DS2460
带有 EEPROM 的 SHA-1 协处理器

www.maxim-ic.com.cn

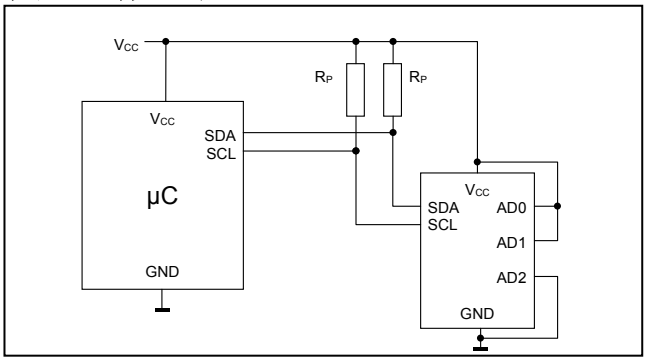
概述

带EEPROM的SHA-1 协处理器DS2460 是ISO/IEC 10118-3 安全散列算法(SHA-1)的硬件实施方案，无需开发执行复杂SHA计算的软件，即可鉴别SHA器件以及验证数字签名服务数据的有效性。DS2460 通过广泛使用的I^2C接口与微控制器通信。其应用包括主机访问控制、电子支付系统的令牌认证和服务数据确认，以及为短消息加密生成一次性的加密密钥和为消息解密生成长度不超过SHA-1 计算结果（20 字节）的解密密钥。

应用

授权管理
安全管理
系统认证
防克隆
门锁
电表

典型工作电路



特性

- 专用的硬件加速 SHA 引擎，用来计算 SHA-1 MAC
- 112 字节的用户 EEPROM, 用于存储终端设备的特征数据
- I^2C主机接口支持 100kHz和 400kHz通信速率
- I^2C地址分配由 3 个地址输入控制
- 单字节至 8 字节 EEPROM 写序列
- 64 位唯一注册码
- EEPROM 可承受：25°C 下 200k 写次数，每次 8 字节块操作
- 10ms 最大 EEPROM 写周期
- 较宽的工作电压范围和工作温度范围：2.7V 至 5.5V，-40°C 至+85°C
- 所有引脚都具有±4kV IEC 1000-4-2 ESD 保护
- 8 引脚 SO (150mil)封装

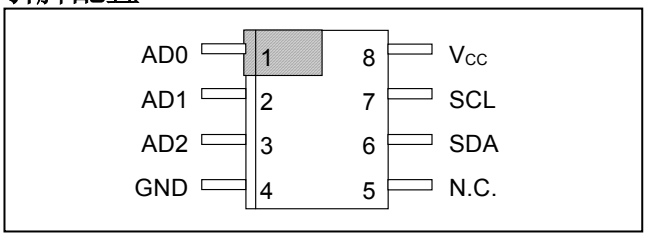
定购信息

PART	TEMP RANGE	PIN-PACKAGE
DS2460S	-40°C to +85°C	8 SO (150 mils)
DS2460S/T&R	-40°C to +85°C	8 SO (150 mils)
DS2460S+	-40°C to +85°C	8 SO (150 mils)
DS2460S+T&R	-40°C to +85°C	8 SO (150 mils)

+表示无铅封装。

申请完整的数据资料，请访问：
www.maxim-ic.com.cn/fullds/ds2460

引脚配置



注: 该器件的一些修订可能与已经发表的勘误表规格不同，通过不同的销售途径有可能同时获得不同修订版的器件。查询器件的勘误表信息，请点击: www.maxim-ic.com.cn/errata。

ABSOLUTE MAXIMUM RATINGS

Voltage Range on Any Pin Relative to Ground	-0.5V, +6V
Maximum Current Into Any Pin	±20mA
Operating Temperature Range	-40°C to +85°C
Junction Temperature	+150°C
Storage Temperature Range	-55°C to +125°C
Soldering Temperature	See IPC/JEDEC J-STD-020

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 the absolute maximum rating conditions for extended periods may affect device.

