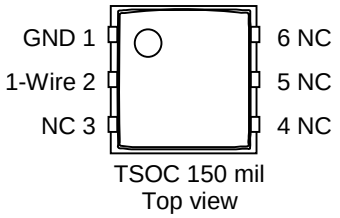
DS2432
带有 SHA-1 引擎保护的 1k位 1-Wire EEPROM

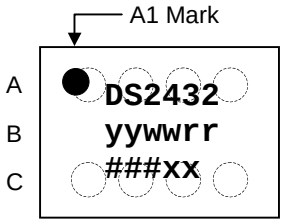
特性

- 1128 位 5V EEPROM 存储器，分为四页，每页 256 位，64 位只写密钥和多达五个通用读/写寄存器
- 内置 512 位 SHA-1 引擎，用于计算 160 位信息鉴定码（MAC）或生成密钥
- 写访问需要知道密钥，并且能够计算和传送 160 位 MAC，以鉴别真伪
- 可以对密钥和数据存储器加写保护（所有页或者只是第 0 页），或者将它们置于 EPROM 仿真模式(“写入 0”，第 1 页)
- 唯一的、由工厂光刻并经过测试的 64 位注册号没有任何两个器件相同，保证绝对可溯
- 内置多点控制，保证兼容于其它 1-Wire® 网络产品
- 将控制、寻址、数据和供电集于一个数据引脚
- 直接与微处理器的单个端口连接，通信速率达 16.3kbps
- 高速模式下速率可提高至 142kbps
- 低成本、6 引脚 TSOC 表面贴封装或 6 焊球 µCSP 封装
- 可以在-40°C 至 +85°C、2.8V 至 5.25V 宽压范围内进行读、写操作

引脚配置



TSOC 150 mil
Top view



µCSP*, Top View with Laser Mark, Contacts Not Visible.

A2 = 1-WIRE
A3 = GND
All Other Bumps: NC

yywwrr = Date/Revision
###xx = Lot Number

See 56-G7006-002 for package outline.
* Refer to package reliability report for important guidelines on qualified usage conditions.

定购信息

DS2432P	6 引脚 TSOC 封装
DS2432P/T&R	DS2432P 卷带
DS2432P+	6 引脚 TSOC 封装
DS2432P+T&R	DS2432P+卷带
DS2432X	µCSP，10k 卷带
DS2432X-S	µCSP，2.5k 卷带

