Rev 0; 3/08

MAXIM

安全微处理器芯片

DS5003

概述

DS5003安全微处理器集成了最先进的加密功能，包括一系列专门设计的安全机制，能够抵御各种级别的威胁，包括监测、分析和物理攻击。这样，想要获得任何有关存储器内容的信息，都需付出极大努力。而且，DS5003所特有的“柔性”特性使用户能够频繁修改安全信息，使攻击者经过大量努力获得的任何安全信息失去价值。该器件是DS5002FP安全微处理器芯片的增强版，具有额外的暂存器RAM。

与DS5002FP的区别

DS5003仅比DS5002FP多了一项特性：增加了128字节的内部暂存器(总存储量达到了256字节)，类似于8032/8052架构中采用的暂存器。增加的存储区可通过间接寻址8051指令进行访问，例如“mov a, @r1,”，其中r1的取值范围现在可为0到255。它还可以作为堆栈空间进行入栈、出栈、调用和返回操作。

采用寄存器间接寻址访问7Fh以上的暂存RAM。如果需要，亦可用来访问较低地址的RAM (0h–7Fh)。地址是由指令中指定的工作寄存器的内容提供的。因此，通过改变指定工作寄存器的内容，即可通过一条指令获得多个值。注意，只有R0和R1可作为指针。以下是寄存器间接寻址的一个例子：

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

应用

密码键盘

游戏机

需要软件保护的任何应用

特性

- ♦ 适合于安全/敏感应用的8051兼容微处理器
  - 可访问32kB、64kB或128kB非易失SRAM的程序和/或数据存储器
  - 128字节RAM
  - 128字节间接暂存器RAM
  - 通过片内串行接口进行在系统编程
  - 能够在最终系统中修改自身的程序或数据存储器
- ♦ 固件安全特性
  - 存储器以密文方式存储信息
  - 加密算法采用片内64位密钥
  - 自动操作的真随机密钥生成器
  - 自毁输入(SDI)
  - 顶部敷层防止微探针探测
  - 防止存储内容被盗版
- ♦ 防冲击工作
  - 在没有电源的情况下，所有的非易失资源可保持10年以上(室温下)
  - 电源失效复位
  - 电源失效预警中断
  - 看门狗定时器

定购信息

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

+表示无铅(Pb)/符合RoHS标准的封装。

引脚配置在数据资料的最后给出。

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 ($\overline{RST}$, 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.