ELECTRICAL CHARACTERISTICS

(-40°C to +85°C, see Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.7		5.5	V
Standby Current	I_{CCS}	Bus idle			3	µA
		Bus idle, +25°C			1	
Operating Current	I_{CCA}	Bus active at 400kHz		250	500	µA
Programming Current	I_{PROG}			500	1000	µA
SHA-1 Computation Current	I_{SHA}	See full version of data sheet				mA
SHA-1 Engine						
SHA-1 Computation Time	t_{SHA}	See full version of data sheet				ms
EEPROM						
Programming Time	t_{PROG}				10	ms
Endurance	N_{CYCLE}	At +25°C (Notes 2, 3)	200k			
Data Retention	t_{RET}	At +85°C (Notes 4, 5, 6)	40			years
I²C-Pins (Note 7) See Figure 6						
LOW Level Input Voltage	V_{IL}	(Note 8)	-0.5		0.3 × V_{CC}	V
HIGH Level Input Voltage	V_{IH}	(Notes 8, 9)	0.7 × V_{CC}		V_{CC} + 0.5V	V
Hysteresis of Schmitt Trigger Inputs	V_{hys}	(Note 9)	0.05 × V_{CC}			V
LOW Level Output Voltage at 4mA Sink Current	V_{OL}				0.4	V
Output Fall Time from V_{Ihmin} to V_{ILmax} with a Bus Capacitance from 10pF to 400pF	t_{of}	(Note 9)	20 + 0.1Cb		250	ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}	SDA and SCL pins only (Note 9)			50	ns
Input Current Each I/O Pin with an Input Voltage Between $0.1V_{CCmax}$ and $0.9V_{CCmax}$	I_i	(Notes 8, 10)	-10		10	µA
Input Capacitance	C_i	(Notes 8, 9)			10	pF
SCL Clock Frequency	f_{SCL}		0		400	kHz
Hold Time (Repeated) START Condition. After this Period, the First Clock Pulse is Generated.	$t_{HD:STA}$		0.6			µs
LOW Period of the SCL Clock	t_{LOW}		1.3			µs
HIGH Period of the SCL Clock	t_{HIGH}		0.6			µs

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Setup Time for a Repeated START Condition	$t_{SU:STA}$		0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 11, 12)			0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Note 13)	100			ns
Setup Time for STOP Condition	$t_{SU:STO}$		0.6			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}		1.3			µs
Capacitive Load for Each Bus Line	C_b	(Note 14)			400	pF

Note 1: Specification at -40°C is guaranteed by design and characterization only and not production tested.
Note 2: Write-cycle endurance is degraded as T_A increases.
Note 3: Not 100% production-tested; guaranteed by reliability monitor sampling.
Note 4: Data retention is degraded as T_A increases.
Note 5: Guaranteed by 100% production test at elevated temperature for a shorter amount of time; equivalence of this production test to data sheet limit at operating temperature range is established by reliability testing.
Note 6: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended; the device can lose its write capability after 10 years at +125°C or 40 years at +85°C.
Note 7: All values are referred to V_{IHmin} and V_{ILmax} levels.
Note 8: Applies to SDA, SCL, AD2, AD1, AD0.
Note 9: Guaranteed by simulation only, not production tested.
Note 10: I/O pins of the DS2460 do not obstruct the SDA and SCL lines if V_{CC} is switched off.
Note 11: The DS2460 provides a hold time of at least 300ns for the SDA signal (referred to the V_{IHmin} of the SCL signal) to bridge the undefined region of the falling edge of SCL.
Note 12: The maximum $t_{HD:DAT}$ has only to be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal.
Note 13: A Fast-mode I²C-bus device can be used in a standard-mode I²C-bus system, but the requirement $t_{SU:DAT} \geq$250ns must then be met. This is automatically the case if the device does not stretch the LOW period of the SCL signal. If such a device does stretch the LOW period of the SCL signal, it must output the next data bit to the SDA line tr max + $t_{SU:DAT}$ = 1000 + 250 = 1250ns (according to the standard-mode I²C-bus specification) before the SCL line is released.
Note 14: C_B = total capacitance of one bus line in pF. If mixed with HS-mode devices, faster fall-times according to I²C-Bus Specification v2.1 are allowed.