+表示无铅封装。

申请完整的数据资料，请访问：
www.maxim-ic.com.cn/fullds/DS2432

1-Wire 是 Dallas Semiconductor Corp.的注册商标。

简介

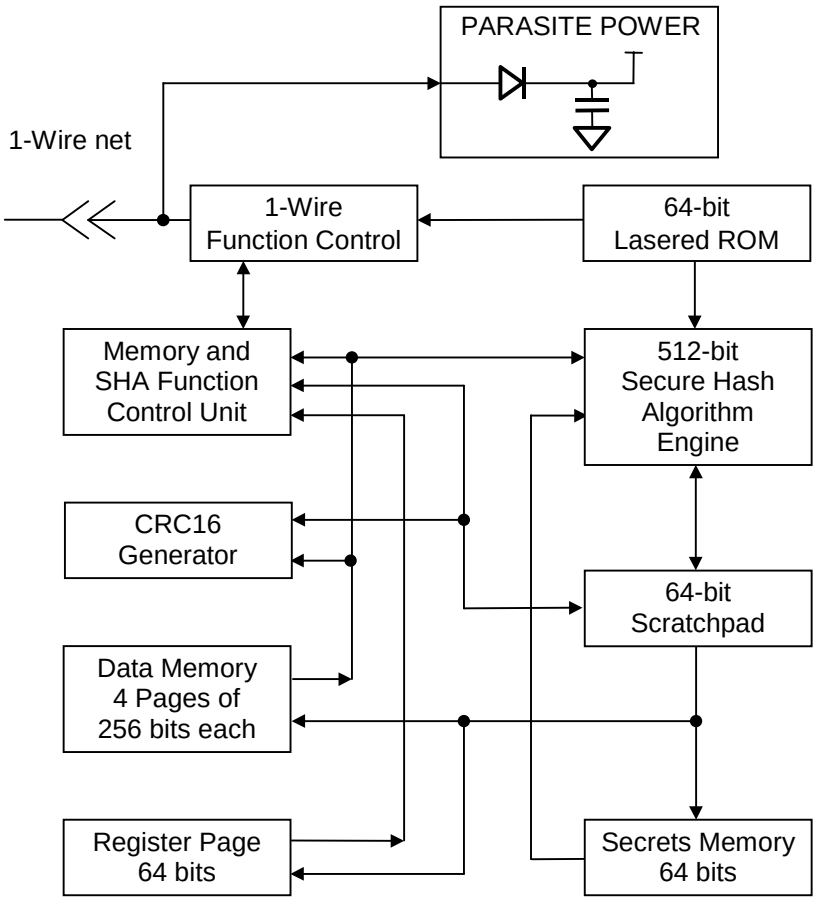
DS2432 在单个芯片内集成了 1024 位 EEPROM、64 位密钥、一个 8 字节的寄存器/控制页(其中包含五个用户读/写字节)、512 位 SHA-1 引擎和一个全功能的 1-Wire 接口。每个 DS2432 具有自身的、由工厂刻入的 64 位 ROM 注册码，可确保唯一识别、绝对可溯。数据按照 1-Wire 协议串行传送，只需一根数据线和返回地线。DS2432 有一个称为暂存器的辅助存储区，在向主存储器、寄存器写入数据时，或者在安装新密钥时充当缓冲器。数据首先被存入暂存器，并可从这里读回。经过验证后，假定 DS2432 接收到了匹配的 160 位 MAC，那么 Copy Scratchpad（复制暂存器）命令

将把数据传送到最终的存储单元。MAC 的计算涉及到存储在 DS2432 中(包含器件身份寄存器)的密钥和附加数据。只有加载新的密钥时才无需提供 MAC。当读取存储页或是计算新密钥的时候，也可以激活 SHA-1 引擎来计算 160 位的 MAC，而不必加载它。DS2432 的典型应用包括：知识产权安全性检测、消费品的售后管理和数据装载器认证等。

概述

图 1 中的框图说明了DS2432 的主控部分和存储单元之间的关系。DS2432 有五个主要的数据部件：1）64 位光刻ROM，2）64 位暂存器，3）四个 32 字节的EEPROM页，4）64 位寄存器页，5）64 位密钥存储器，6）一个 512 位SHA-1（安全散列算法）引擎。1-Wire协议分层结构见图 2。总线主机必须首先提供七个ROM操作命令中的一个：1）Read ROM, 2） Match ROM, 3）Search ROM, 4）Skip ROM, 5）Resume Communication, 6）Overdrive Skip ROM或 7）Overdrive Match ROM。一旦以标准速率完成Overdrive ROM命令，器件就进入高速模式，随后的所有通信都以高速进行。图 9 说明了协议所要求的这些ROM操作命令。成功地执行了ROM操作命令后，就可以进行存储器操作，主机可以发出七条存储器中的任何一个。图 7 * 说明了有关这些存储器和SHA操作命令的协议。所有数据读写都是LSB在前。