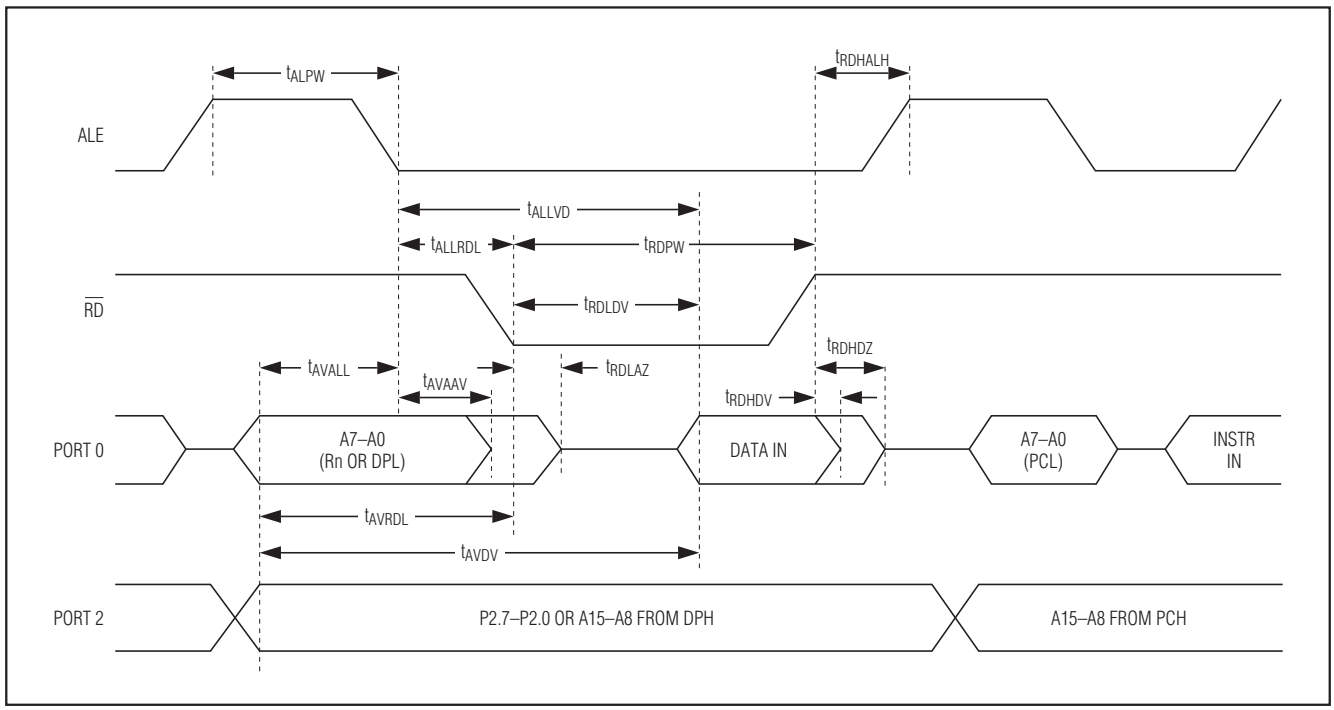

图1. 扩展数据存储器的读周期

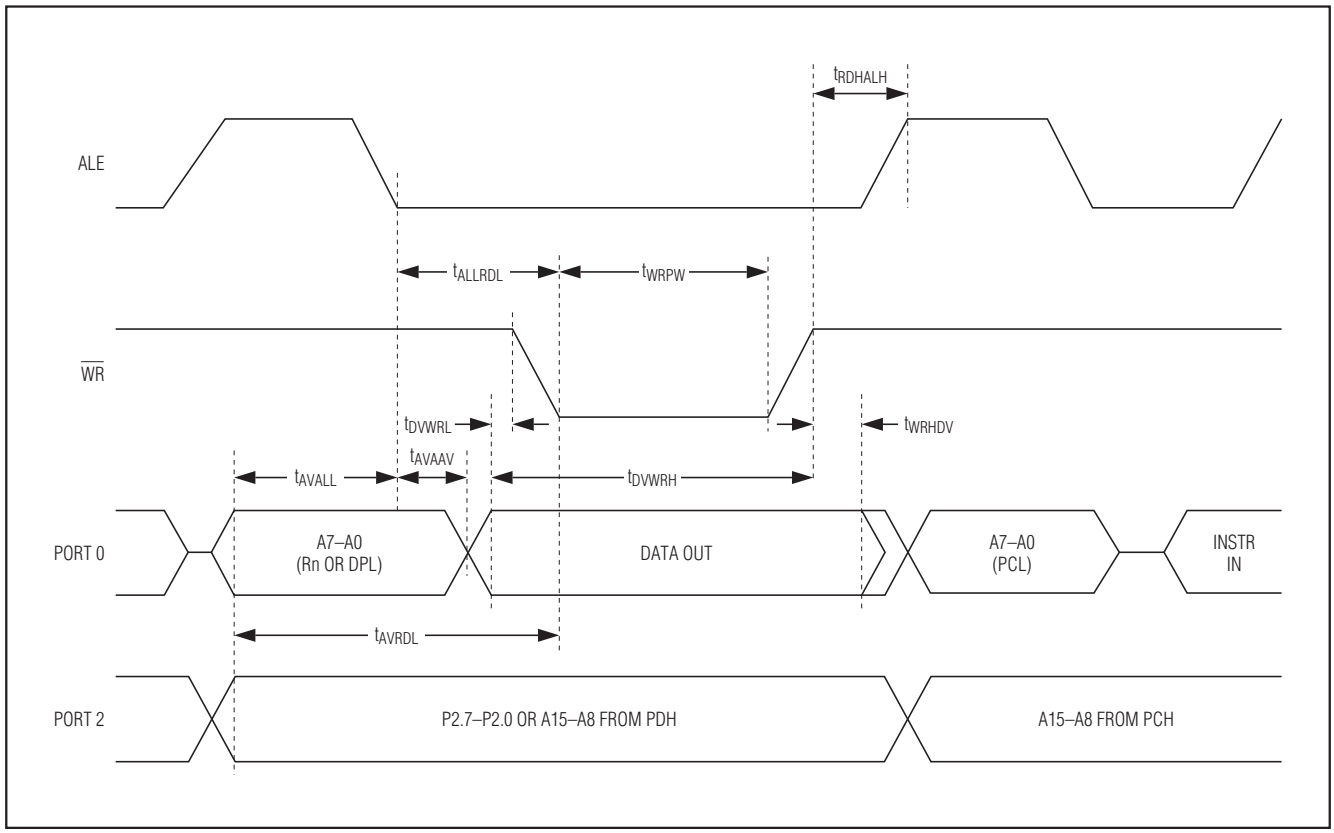

图2. 扩展数据存储器的写周期

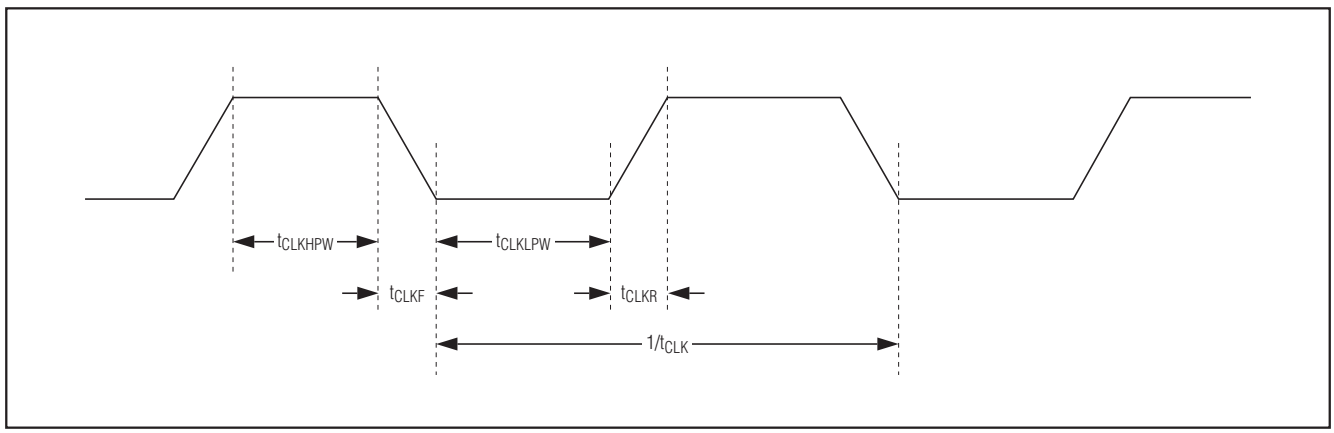

图3. 外部时钟时序

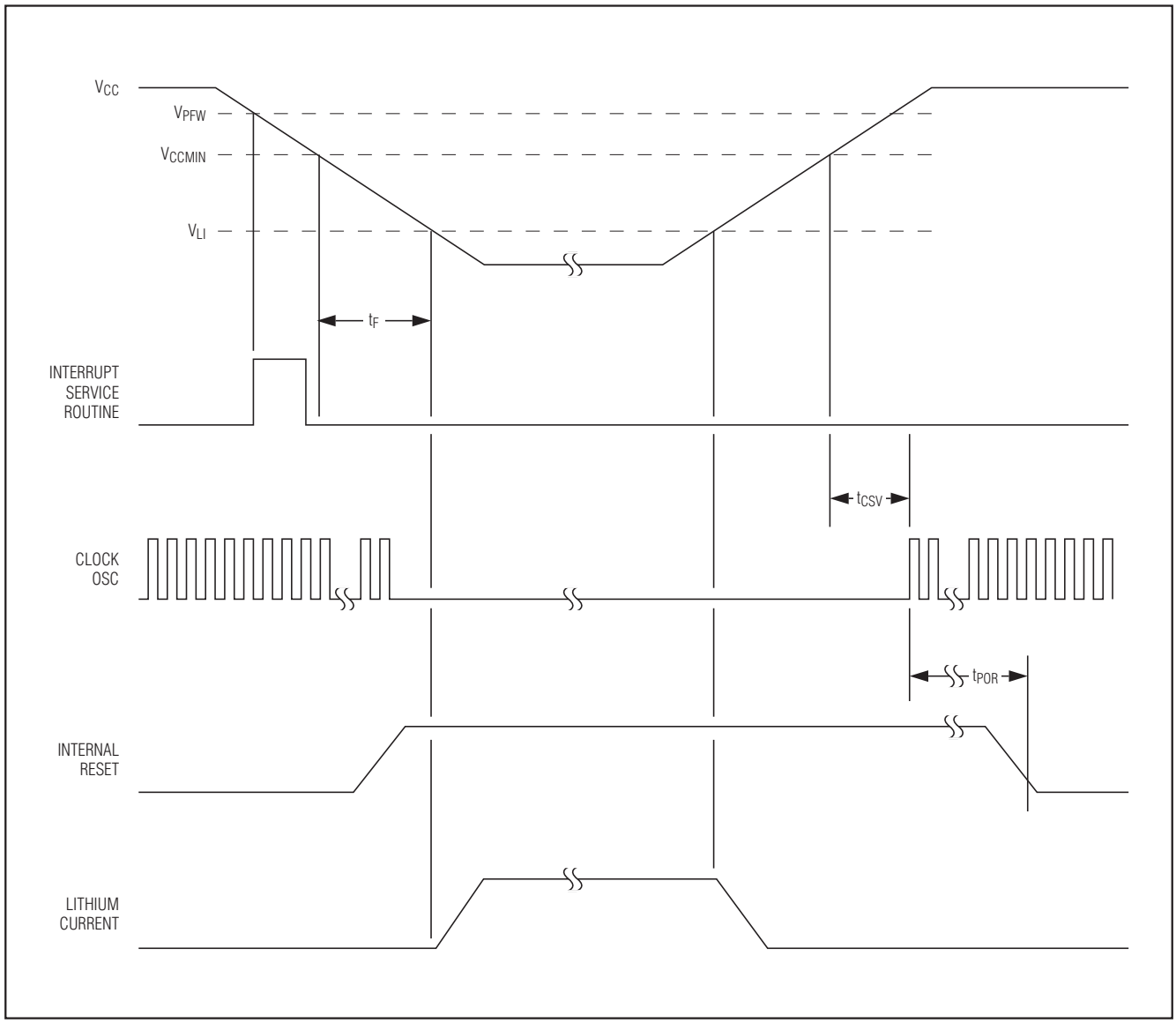
VCC
VPFW
VCCMIN
VLI
tF
INTERRUPT SERVICE ROUTINE
tCSV
CLOCK OSC
tPOR
INTERNAL RESET
LITHIUM CURRENT

图4. 电源重新上电时序

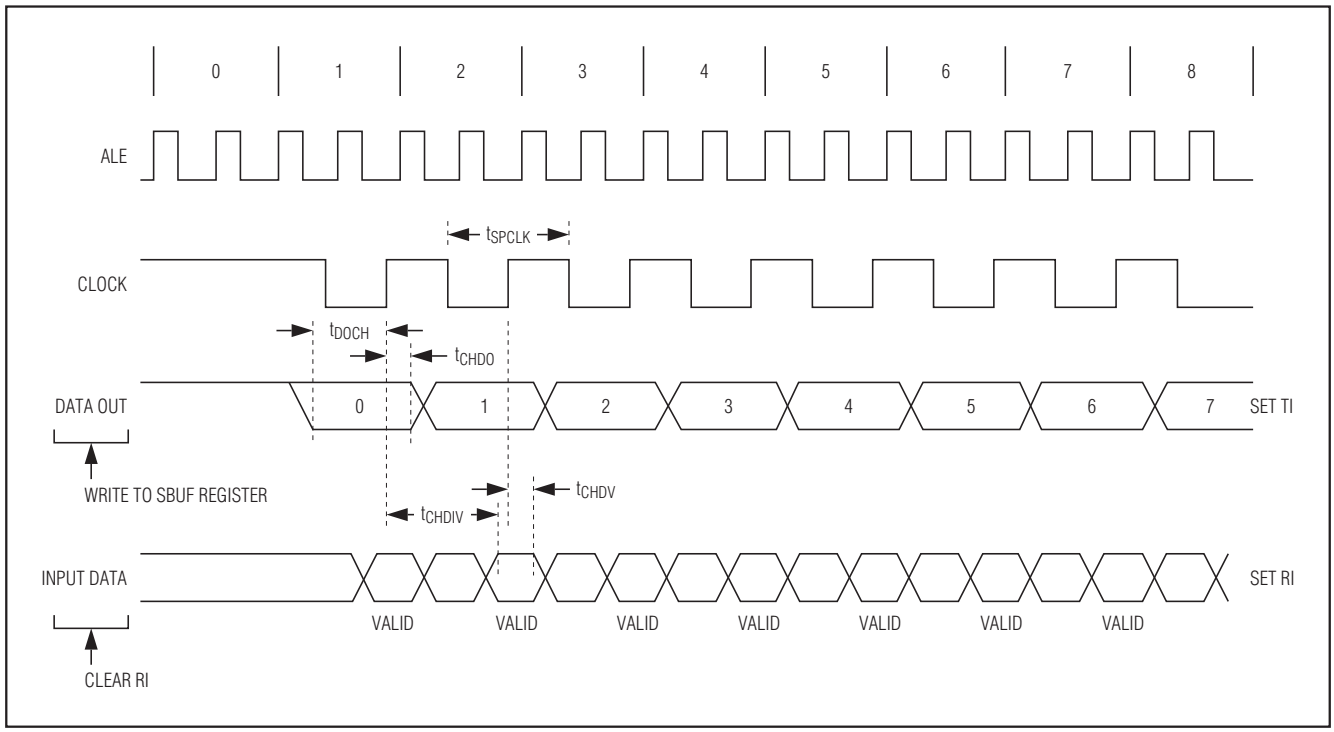

图5. 串口时序(模式0)