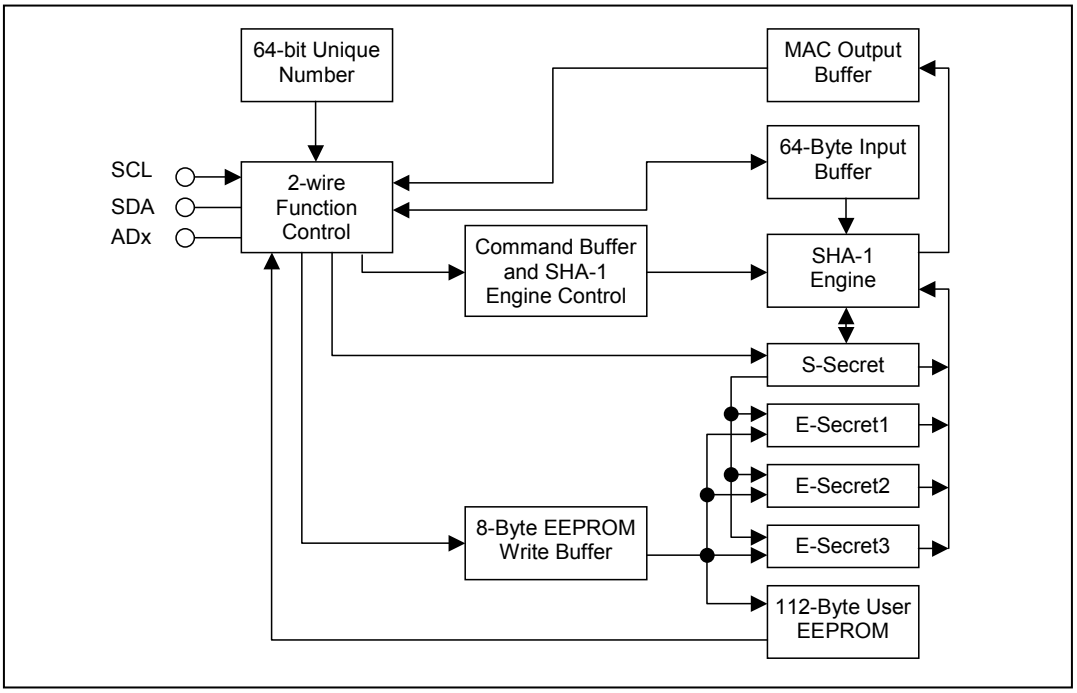
引脚说明

引脚	名称	功能
1	AD0	I^2C地址输入；必须接VCC或GND。这些输入决定器件的I^2C从地址，参见图 5。
2	AD1	
3	AD2	
4	GND	地参考。
5	NC	空脚。
6	SDA	I^2C串行数据输入/输出；该引脚必须通过一个上拉电阻接V_{CC}。
7	SCL	串行时钟输入；该引脚必须通过一个上拉电阻接V_{CC}。
8	V_{CC}	电源输入。

综述

DS2460 主控制器和存储器部分之间的关系框图如图 1 所示。DS2460 通过标准模式或高速模式下的I^2C总线接口与主机处理器通信。3 个地址引脚的逻辑状态确定了DS2460 的I^2C从地址，一条总线上允许挂接多达 8 个器件，无需集线器。更多信息(包括图 2)请参阅完整的数据资料。

图 1. 内部框图



寄存器详细描述

该部分内容 (包括图 3)请参考完整的数据资料。

器件工作情况

应用中DS2460 的典型功能包括写、读、运行SHA-1 引擎、传输密钥和比较MAC。所有这些活动均通过I^2C串行接口控制。

I^2C串行通信接口

一般特性

I^2C总线通过数据线(SDA)和时钟信号(SCL)进行通信。SDA和SCL是双向传输线，通过上拉电阻连接到正电源电压。不进行通信时SDA和SCL均为高电平。连接到总线的器件输出级必须是漏级开路或集电极开路，以满足线与功能。标准模式下I^2C总线数据的传输速率可达100kbps，高速模式下可达400kbps。DS2460可工作在两种模式下。