DS2432 原理框图 图 1

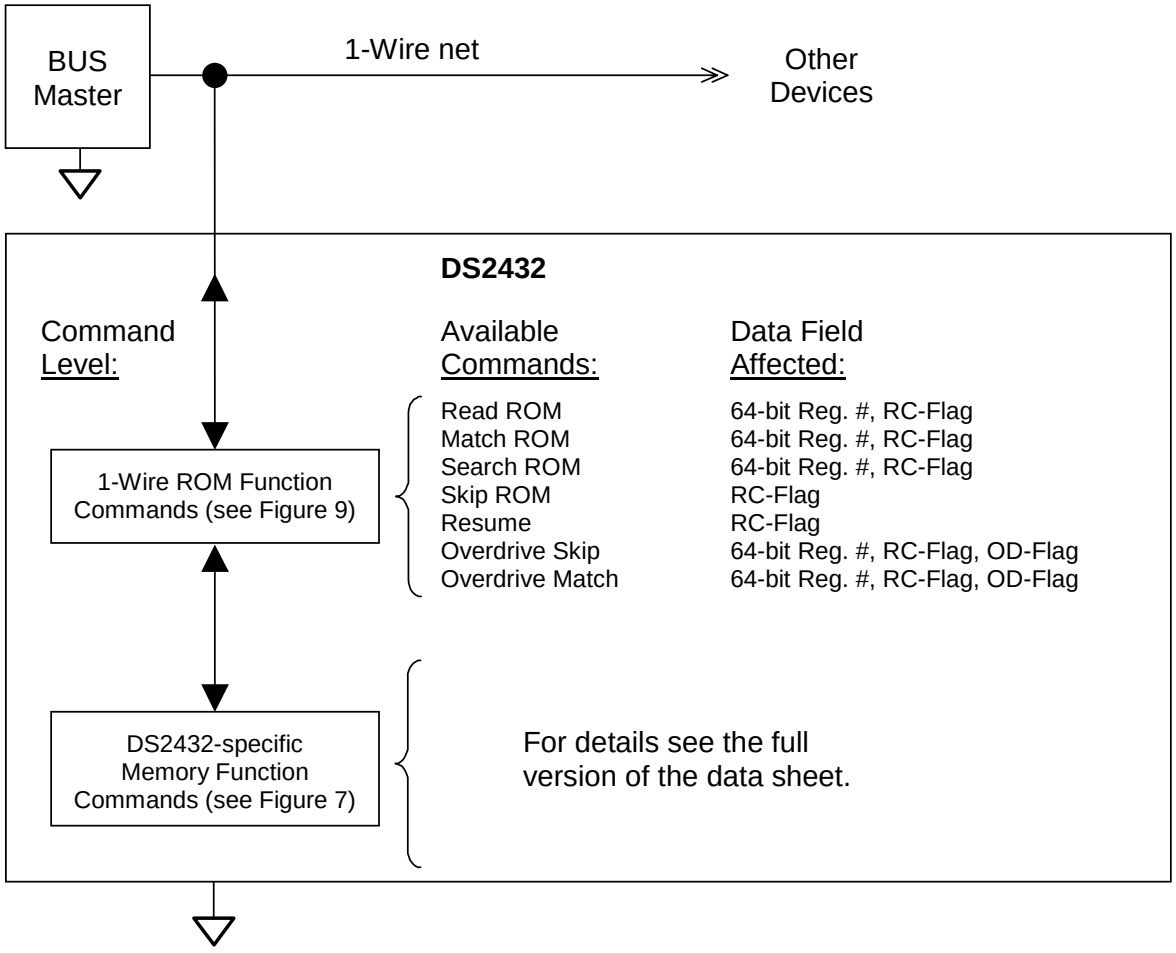


* 图 7 请参考完整的数据资料。

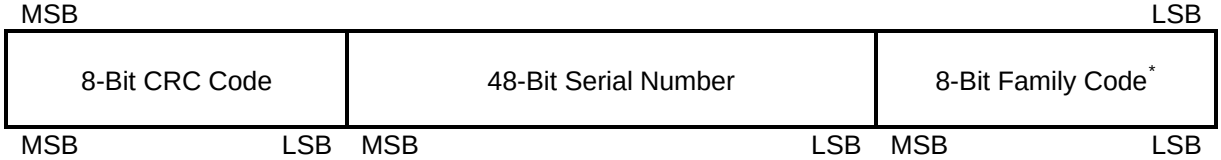
64 位光刻 ROM

每个DS2432 都有一个 64 位的唯一ROM代码。前 8 位是 1-Wire家族代码。然后是 48 位的唯一序列号。最后 8 位是前 56 位的CRC检验码（图 3）。1-Wire CRC校验码由一个包含移位寄存器和异或门的多项式发生器产生，如图 4 所示。生成多项式为$X^8 + X^5 + X^4 + 1$。关于Dallas 1-Wire CRC的更多信息参见Dallas Semiconductor的Book of DS19xx iButton Standards。移位寄存器初值为零。然后，从家族代码的LSB开始，每次移入一位。当家族代码第 8 位移入后，再移入序列号。当序列号第 48 位也移入后，留在移位寄存器中的就是CRC值。移入八位CRC校验码后，移位寄存器应该全部归零。

1-Wire 协议的层次结构 图 2

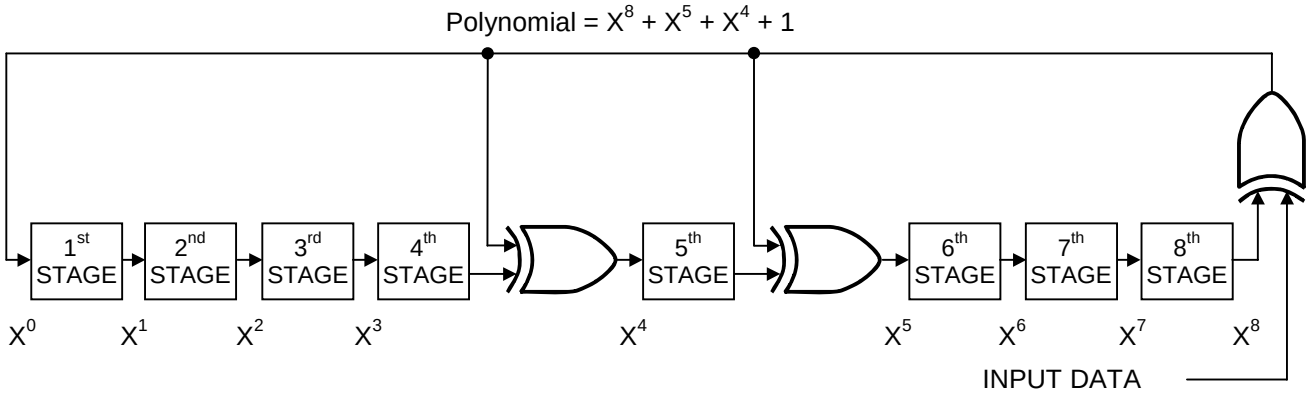


64 位光刻 ROM 图 3



*实际家族码请参考完整的数据资料。

1-Wire CRC 发生器 图 4



存储器图