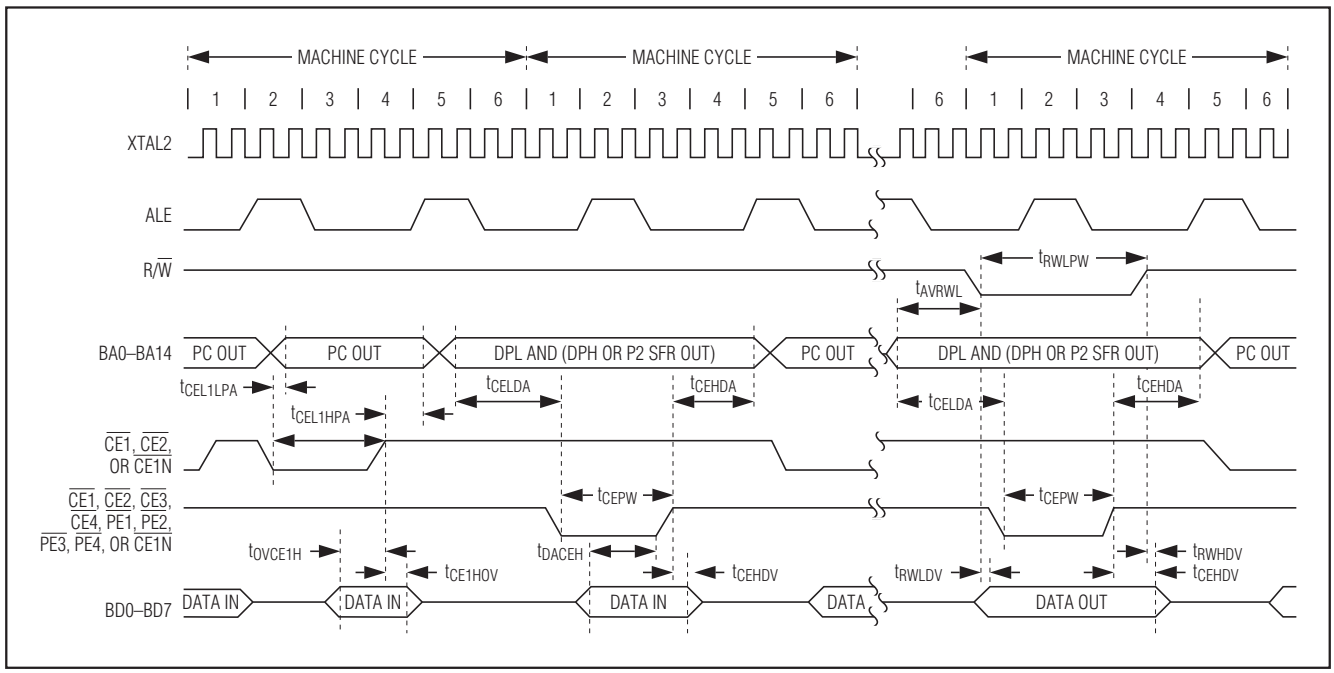

图6. 字节宽总线时序

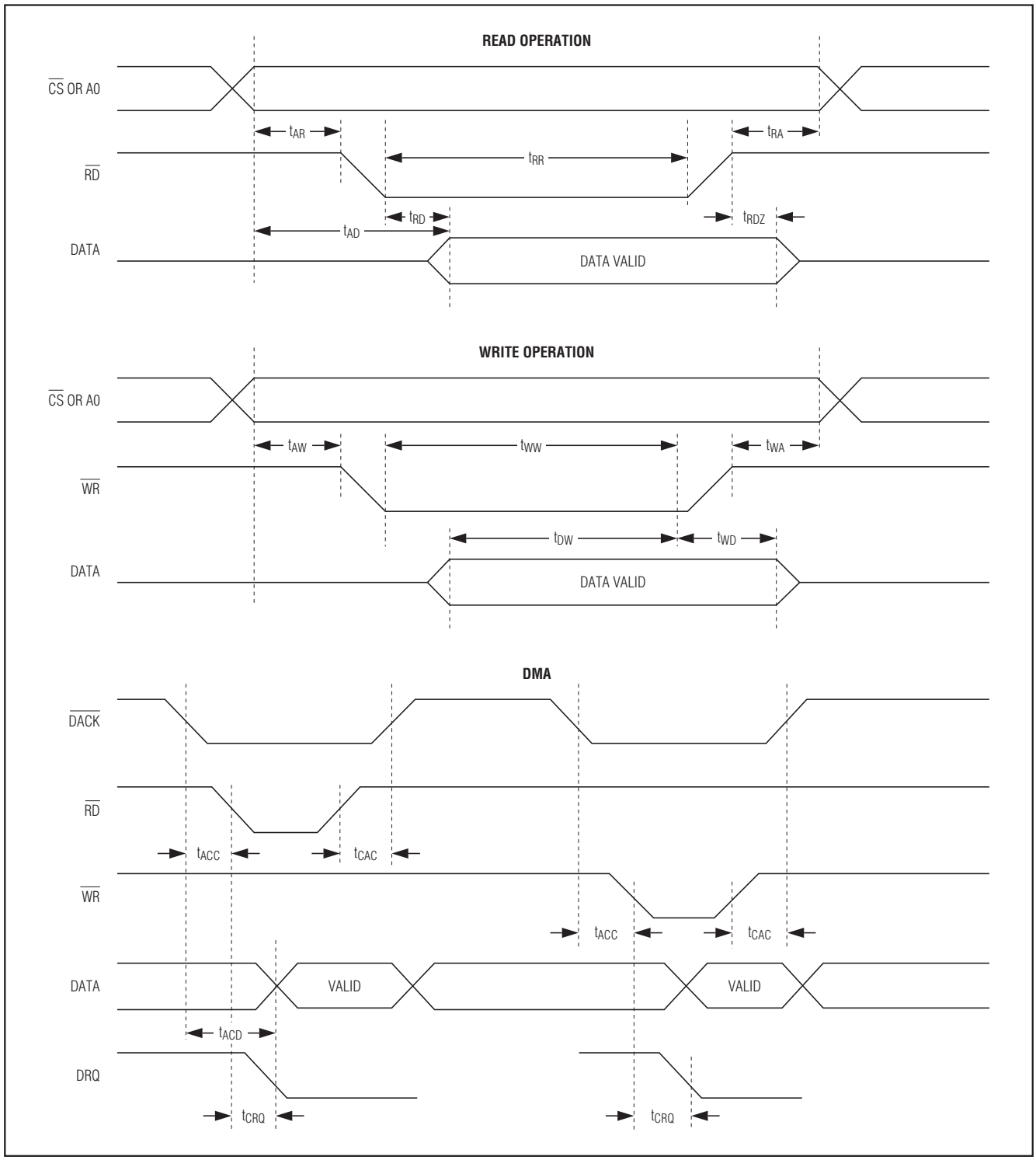
READ OPERATION
CS OR A0
tAR
tRA
RD
tRR
tRD
tRDZ
tAD
DATA
DATA VALID
WRITE OPERATION
CS OR A0
tAW
tWW
tWA
WR
tDW
tWD
DATA
DATA VALID
DMA
DACK
RD
tACC
tCAC
WR
tACC
tCAC
DATA
VALID
VALID
tACD
DRQ
tCRQ
tCRQ

图7. RPC时序模式

引脚说明

引脚	名称	功能
		电源引脚
13	V_{CC}	**电源**，+5V。
12	V_{CCO}	**V_{CC}输出**。根据V_{CC}的电平由内部电路控制在V_{CC}和V_{LI}之间的切换。当电源高于锂电池输入时，由V_{CC}供电，锂电池与负载保持隔离；当V_{CC}低于V_{LI}时，V_{CCO}切换至V_{LI}。V_{CCO}应连接到SRAM的V_{CC}引脚。
54	V_{LI}	**锂电池电压输入**。如电气指标部分所述，连接到电压高于V_{LIMIN}但不高于V_{LIMAX}的锂电池。标称值为+3V。
52	GND	**逻辑地**。
		通用I/O引脚
11	P0.0/AD0	**通用I/O端口0**。该端口为漏极开路，不能驱动逻辑1。该端口需要外部上拉。端口0还可复用为扩展地址/数据总线，当用于该模式时，不需要上拉。
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	**通用I/O端口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	**通用I/O端口2**，也可用作扩展地址总线的MSB。
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	**通用I/O端口引脚3.0**，也可用作板上UART的接收信号。该引脚不能直接连接到PC的COM端口。
38	P3.1/TXD	**通用I/O端口引脚3.1**，也可用作板上UART的发送信号。该引脚不能直接连接到PC的COM端口。
39	P3.2/$\overline{INT0}$	**通用I/O端口引脚3.2**，也可用作低电平有效的外部中断0。
40	P3.3/$\overline{INT1}$	**通用I/O端口引脚3.3**，也可用作低电平有效的外部中断1。
41	P3.4/T0	**通用I/O端口引脚3.4**，也可用作定时器0的输入。
44	P3.5/T1	**通用I/O端口引脚3.5**，也可用作定时器1的输入。
45	P3.6/$\overline{WR}$	**通用I/O端口引脚3.6**，也可用作扩展总线操作的写选通。
46	P3.7/$\overline{RD}$	**通用I/O端口引脚3.7**，也可用作扩展总线操作的读选通。

引脚说明(续)