总线上发送数据的器件被定义为发射机，接收数据的器件为接收器。控制通信的器件称为“主机”。由主机控制的器件是“从器件”。为了实现单独访问，各器件必须有一个从地址，且不和总线上其他器件相冲突。

当总线空闲时才能进行数据传输。主机产生串行时钟(SCL)，控制总线访问，发出启动和停止条件，并决定在启动和停止条件之间传输的数据字节的个数(图 4)。 数据传输时首先传送的是最高有效位。每个字节之后跟着的是应答位，以实现主机和从器件之间的同步。

从地址

DS2460 响应的从地址见图 5。地址引脚 AD0、AD1 和 AD2 的逻辑状态决定地址位 A0、A2 和 A4 的值。地址引脚允许器件对八个可能的从地址当中的一个做出响应。从地址是从地址/控制字节的一部分。从地址/控制字节(R/$\overline{W}$)的最后一位定义数据方向。设置为 0 时，随后数据将从主机发往从器件（写访问模式），设置为 1 时，数据将由从器件到主机(读访问模式)。

图 4. I²C协议概括说明

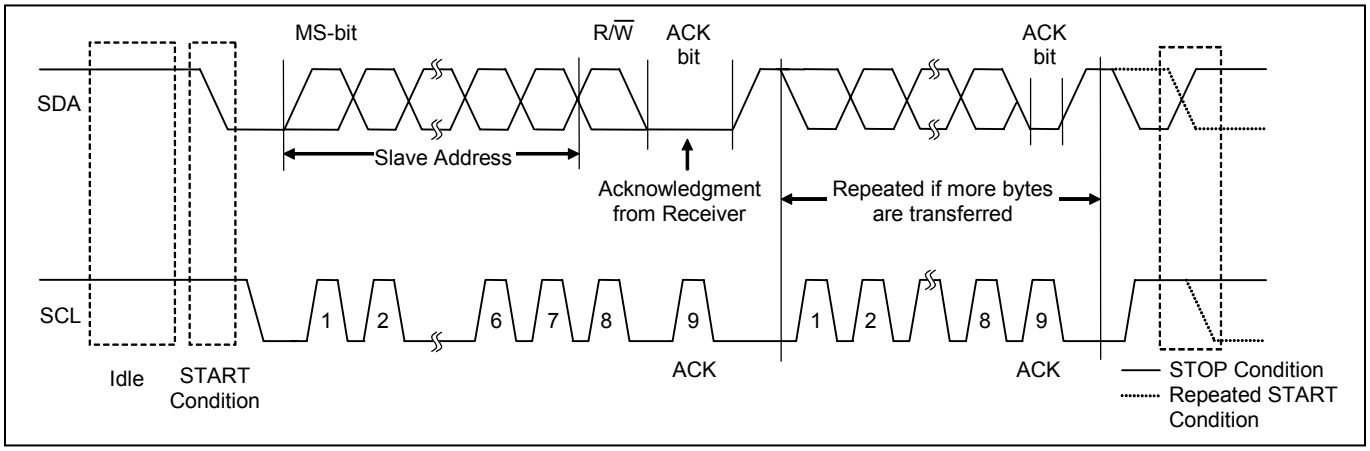
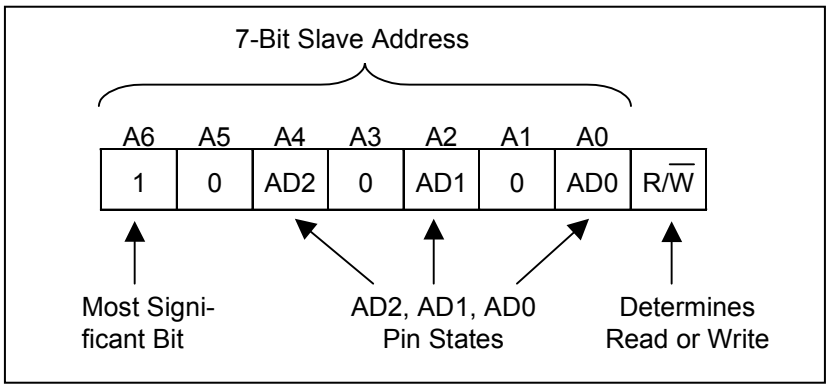