DS2432 有四个存储区：数据存储器，密钥存储器，含有特定功能和用户字节的寄存器页和暂存器。数据存储器每页 32 个字节。密钥、寄存器页和暂存器均为 8 字节。向数据存储器写数据，装载初始密钥，或者向寄存器页写入数据时，暂存器作为缓存器使用。详细信息(包括图 5)请参考完整的数据资料。

地址寄存器和传输状态

DS2432 使用三个地址寄存器：TA1，TA2 和 E/S（图 6）。这些寄存器普遍用于许多其它 1-Wire 器件，但在 DS2432 中的工作略有不同。寄存器 TA1 和 TA2 装载写入数据的目的地址或读取数据的源地址。寄存器 E/S 是一个只读的传输状态寄存器，用于验证写命令的数据完整性。因为 DS2432 的暂存器只接收 8 字节的数据块，所以 TA1 的低三位总为 0，E/S 寄存器（结束偏移量）的低三位总是 1。这意味着暂存器中的所有数据随后都要复制到主存储器或密钥中。E/S 寄存器的第 5 位称为 PF 或“字节不全标志（partial byte flag）”，该位如果为逻辑 1 则意味着主机发送的数据位数不是 8 的整数倍，或者暂存器中的数据由于掉电的关系而成为无效数据。有效的写暂存器操作将清除 PF 位。第 3，4 和 6 位没有功能；读出时总为 1。利用 PF 标志，主机可以在写命令之后检验数据的完整性。E/S 寄存器的最高位称为 AA 或授权许可（Authorization Accepted），用以指示暂存器中的数据已复制到目的存储器地址。向暂存器中写入数据将清除该标志。