引脚	名称	功能
		字节宽总线接口引脚
37	BA0	**字节宽地址总线位14–0**。该总线与非复用数据总线(BD7–BD0)配合，访问外部SRAM，采用$\overline{CE1}$–$\overline{CE4}$解码。因此，实际上不需要BA15。读/写操作由R/$\overline{W}$控制。BA14–BA0直接连接到一个8kB、32kB或128kB SRAM。如果采用8kB SRAM，则不连接BA13和BA14；如果采用128kB SRAM，微控制器分别将$\overline{CE2}$和$\overline{CE3}$变为A16和A15。
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	**字节宽数据总线位7–0**。该8位双向总线与非复用地址总线(BA14–BA0)配合，访问外部SRAM。采用$\overline{CE1}$和$\overline{CE2}$解码。读/写操作由R/$\overline{W}$控制。D7–D0直接连接到一个SRAM，亦可选择连接到一个实时时钟或其它外围设备。
57	BD1	
59	BD2	
61	BD3	
65	BD4	
67	BD5	
69	BD6	
71	BD7	
70	ALE	**地址锁存使能**。用来分离端口0上被复用的扩展地址/数据总线。在'373透明锁存电路中，该引脚通常被连接到时钟输入。
10	R/$\overline{W}$	**读/写(低电平有效)**。该信号为字节宽总线上的SRAM提供写使能信号。它是由存储器映射和分配表控制的，被选为程序的分区(ROM)具有写保护。
74	$\overline{CE1}$	**低电平有效芯片使能1**。该信号为主解码芯片使能信号，用于字节宽总线上的存储器访问。它连接到一个SRAM的芯片使能输入。$\overline{CE1}$具有锂电池备份供电。当V_{CC}降至低于V_{LI}时，它保持为逻辑高禁止状态。
72	$\overline{CE1N}$	**CE1的无电池备份供电版本**。由于DS5003加密的原因而不能使用EPROM，所以一般不使用该引脚。
2	$\overline{CE2}$	**低电平有效芯片使能2**。该芯片使能信号用于访问第二个32kB的内存分区。它连接到一个SRAM的芯片使能输入。当MSEL = 0时，微控制器将$\overline{CE2}$变为一个128kB x 8 SRAM的A16。$\overline{CE2}$具有锂电池备份供电，当V_{CC}降至低于V_{LI}时，它保持为逻辑高状态。
63	$\overline{CE3}$	**低电平有效芯片使能3**。该芯片使能信号用于访问第三个32kB的内存分区。它连接到一个SRAM的芯片使能输入。当MSEL = 0时，微控制器将$\overline{CE3}$转换为一个128kB x 8 SRAM的A15。$\overline{CE3}$具有锂电池备份供电，当V_{CC}降至低于V_{LI}时，它保持为逻辑高状态。

引脚说明(续)

引脚	名称	功能
62	$\overline{CE4}$	**低电平有效芯片使能4**。该芯片使能信号用于访问第四个32kB的内存分区。它连接到一个SRAM的芯片使能输入。当MSEL = 0时，不使用该信号。$\overline{CE4}$具有锂电池备份供电，当V_{CC}降至低于V_{LI}时，它保持为逻辑高状态。
78	$\overline{PE1}$	**低电平有效外设使能1**。当PES位被置为逻辑1时，访问地址0000h到3FFFh的数据存储空间。常用于使能一个字节宽实时时钟，例如DS1283。$\overline{PE1}$具有锂电池备份供电，当V_{CC}降至低于V_{LI}时，它保持为逻辑高状态。$\overline{PE1}$仅能连接到具有电池备份供电的电路。
3	$\overline{PE2}$	**低电平有效外设使能2**。当PES位被置为逻辑1时，访问地址4000h到7FFFh的数据存储空间。$\overline{PE2}$具有锂电池备份供电，当V_{CC}降至低于V_{LI}时，它保持为逻辑高状态。$\overline{PE2}$仅能连接到具有电池备份供电的电路。
22	$\overline{PE3}$	**低电平有效外设使能3**。当PES位被置为逻辑1时，访问地址8000h到BFFFh的数据存储空间。$\overline{PE3}$无锂电池备份供电，可以连接至任何类型的外设。如果要将该信号连接至具有电池备份供电的芯片，需要额外的电路在$V_{CC} < V_{LI}$时将芯片使能维持在禁止状态。
23	$\overline{PE4}$	**低电平有效外设使能4**。当PES位被置为逻辑1时，访问地址C000h到FFFFh的数据存储空间。$\overline{PE4}$无锂电池备份供电，可以连接至任何类型的外设。如果要将该信号连接至具有电池备份供电的芯片，需要额外的电路在$V_{CC} < V_{LI}$时将芯片使能维持在禁止状态。
14	MSEL	**存储器选择**。该信号控制存储器大小选项。当MSEL = +5V时，DS5003使用32kB x 8 SRAM；当MSEL = 0V时，DS5003使用128kB x 8 SRAM。无论采用何种分区、模式，都必须连接MSEL。
时钟引脚		
47, 48	XTAL2, XTAL1	**晶体连接**。用于将外部晶体连接到内部振荡器。XTAL1为反相放大器的输入，XTAL2为输出。
复位、状态和自毁引脚		
34	RST	**高电平有效复位输入**。在该引脚上加逻辑1信号将激活复位状态。该引脚具有内部下拉，所以不使用时可悬空。不需要也不建议使用RC上电复位电路。
32	$\overline{PROG}$	**在下降沿调用引导程序**。应对该信号进行去抖动，从而保证只检测到一个信号沿。如果该信号被连接至地，微控制器进入上电引导状态。该信号具有内部上拉。
42	$\overline{VRST}$	**低V_{CC}时复位有效**。该I/O引脚(带内部上拉的漏极开路)表示电源(V_{CC})已经下降至低于V_{CCMIN}，并且微处理器处于复位状态。当发生这种情况时，DS5003将该引脚驱动为逻辑0。由于微控制器具有锂电池备份供电，所以即使在V_{CC} = 0V时也能确保该信号有效。作为一个I/O引脚，在通过外部拉低时，该信号也能强制复位。这样能够使多个器件同步其断电复位。
43	$\overline{PF}$	**锂电池备份供电有效**。该输出变为逻辑0表示微控制器已经切换至由锂电池备份供电，这对应于$V_{CC} < V_{LI}$。由于微处理器具有锂电池备份供电，所以即使在V_{CC} = 0V时也能确保该信号有效。该信号的常见应用是控制锂电池供电电流，将具有电池备份供电和无电池备份供电的功能隔离开。
53	SDI	**自毁输入**。该引脚的高电平有效状态，将激活一个解锁程序，从而导致向量SRAM、加密密匙被破坏，并断开V_{CCO}电源。在不使用时，应该将该引脚接地。
其它引脚		
68, 73	N.C.	**未连接**。

详细说明

DS5003采取了一种安全机制，以加密的形式加载和执行应用软件。通过其字节宽总线可访问高达128kB的标准SRAM (64kB程序 + 64kB数据)。DS5003将该SRAM转换为具有锂电池备份供电的非易失存储器，用于存储程序和数据。使用极小的锂电池，即可使数据在室温下保存长达10年。所以，对于外部监测者来说，SRAM的内容和软件执行是无法了解的。加密算法采用了一个内部存储和保护的密匙，任何试图窃取密钥数值的行为都会造成其被擦除，使SRAM的内容变得毫无价值。

安全微处理器芯片采用了一种功能强大的软件加密算法，并结合了DES加密原理。这种加密方法基于一个64位的密匙字，并且该密匙只能从片内真随机数发生器获取。所以，用户无法获知真实的密匙。器件还提供了一个自毁输入(SDI)引脚，用于连接外部篡改检测电路。无论V_{CC}是否有效，激活SDI引脚都会复位安全锁：立即擦除密匙字以及48字节的向量SRAM区域。此外，还可选择管芯的顶部敷层来防止采用微探针分析技术获取信息。

当作为总体安全系统设计的一部分时，基于DS5003的系统能够提供更高的安全级别，未经授权的个人试图破坏该系统，都需花费更长的时间和更多的资源。

图8所示为DS5003的内部结构方框图。若没有特别说明，DS5003的工作方式均与DS5002FP相同。

安全工作概述

DS5003对其字节宽地址/数据总线的活动采取了加密措施，以防止未经授权访问外部SRAM中保存的程序和数据信息。以这种方式加载应用程序是通过引导程序按照以下的大体顺序实现的：

1) 将$\overline{\text{PROG}}$引脚保持为逻辑低状态至少48个时钟周期，激活引导程序。
2) 清除安全锁。
3) 设置存储器映射配置。这些设置与基于DS5002FP的设计完全相同。
4) 加载应用软件。
5) 设置安全锁。
6) 将$\overline{\text{PROG}}$引脚重新设置为逻辑高状态，退出引导程序。

将应用软件加载到程序/数据SRAM是在DS5003处于其引导模式时完成的。只有在安全锁被清除时才有可能进行加载。如果之前已经设置了安全锁，必须通过引导程序执行U命令将其清除。清除安全锁会立即清除之前的密匙字和向量SRAM的内容。此外，引导ROM还会向外部SRAM的前32kB写入零。