图 5. DS2460 从地址



I²C定义

下面列出通常用来描述I²C数据传输的一些术语。时序参考见图6。

总线空闲或非忙状态

SDA和SCL空闲，此时逻辑状态为高电平。

启动条件

为了与从器件进行数据传输，主机产生启动条件。SCL保持高电平时，SDA从高电平跳变为低电平将产生一个启动条件。在随后的其它启动条件被确认前，主机必须发送一个有效从地址，且被从器件确认。

停止条件

为了终止与从器件之间的数据传输，主机产生停止条件。SCL保持高电平时，SDA从低电平跳变为高电平将产生一个停止条件。在随后的其它停止条件被确认前，主机必须发送一个有效从地址，且被从器件确认。

重复启动条件

重复启动通常用于读访问，以选择进行读访问的特定数据源或地址。在一次数据传输结束后，主机可以使用重复启动条件，说明它会在当前传输结束后立即启动一次新的数据传输。重复启动条件的触发与通常的启动条件一样，只是在停止条件之后，总线不会处于空闲状态而已。

数据有效

除启动和停止条件之外，SDA的跳变必须发生在SCL低电平期间。在整个SCL高电平期间、并在建立时间和保持时间(SCL下降沿后$t_{HD:DAT}$，SCL上升沿前$t_{SU:DAT}$，参见图6)要求的范围内，SDA数据须保持稳定有效。每位数据对应一个时钟脉冲，在SCL脉冲的上升沿数据被移入接收器件。

写操作完成后，主机必须释放SDA线，以保证在下一个SCL上升沿之前有充足的建立时间(最小值$t_{SU:DAT} + t_R$，见图6)启动读操作。在SDA总线的前一个SCL脉冲下降沿，从器件逐位移出数据，数据位在当前SCL脉冲的上升沿时有效。主机产生所有的SCL时钟脉冲，包括那些读从器件数据所需的时钟。

应答

通常，寻址的接收器件收到每一个字节后，必须生成一个应答信号。主机必须生成一个与该应答位相关的时钟脉冲。应答时钟脉冲期间应答器件必须拉低SDA，即在相关的应答时钟脉冲为高期间，并在所需的建立和保护时间(SCL下降沿后$t_{HD:DAT}$，SCL上升沿前$t_{SU:DAT}$)内，SDA稳定为低电平。

从器件未应答

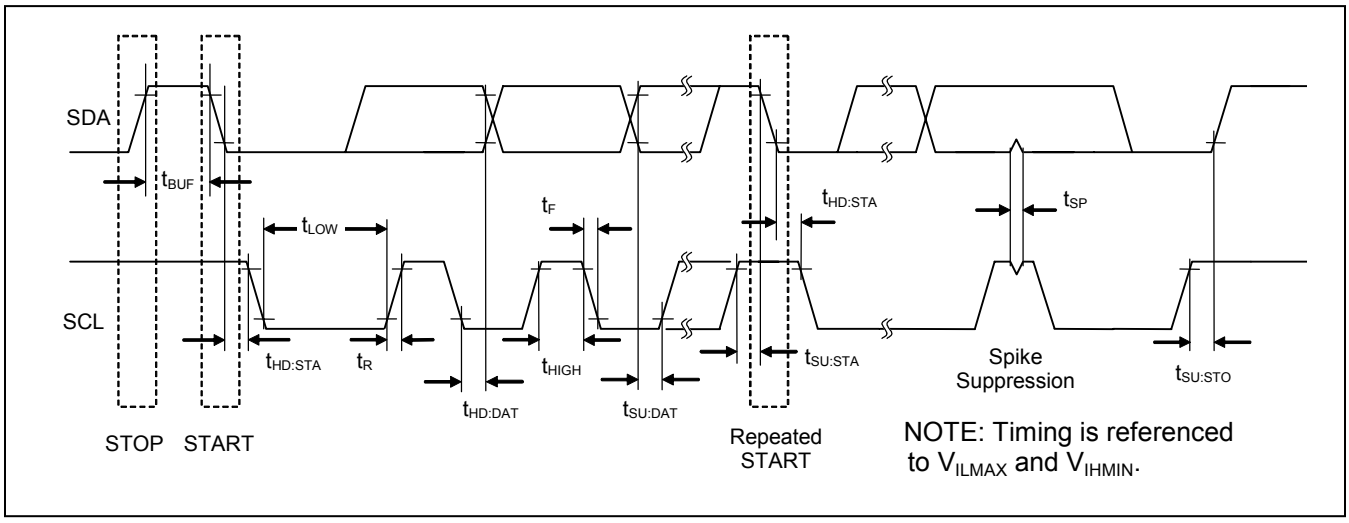
当从器件忙于执行一个实时任务，如MAC计算或EEPROM写周期时，从器件也许无法接收或传送数据。在这种情况下从器件不会应答其从地址，SDA线为高电平。