地址寄存器 图 6

Bit #	7	6	5	4	3	2	1	0
Target Address (TA1)	T7	T6	T5	T4	T3	T2 (0)	T1 (0)	T0 (0)
Target Address (TA2)	T15	T14	T13	T12	T11	T10	T9	T8
Ending Address with Data Status (E/S) (Read Only)	AA	1	PF	1	1	E2 (1)	E1 (1)	E0 (1)

带验证的写操作

为了向 DS2432 写入数据，需要把暂存器用作中间存储器。首先，主机发 Write Scratchpad（写暂存器）命令并指定目的地址和要写入暂存器的数据。需要注意的是，数据必须按 8 字节边界写入存储器内，目的地址的三个最低有效位（T2..T0）必须等于 000b。如果发送的 T2..T0 为非零值，器件将把这些位强制置为零，命令序列结束后写入修改后的地址。此外，执行命令时暂存器内的所有 8 个字节将拷贝到存储器，因此，应该向暂存器写入八个字节的数据，以保证所拷贝的数据是已知的。在一定条件下（参考 Write Scratchpad），Write Scratchpad 命令序列结束时，主机将接收命令、地址（实际发送地址）和数据取反后的 CRC16 校验码，该 CRC 计算时使用的地址和数据均为主机实际发送的值，而不是在非零 T2..T0 情况下的修正值。知道了 CRC 值，主机能够将接收到的 CRC 与自己计算的结果进行比较来判断通信是否成功，是否执行 Copy Scratchpad 命令。如果主机不能接收 CRC16，应该执行一次 Read Scratchpad 来验证写入数据的完整性。读暂存器时，作为暂存数据的导码，DS2432 会重新发回目的地址 TA1 和 TA2，以及 E/S 寄存器的内容。如果 PF 标志置位，则说明数据没有正确送达暂存器，或是上一次写暂存器后发生过掉电故障。主机不需要继续读操作，可以启动新一轮写暂存器操作。同样，授权许可（AA）标志置位、PF 标志清零，则说明器件未能正确识别写命令。如果每一过程都是正确的话，两个标志位将被清零。主机可以连续地读数据、验证数据字节。完成数据验证后，主机可以发 Copy Scratchpad 等命令。该命令必须跟随三个地址寄存器 TA1、TA2 和 E/S 的数据。主机应该通过读取暂存器获得这些寄存器的内容。

存储器和 SHA 命令

这一部分描述了存储器和器件 SHA-1 引擎的命令及流程图，包括表 1 至表 4 和图 7，请参考完整的数据资料。

SHA-1 算法

SHA算法的说明译自安全散列标准（Secure Hash Standard）SHA-1 文档，该文档可从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。