用户的应用软件通过L命令由片上加密电路以“扰码”的形式加载到用户提供的外部SRAM。每个外部SRAM地址都以加密的形式表示片上的逻辑地址。所以，正常程序的连续指令或数据表在SRAM存储器中是以非连续方式储存的。程序/数据SRAM的内容也是加密的。SRAM中的每个字节都是通过密匙及与地址相关的加密电路进行加密的，所以完全相同的字节在不同的存储位置将被保存为不同的值。

程序/数据SRAM的加密依赖于一个片上64位密匙字。该密匙是由ROM固件在应用软件被加载之前自动产生的，并且在断开V_{CC}时由锂电池备份供电电路维持为非易失信息。完成应用软件的加载后，通过设置片上安全锁对密钥进行保护，该安全锁在断开V_{CC}时也保持为非易失信息。任何尝试篡改密匙字，进而访问真正的程序/数据SRAM内容的企图，都会造成密匙字以及SRAM的内容被擦除。

在执行应用软件期间，从程序计数器或数据指针寄存器产生的DS5003逻辑地址在被送到字节宽地址总线之前都将被加密。操作码和数据在被CPU操作之前被读回并解码。类似地，程序执行期间被写入到外部NV SRAM存储器的数据值，在写操作时出现在字节宽数据总线之前也被加密。这种加密/解密过程是实时的，所以不会损失执行时间，从而使得加密电路的操作对应用软件是透明的。

DS5003的安全特性总是有效的。

安全微处理器芯片

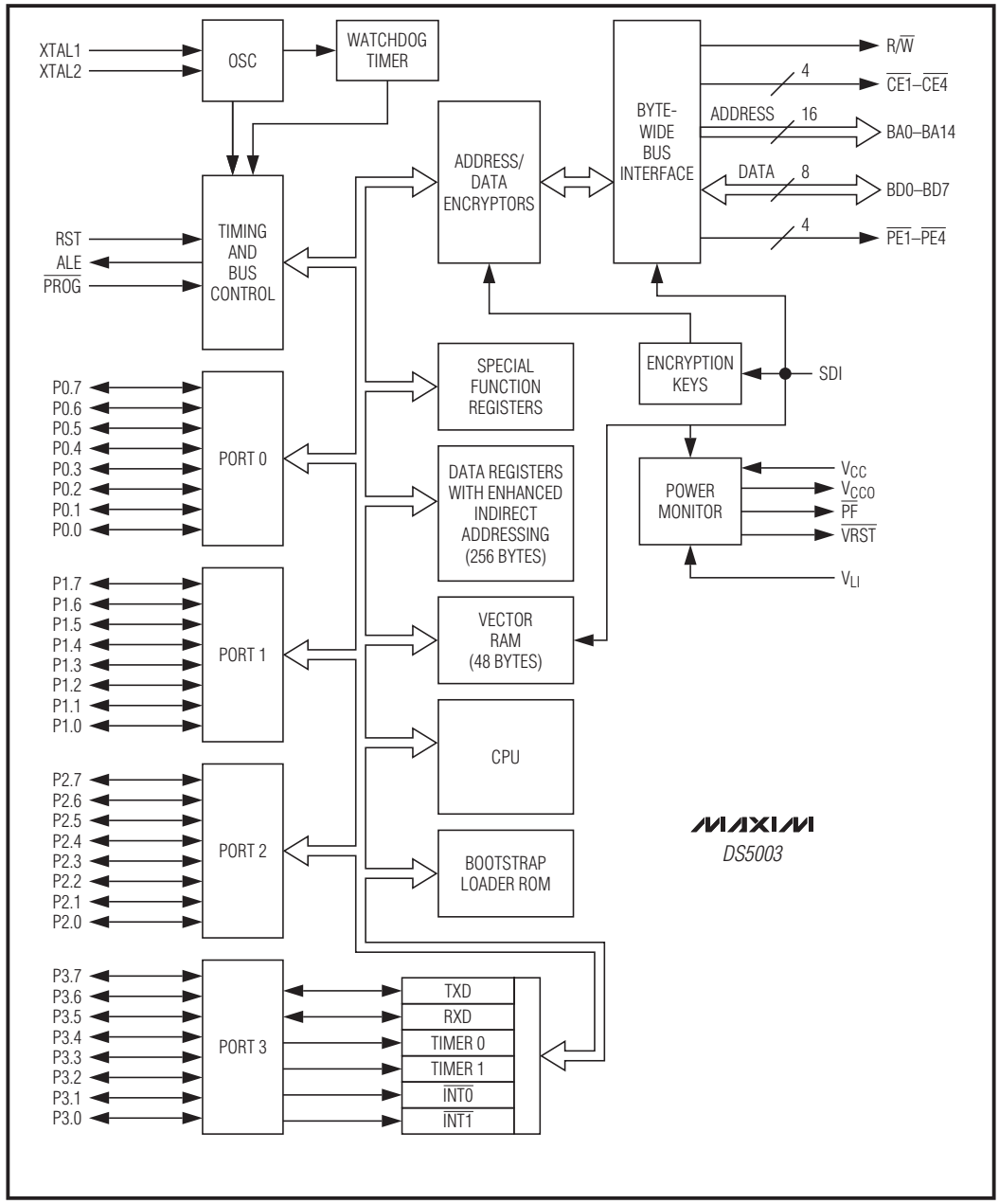

图8. 方框图

安全电路

图9所示为与DS5003的软件安全特性相关的片上功能。加密逻辑电路包括一个地址加密器和一个数据加密器。尽管每个加密器都采用各自的算法加密数据，但是两者均依赖于加密密匙寄存器中的64位密匙字。两个加密器在应用软件的加载及执行期间均工作。

地址加密器将每个逻辑地址，也就是程序执行的逻辑流中产生的正常地址序列，转换为一个加密地址(或物理地址)，也就是实际存储字节的地址。每次产生一个逻辑地址时，在程序加载或执行期间，地址加密器采用64位密匙字和地址本身的值来形成物理地址，该地址出现在SRAM的地址线上。加密算法使得每个可能的逻辑地址有且仅有一个物理地址。地址加密器在整个存储器范围内进行操作，它在引导装载期间进行配置，以便访问字节宽总线。在执行应用软件引导装载时，数据加密器将操作码、操作数或任意指定存储单元的数据字节转换为加密的表示方法。在程序执行期间，CPU每读回一个字节，内部数据加密器将其恢复为原始值。在程序执行期间，当一个字节被写入到外部非易失程序/数据SRAM时，该字节也以加密的形式进行储存。数据加密逻辑电路采用64位密匙、写入数据的逻辑地址以及数据本身的值来生成加密后的数据，并将其写入非易失程序/数据SRAM。加密算法是可重复的，所以对于给定的数据值、加密密匙值和逻辑地址，加密后的字节总是相同的。然而，由于算法依赖于逻辑地址和加密密匙，所以对于每个真实数据值来说，可能具有多个加密数据值。