准备好通信的从器件至少会对其从地址做出应答。但是，有时从器件也许会拒绝接收数据，如，由于无效命令或访问模式，或发非匹配MAC。在这种情况下从器件对其所拒绝接收的任何字节不进行应答，并使SDA为高。无论如何，在从器件应答失败之后，主机首先需要生成重复启动条件，或在停止条件后跟一个启动条件以重新开始数据传送。

主机未应答

有时当接收数据时，主机必须向从器件发送一个数据终止信号。为了获得这一信号，主机不应答它从从器件接收到数据的最后一个字节。作为响应，从器件释放 SDA，允许主机发出停止条件。

图 6. I^2C时序图



读和写

有关不同寄存器和EEPROM的读、写操作，请参考完整的数据资料。

SHA-1引擎控制

这部分内容为用户介绍 SHA-1 引擎及其操作，请参考完整的数据资料 (包括图 7-9 和表 1、表 2)。

SHA-1算法

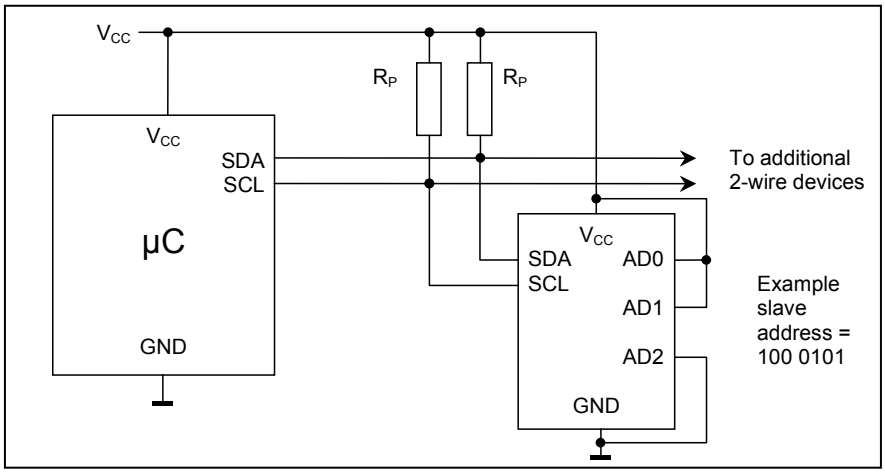
以下有关SHA算法的说明译自安全散列标准（Secure Hash Standard）SHA-1文档，可以从NIST网站下载（www.itl.nist.gov/fipspubs/fip180-1.htm）。详细信息请参考完整的数据资料。

应用信息

SDA 和 SCL 上拉电阻

DS2460 的 SDA 是漏极开路输出，需要一个上拉电阻器(图 10)来实现逻辑高电平。由于 DS2460 只把 SCL 做为输入(无时钟伸展)，因此主机可以通过一个带上拉电阻器的漏极开路/集电极开路输出或推挽式输出驱动 SCL。

