voltage on Any Pin Relative to Ground	-0.3V to (V_{CC} + 0.5V)
Voltage on V_{CC} Relative to Ground	-0.3V to +6.0V
Operating Temperature[2]	-40°C to +85°C
Storage Temperature	-55°C to +125°C
Soldering Temperature	260°C for 10 seconds

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

[2] 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 (t_A=0°C to 70°C; V_{CC}=5V ± 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Input Low Voltage	V_{IL}	-0.3		+0.8	V	1
Input High Voltage	V_{IH1}	2.0		V_{CC}+0.3	V	1
Input High Voltage (RST, XTAL1, $\overline{PROG}$)	V_{IH2}	3.5		V_{CC}+0.3	V	1
Output Low Voltage @ I_{OL}=1.6 mA (Ports 1, 2, 3)	V_{OL1}		0.15	0.45	V	1
Output Low Voltage @ I_{OL}=3.2 mA (Ports 0, ALE)	V_{OL2}		0.15	0.45	V	1
Output High Voltage @ I_{OH}= -80 µA (Ports 1, 2, 3)	V_{OH1}	2.4	4.8		V	1
Output High Voltage @ I_{OH}=-400 µA (Ports 0, ALE)	V_{OH2}	2.4	4.8		V	1
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	
Input Leakage Current 0.45 < V_{IN} < V_{CC} (Port 0)	I_{IL}			±10	µA	
RST Pulldown Resistor	R_{RE}	40		150	kΩ	
Power Fail Warning Voltage	V_{PRW}	4.25	4.37	4.50	V	1
Minimum Operating Voltage	V_{CCMIN}	4.00	4.12	4.25	V	1
Operating Current @ 16 MHz	I_{CC}			45	mA	4
Idle Mode Current @ 12 MHz	I_{IDLE}			7.0	mA	5
Stop Mode Current	I_{STOP}			80	µA	6
Pin Capacitance	C_{IN}			10	pF	7

DC CHARACTERISTICS (continued) (t_A=0°C to 70°C; V_{CC}=5V ± 10%)

Reset Trip Point in Stop Mode w/BAT=3.0V w/BAT=3.3V		 4.0 4.4		 4.25 4.65	V	1
SDI Input High Voltage	V_{IHS}	2.0		V_{CC}	V	1, 2
SDI Input High Voltage	V_{IHS}	2.0		3.5	V	1, 2
SDI PullDown Resistor	R_{SDI}	25		60	kΩ	

AC CHARACTERISTICS (t_A=0°C to 70°C; V_{CC}=0V to 5V)

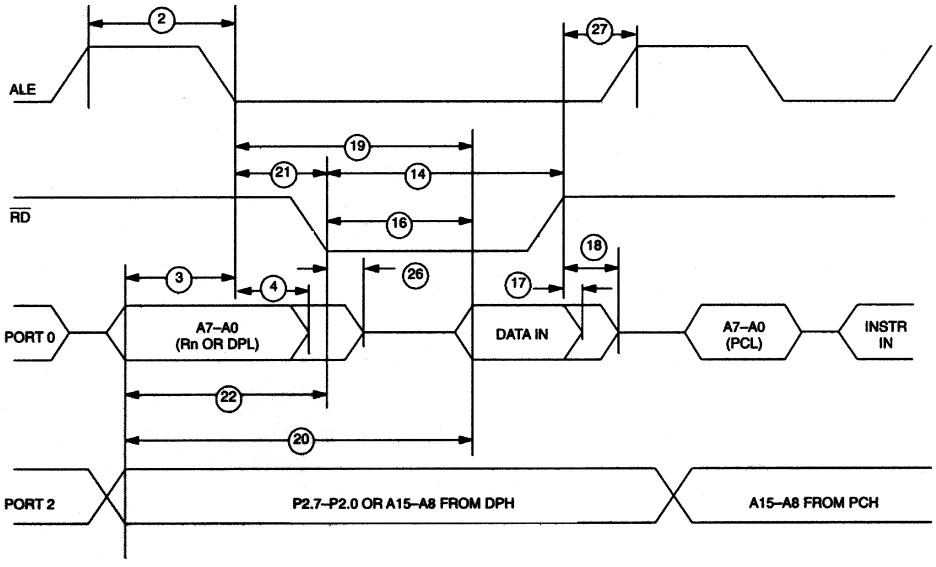
PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
SDI Pulse Reject (4.5V < V_{CC} < 5.5V) (V_{CC}=0V, V_{BAT}=2.9V)	t_{SPR}			 2 4	µs	10
SDI Pulse Accept (4.5V < V_{CC} < 5.5V) (V_{CC}=0V, V_{BAT}=2.9V)	t_{SPA}	 10 50			µs	10