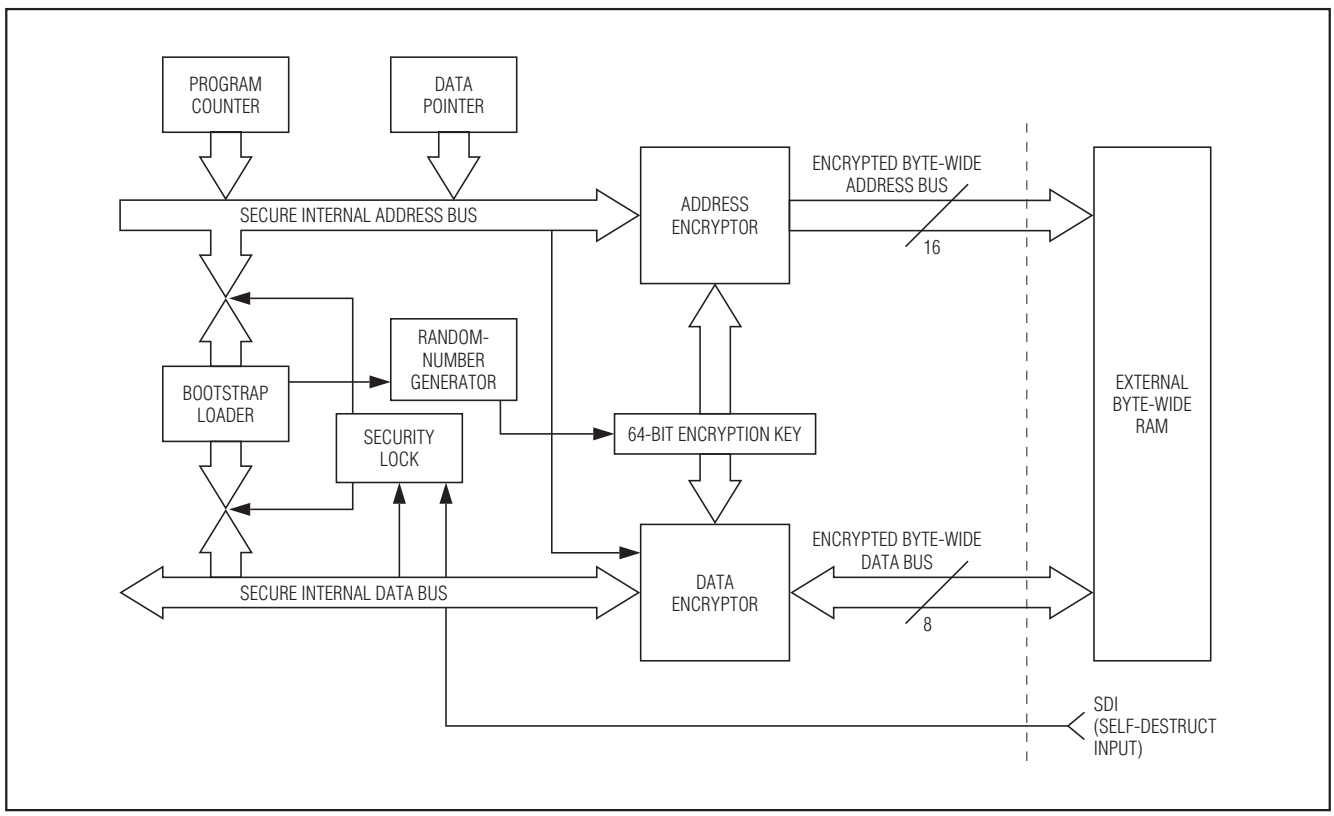

图9. 安全电路

安全微处理器芯片

执行应用软件时，DS5003的内部CPU正常工作。计算用于操作码取码周期、数据读/写操作的逻辑地址。在程序正常执行期间，DS5003可对内部产生的逻辑地址进行加密。类似地，CPU处理的是数据真实值。然而，当数据被写入到外部程序/数据SRAM时，也会被加密，并在读回时恢复为原始值。

当一个应用程序按照上述方式储存时，几乎不可能将操作码反汇编或将数据转换为其真实值。地址加密使得操作码和数据不是按照其被编译时的连续形式储存的，而是被保存在随机的存储单元。这就造成几乎无法确定正常的程序流。作为一项额外的保护措施，在程序执行期间，只要时间允许，地址加密器还会生成一个伪读周期。

伪读周期

与DS5002FP一样，在程序执行期间，只要时间允许，DS5003就会生成一个对外部SRAM存储器的非连续地址进行操作的伪读周期。这一措施使确定正常的程序流变得更加复杂。在这些伪随机伪读周期中，表面上读取了SRAM，但是在内部并不使用该数据。伪读周期和真正的读周期操作交替执行，从而很难在两者之间进行区分。

加密算法

DS5003采用了专有的硬件算法，可对SRAM字节宽总线上的地址和数据进行扰乱。其优点包括：

- 64位加密密匙(由安全锁功能加以保护)。
- 采用了类似DES的操作，具有更大程度的非线性。
- 可自定义加密方法。

加密密匙

如前所述，片上64位加密密匙是地址和数据加密器的基础。当装载器接收到特定的命令后，片上的硬件随机数发生器就会生成密匙，该操作恰好在将代码实际加载到外部SRAM之前完成。这一机制可防止通过连续加载新的已知密匙来分析加密算法，也使用户省去了保护密匙选择的负担。

随机数发生器采用了两个内部环形振荡器与处理器主时钟(由XTAL1和XTAL2决定)的异步频率差，所以产生的是真正的随机数。

向量RAM

芯片上采用了一个48字节的向量RAM区域，用来保存DS5003的复位和中断向量。这种架构有助于保证应用程序的安全。

程序执行期间，如果能够从外部非易失程序/数据RAM中获取复位和中断向量，就有可能判断出已知地址的加密值。这可通过强制中断或复位，并观察在字节宽地址/数据总线上产生的地址来实现。例如，当发生硬件复位时，程序逻辑地址被强制指向单元0000h，并且从该位置开始执行程序。那么就有可能通过观察硬件复位之后外部SRAM上出现的地址，判断出逻辑地址0000h的加密值(或物理地址)。中断向量的地址关系亦可通过类似的方式确定。通过采用片上向量RAM保存中断和复位向量，就不可能会观察到这样的关系。向量RAM避免了通过观察向量地址关系破译应用程序的可能性。需要注意的是，以上提及的伪访问操作是从向量RAM取码的。

向量RAM在引导期间自动加载Intel hex文件中的用户复位和中断向量。

安全锁

一旦应用程序被加载到DS5003的外部和向量RAM，即可在引导程序中执行Z命令启动安全锁。在设置了安全锁后，片上ROM即不再允许访问程序/数据信息。引导程序固件和DS5003的加密器电路都防止进行访问。

只有通过引导程序中的U命令清除安全锁之后，才可访问SRAM。这一动作将触发若干防篡改事件。首先，加密密匙将被立即擦除。若没有加密密匙，DS5003就不再能够解密SRAM的内容，所以应用软件就不能正确执行，也不能被引导程序以真实的形式读回；其次，向量RAM区域也被立即擦除，从而会丢失复位和向量信息；第三，引导程序固件随后会擦除加密的SRAM分区；最后，引导程序会创建并加载一个新的随机密匙。

安全锁位采用了多位锁存结构，在发生篡改时与自毁功能联动。锁的设计使其能够建立“多米诺效应”，当该位被擦除后，将产生一系列不可中止的事件，进而清除关键数据，包括加密密匙和向量RAM。此外，利用顶部敷层，还可防止该位被探针分析。

自毁输入(SDI)

自毁输入(SDI)引脚是一个高电平有效输入，用于在发生各种用户定义的外部事件时复位安全锁。SDI输入与外部篡改检测电路共同作用。无论V_{CC}引脚上是否有电源，该功能均可被激活。SDI引脚有效后将立即复位安全锁，并引起上述由此造成的一系列事件。此外，会立刻断开包括V_{CC}引脚在内的字节宽总线接口上的电源，导致外部SRAM中数据的丢失。

顶部敷层

DS5003M具有特殊的顶部敷层，可防止探针攻击。该敷层是采用特殊工艺在微控制器管芯增加第二层金属实现的。增加的敷层并不是简单的金属片，而是一种复杂的设计结构，与电源和地交织在一起，进而又被连接到加密密匙和安全锁的逻辑电路。所以，任何尝试去除敷层或通过敷层进行探测的企图，都会造成安全锁被擦除和/或加密密匙位的丢失。

引导程序

DS5003初始加载应用程序是通过片上引导装载器中的固件与PC采用片上串口进行通信实现的。表1概括了引导程序接受的命令。

当调用引导程序时，256字节的暂存RAM分区将被自动填充为零，然后用于引导固件的变量存储。此外，通过随机数发生器电路生成一组8字节数据，并保存作为64位加密密匙的一个可能的字。

只有在安全锁位处于清除状态时，才能对DS5003的外部程序/数据SRAM进行读或写操作。因此，加载程序的第一步应该是通过U命令清除安全锁位。

表1. 串行引导命令

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.

执行特定的引导命令会将新产生的64位随机数加载到加密密匙字。这些命令如下：

填充　F

加载　L

转存　D

校验　V

CRC　C

执行填充和加载命令将会利用新产生的加密密匙字中的密匙把加密的数据加载到SRAM。随后*在同一引导进程中*执行转存命令，将会把加密SRAM的内容读出并以解密的

安全微处理器芯片

形式送回到主PC。类似地，*在同一引导进程中*执行校验命令将会把送来的绝对十六进制数据与加密SRAM的真实内容进行比较，CRC命令将返回根据加密SRAM的真实内容计算出的CRC值。只要*在同一引导进程中*执行任意这些命令，加载的密匙值都保持相同，并且在设置安全锁位之前，可以任意、正常地读或写加密程序/数据SRAM。

当使用Z命令设置安全锁位后，就不能再用任何引导命令或其它任何方法访问真正的SRAM内容。

关于串行引导操作的更多介绍，请参阅*安全微控制器用户指南*(English only) (china.maxim-ic.com/SecureUG)。

指令集

DS5003的指令集是与业内标准8051微控制器兼容的目标代码。所以，为8051编写的软件开发包，例如汇编程序和编译器，均兼容DS5003。关于指令集和操作的完整说明请参阅*安全微控制器用户指南*(English only)。

存储器结构

图10所示为DS5003可访问的存储器映射。整个64kB程序和64kB数据存储区均可用于字节宽总线。这样就将I/O端口保留给用户使用。用户通过选择程序范围和数据范围