图 10. 应用电路原理图



上拉电阻R_P的大小

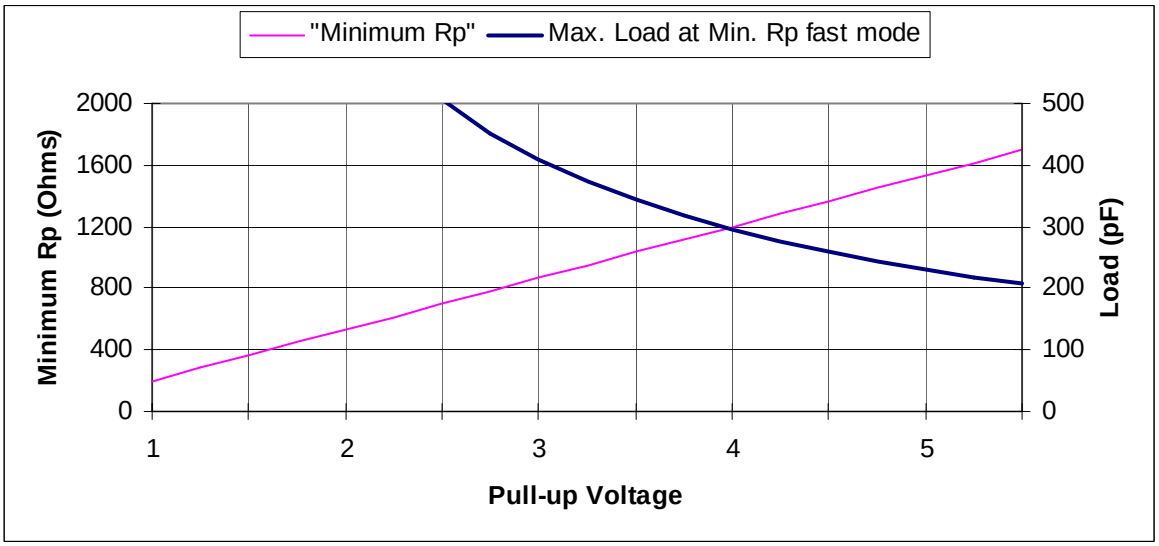
根据I^2C规范，从器件在V_{OL}为0.4V时必须至少能吸收3mA电流。这种DC条件决定了上拉电阻器的最小值：**$R_{PMIN} = (V_{CC} - 0.4V)/3mA$**。工作电压为5.5V时，上拉电阻器最小值为1.7kΩ。图11中的“Minimum R_P”曲线显示了上拉电阻器最小值随工作（上拉）电压的变化情况。

对于I^2C系统，在上拉电压的30%至70%时来测量上升时间和下降时间。总线电容C_B最大值为400pF。最大上升时间不能超过300ns。假定上升时间取最大值，则给定电容C_B时电阻器R_P的最大值为：**$R_{PMAX} = 300ns/(C_B*ln(7/3))$**。总线电容为400pF时上拉电阻器最大值为885Ω。

如果上拉电阻取885Ω，为了符合总线电容取400pF时上升时间的要求，885Ω上拉电阻比5.5V时要求的R_{PMIN}要低，因此必须找出另一种方法。首先计算在任何指定的工作电压(“ Minimum R_P ”曲线)下的最小上拉电阻，然后计算获得300ns上升时间的相应总线电容，就可生成如图11所示的“ Max. Load… ”曲线。

只有当上拉电压为3V或更低时，才可以保持最大允许总线电容为400pF。若上拉电压为4V或更低，则总线电容可以减小到300pF。高速工作模式下，上拉电压为任意值时，总线电容均不能大于200pF。与上拉电压值对应的上拉电阻值如“ Minimum R_P ”曲线所示。

图 11. I^2C 高速模式下的上拉电阻选择曲线



封装信息

(本数据资料给出的封装图并非最新版本，如需最新版本的封装尺寸，请查询：**www.maxim-ic.com.cn/DallasPackInfo**。)

Maxim北京办事处

北京8328信箱邮政编码100083
免费电话：800 810 0310
电话：010-6211 5199
传真：010-6211 5299