AC CHARACTERISTICS: EXPANDED BUS MODE TIMING SPECIFICATIONS

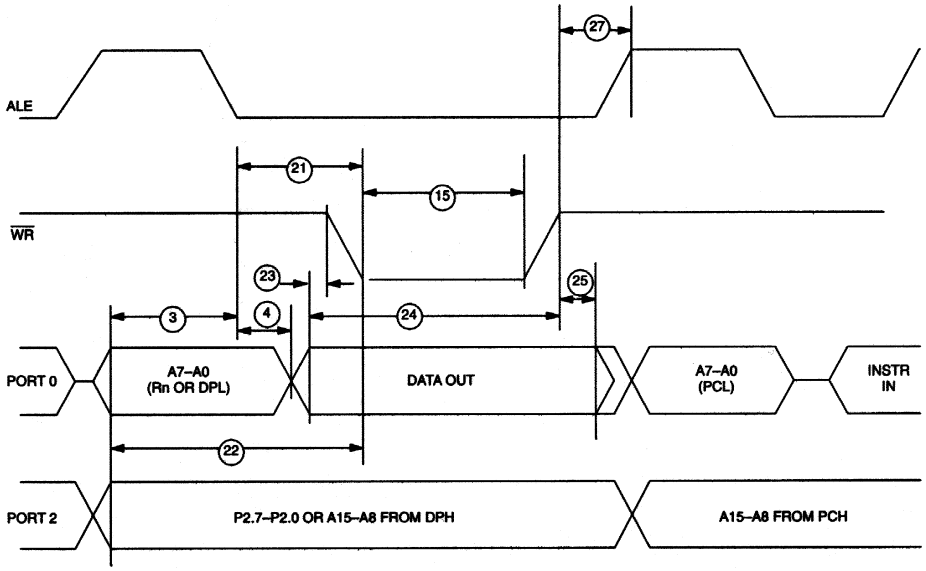
(t_A=0°C to70°C; V_{CC}=5V ± 10%)

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
1	Oscillator Frequency	$1/t_{CLK}$	1.0	16 (-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 @ 12 MHz @ 16 MHz	t_{RDLDV}		$5t_{CLK}$ -165 $5t_{CLK}$ -105	ns ns
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 @ 12 MHz @ 16 MHz	t_{ALLVD}		8_{CLK} -150 $8t_{CLK}$ -90	ns ns
20	Valid Addr. to Valid Data In @ 12 MHz @ 16 MHz	t_{AVDV}		$9t_{CLK}$ -165 $9t_{CLK}$ -105	ns ns
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 @ 12 MHz @ 16 MHz	t_{DVWRH}	$7t_{CLK}$ -150 $7t_{CLK}$ -90		ns ns
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

EXPANDED DATA MEMORY READ CYCLE



EXPANDED DATA MEMORY WRITE CYCLE



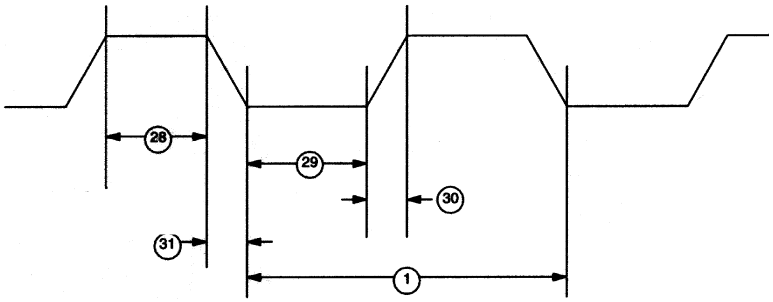
AC CHARACTERISTICS (continued)