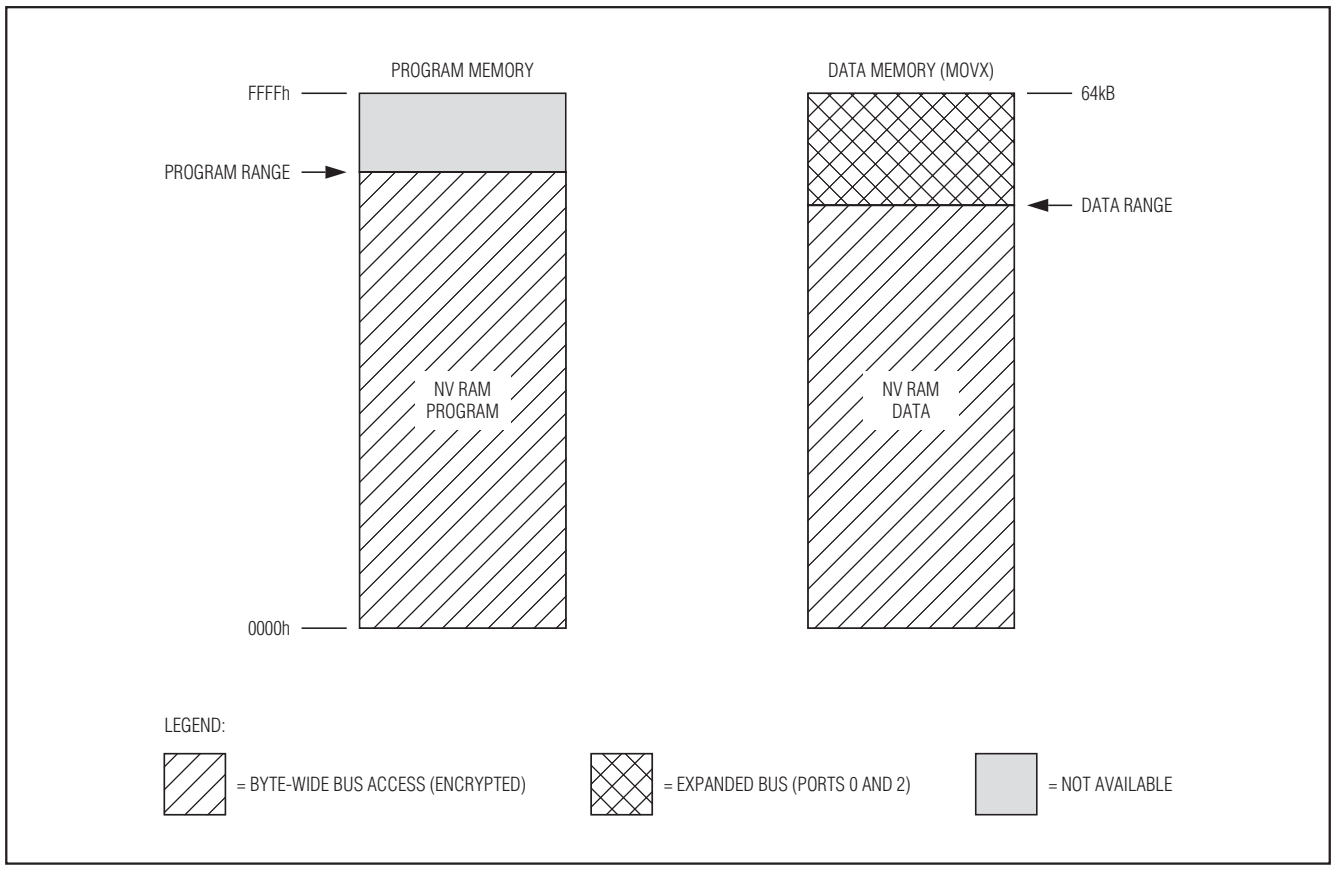

图10. 不可拆分模式下的存储器映射(PM = 1)

来控制实际映射到字节宽总线的存储器部分。任何未被映射到SRAM的分区均可通过端口0和2上的扩展总线访问。另一种配置允许对一个64kB的空间进行动态分区，如图11所示。选择PES = 1即可提供另外64kB可能的数据存储空间或存储器映射的外围空间，如图12所示。这些选择是通过特殊功能寄存器实现的。关于存储器映射及其控制的详细信息，请参阅*安全微控制器用户指南*(English only)。

图13所示为采用一个128kB SRAM的典型存储器连接。注意，在这种配置下，程序和数据均被储存在一个共用的SRAM芯片中。图14所示为采用两个32kB SRAM的类似系统。字节宽地址总线连接到SRAM的地址线。双向字节宽数据总线连接到SRAM的数据I/O线。

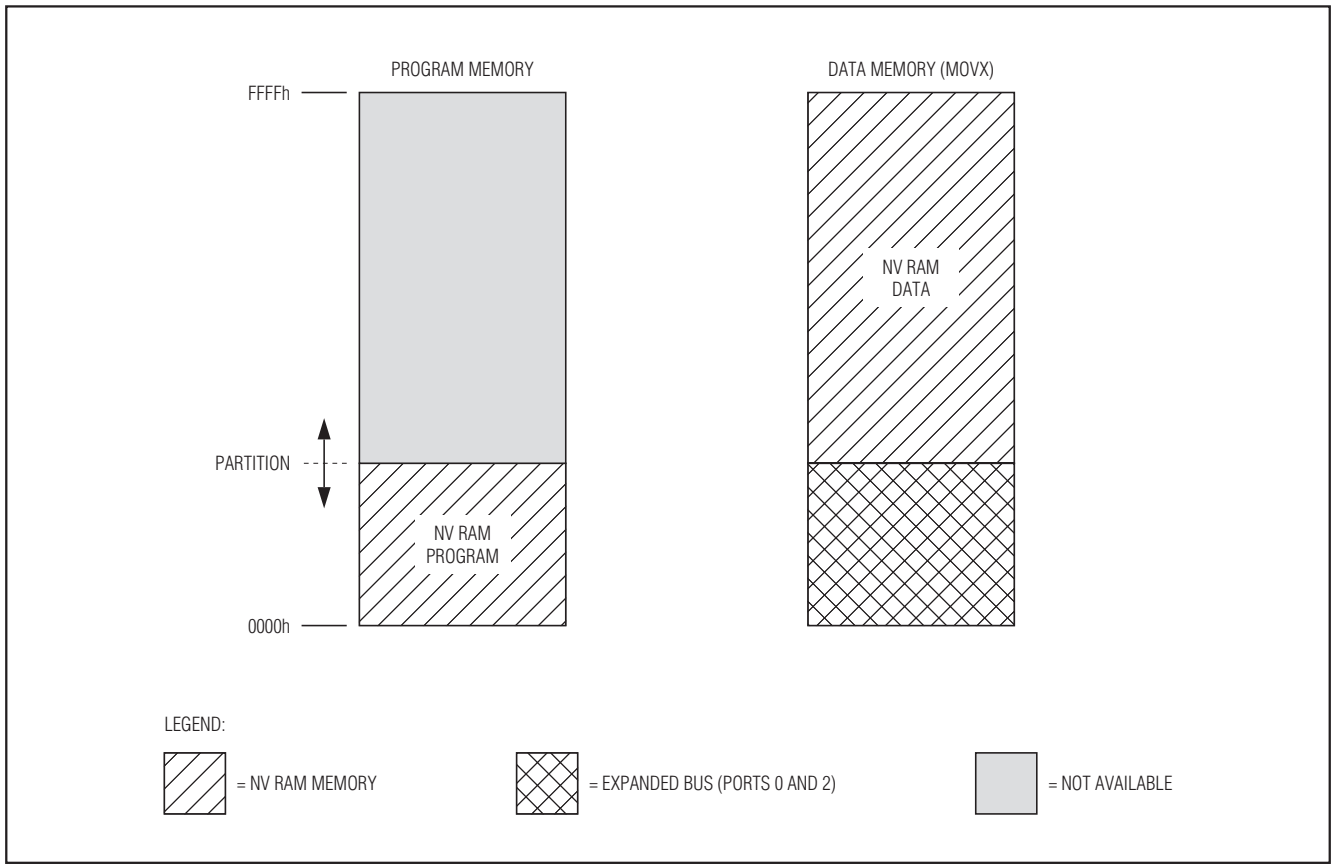

图11. 可拆分模式下的存储器映射(PM = 0)

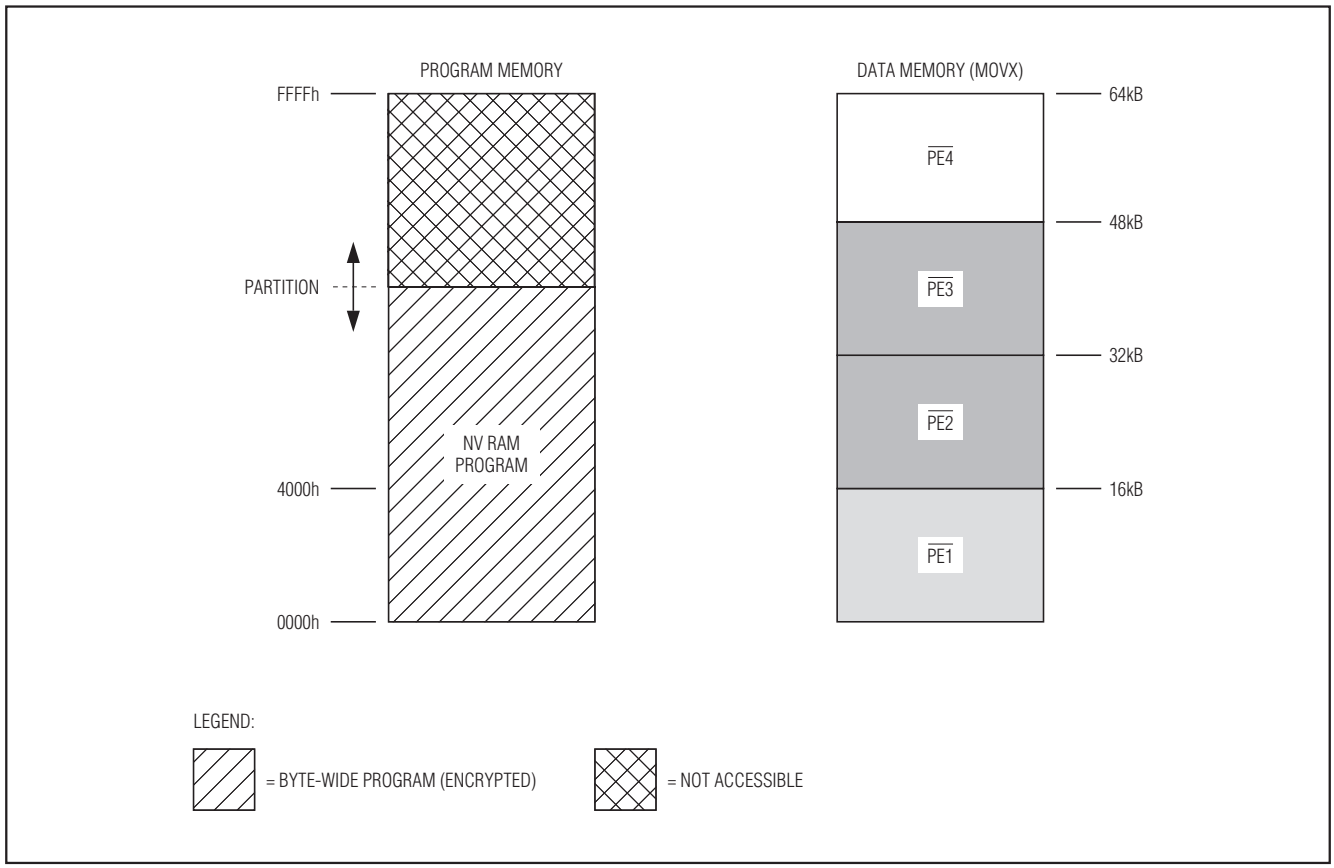

图12. PES = 1时的存储器映射

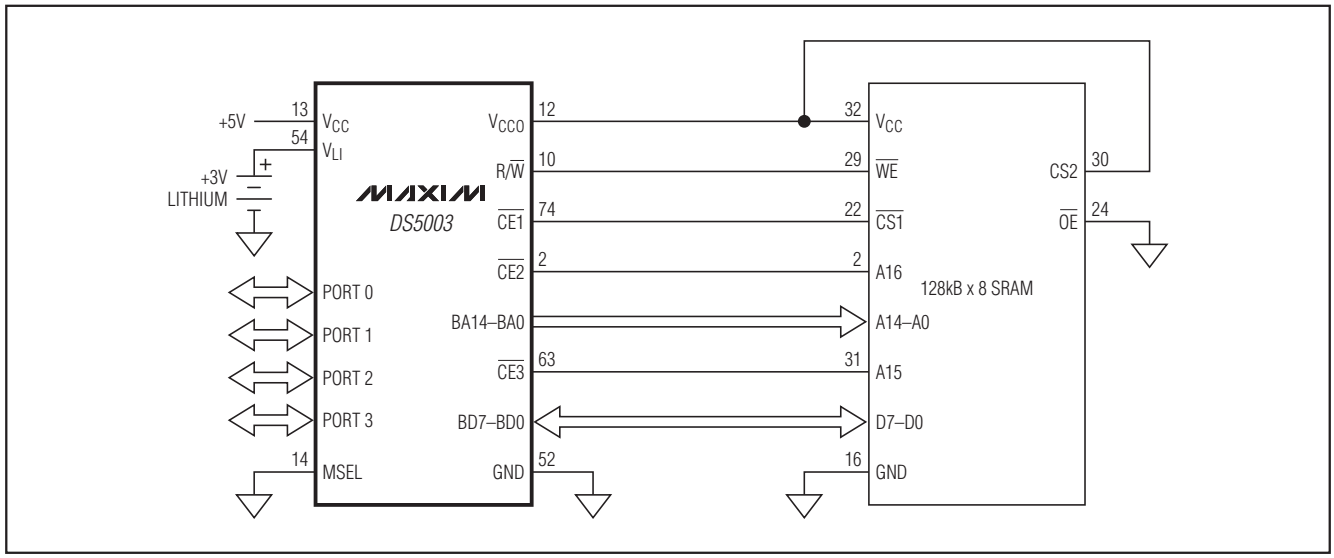

图13. 连接至128kB x 8 SRAM

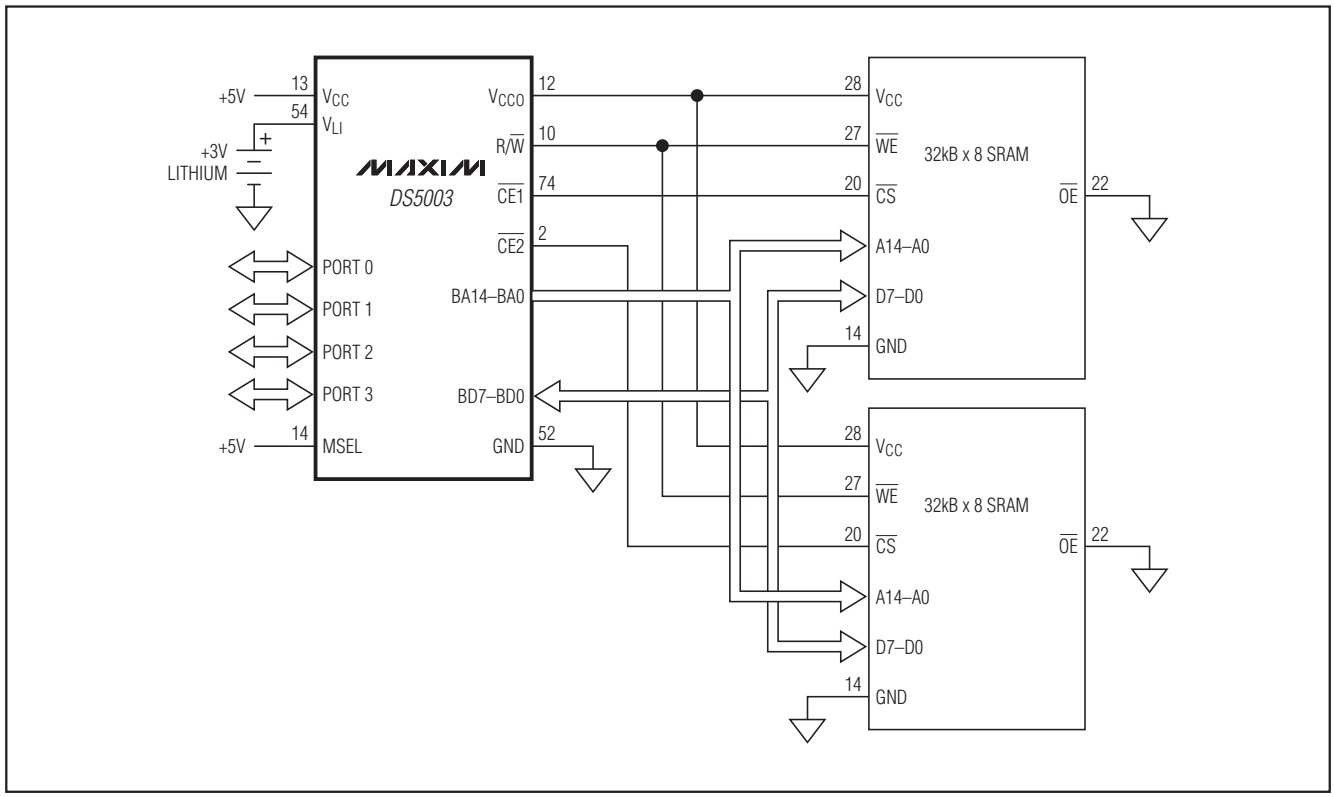

图14. 连接至64kB x 8 SRAM

电源管理

DS5003通过监测V_{CC}来实现电源失效复位、电源失效预警中断、以及转换至锂电池备份供电。采用内部带隙基准来判断切换点，切换点分别称为V_{PFW}、V_{CCMIN}和V_{LI}。如果使能电源失效报警，当V_{CC}降至低于V_{PFW}时，DS5003执行一个中断，向量指向存储单元2Bh。处理器的全部功能将继续工作。当电源进一步下降至V_{CCMIN}时，DS5003将调用复位状态。在电源再次上升到高于V_{CCMIN}之前，不执行任何代码。所有的解码芯片使能信号和R/$\overline{W}$信号都变为无效(逻辑1)状态。此时，V_{CC}仍然作为电源。当V_{CC}进一步下降至低于V_{LI}时，内部电路将切换至由锂电池供电。此时大多数内部电路是关闭的，仅维持非易失状态，连接到V_{CCO}的所有器件都由锂电池供电。V_{CCO}电压为锂电池电压减去约0.45V (低于一个二极管压降)，并取决于负载情况。因此，应该使用低功耗SRAM。当使用DS5003时，用户必须选择与SRAM的数据保持电流和要求的备份时间相匹配的电池。注意，只有当$V_{CC} < V_{LI}$时才使用锂电池。关于更多的详细信息，请参阅*安全微控制器用户指南*(English only)。电气参数部分给出了跳变点V_{CCMIN}和V_{PFW}的值。

封装信息

如需最近的封装外形信息和焊盘布局，请查询**china.maxim-ic.com/packages**。

封装类型	封装编码	文档编号
80 MQFP	M80+2	21-0271

引脚配置