EXTERNAL CLOCK DRIVE

(t_A=0°C to70°C; V_{CC}=5V ± 10%)

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

EXTERNAL CLOCK TIMING

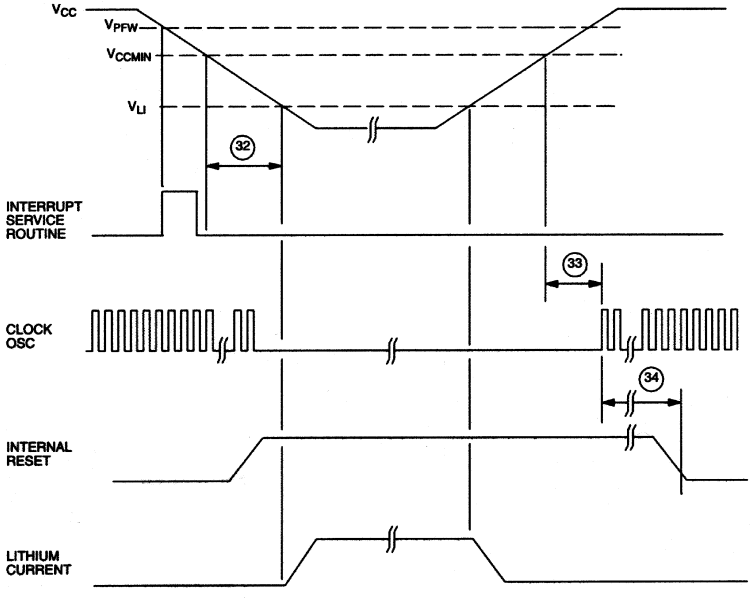


AC CHARACTERISTICS (continued)

POWER CYCLING TIMING (t_A=0°C to70°C; V_{CC}=5V ± 10%)

#	PARAMETER	SYMBOL	MIN	MAX	UNITS
32	Slew Rate from V_{CCMIN} to 3.3V	t_F	130		µs
33	Crystal Start-up Time	t_{CSU}		(note 8)	
34	Power-On Reset Delay	t_{POR}		21504	t_{CLK}

POWER CYCLE TIMING

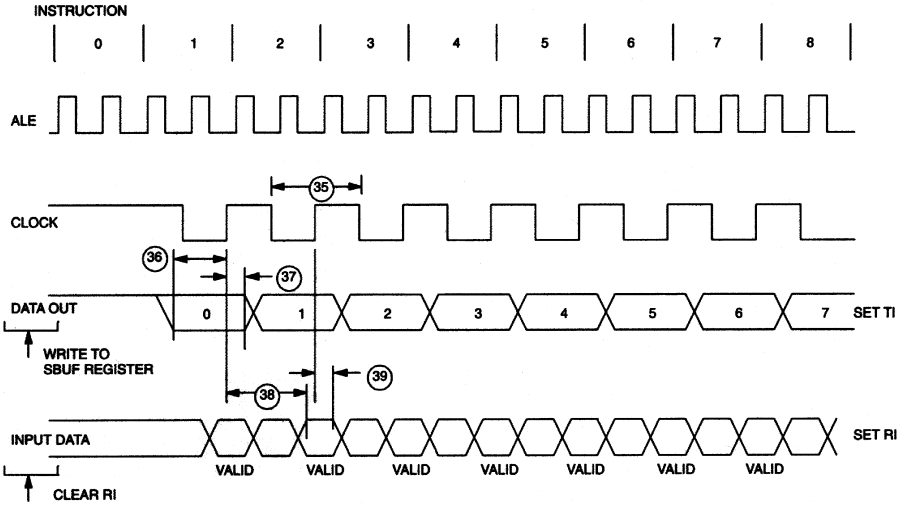


AC CHARACTERISTICS (cont'd)

SERIAL PORT TIMING - MODE 0 (t_A=0°C to70°C; V_{CC}=5V ± 10%)

#	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

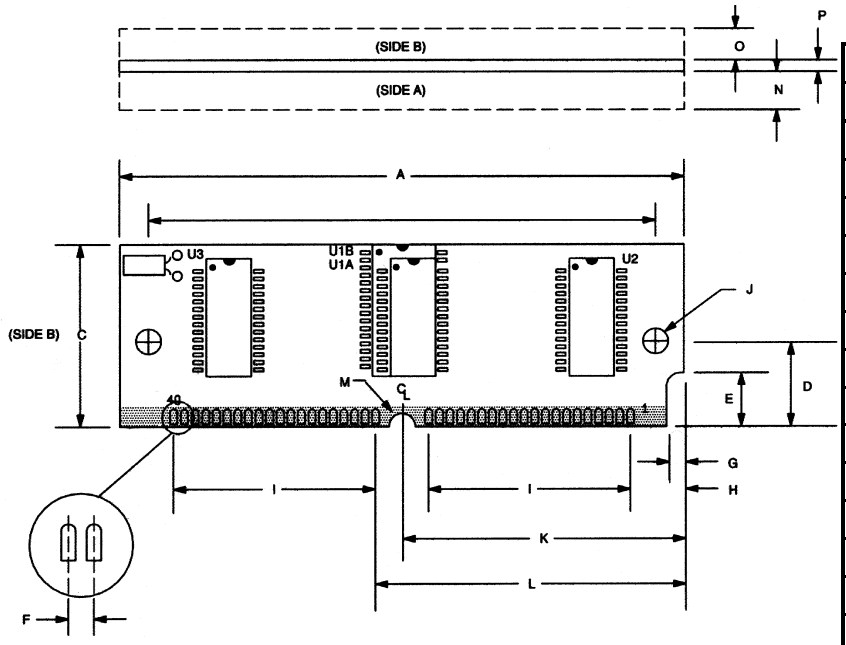
SERIAL PORT TIMING - MODE 0



NOTES:

1. All voltage referenced to ground.
2. SDI should be taken to a logic high when V_{CC}=+5V, and to approximately 3V when V_{CC}<3V.
3. 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}.
4. 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}.
5. Idle mode I_{IDLE} is measured with all output pins disconnected; XTAL1 driven with t_{CLKR}, t_{CLKF}= 10 ns, V_{IL} = 0.5V; XTAL2 disconnected; PORT0 = V_{CC}, RST = V_{SS}.
6. Stop mode I_{STOP} is measured with all output pins disconnected; PORT0 = V_{CC}; XTAL2 not connected; RST = XTAL1 = V_{SS}.
7. Pin capacitance is measured with a test frequency - 1 MHz, t_A= 25°C.
8. Crystal start-up 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.

PACKAGE DRAWING



PKG	INCHES	
DIM	MIN	MAX
A	2.645	2.655
B	2.379	2.389
C	0.995	1.005
D	0.395	0.405
E	0.245	0.255
F	0.050 BSC	
G	0.075	0.085
H	0.245	0.255
I	0.950 BSC	
J	0.120	0.130
K	1.320	1.330
L	1.445	1.455
M	0.057	0.067
N	-	0.300
O	-	0.165
P	0.047	0.054

DATA SHEET REVISION SUMMARY

The following represent the key differences between 12/13/95 and 08/16/96 version of the DS2252T data sheet. Please review this summary carefully.

1. Change V_{CC} slew rate specification to reference 3.3V instead of V_{LI}.
2. Add minimum value to PCB thickness.

The following represent the key differences between 08/16/96 and 05/28/97 version of the DS2252T data sheet. Please review this summary carefully.

1. AC characteristics for battery-backed SDI pulse specification added.

The following represent the key differences between 05/28/97 and 11/08/99 version of the DS2252T data sheet. Please review this summary carefully. (PCN I80903)

1. Correct Absolute Maximum Ratings to reflect changes to DS5002FP microprocessor.
2. Add note clarifying that SRAM contents are not defined under storage temperature conditions.

The following represent the key differences between 11/08/99 and 01/18/00 version of the DS2252T data sheet. Please review this summary carefully.

1. Datasheet conversion from Interleaf to Word.