1-Wire 总线系统

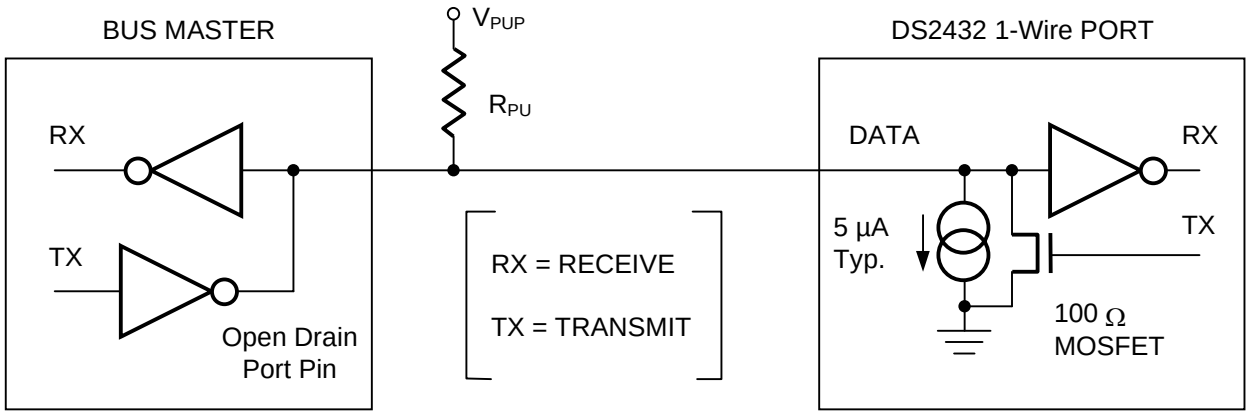
1-Wire 总线系统由一个总线主机和一个或多个从器件组成。在所有应用实例中，DS2432 都作为从器件使用，总线主机通常是一个微控制器。对 1-Wire 总线系统的讨论分为 3 个部分：硬件配置、处理流程和 1-Wire 信令(信号类型和时序)。1-Wire 协议根据特定时隙中总线的状态来工作，这些特定时隙始于总线主机发出的同步脉冲的下降沿。

硬件配置

1-Wire总线只定义了一条数据线，所以，保证在适当的时间驱动总线上的每个器件非常重要。为了达到这一目的，接在 1-Wire总线上的每个器件都必须具有漏极开路或三态输出。DS2432 的 1-Wire端口为漏极开路，其内部等效电路如图 8 所示。多点总线由连接了多个从机器件的 1-Wire总线组成。在标准速率下，1-Wire总线的最大速率为 16.3kbps。在高速模式下，速率可达 142kbps。为了在任意速率下执行存储器和SHA操作命令，DS2432 需要的 1-Wire上拉电阻最大值为 2.2kΩ。当与几个DS2432 同时通信时，例如安装同样的密钥给几个器件，在器件从暂存器向EEPROM传送数据时，应该利用一个上拉至V_{PUP}的低阻抗上拉旁路这个电阻。

1-Wire 总线的空闲状态是高电平。如因某种原因需要暂停通信，稍候要恢复通信的话，总线必须保持在空闲状态。如果不是这样，当总线处于低电平状态超过 16μs（高速模式）或 120μs（常规速率）时，总线上的一个或多个器件将被复位。

硬件配置 图 8



处理流程

通过 1-Wire 端口访问 DS2432 的协议如下：

- 初始化
- ROM 操作命令
- 存储器或 SHA 操作命令
- 交易/数据

初始化

1-Wire 总线上所有的传输操作均从初始化过程开始。初始化过程由主机发出的复位脉冲和从机发出的在线应答脉冲（presence pulse）组成。在线应答脉冲使主机检测到 DS2432 挂接在总线上，并且已经准备就绪。详细内容请参阅“1-Wire 信令”一节。

ROM 功能命令

一旦主机检测到在线应答脉冲，就可以发出 DS2432 支持的七条 ROM 功能命令。所有 ROM 操作命令的长度为八位。以下列出了这些命令的简要介绍（见图 9 中的流程图）：

Read ROM [33h]

此条命令允许主机读取 DS2432 的 8 位家族码、48 位唯一的序列号和 8 位 CRC 校验码。此命令适用于总线上只有一个从机的情况。如果总线上连接了多个从机设备，当同一时间每个从机设备都响应此条命令时，就必然要发生数据冲突（漏极开路输出将产生一个线与结果）。结果导致主机读取的家族码和 48 位序列号无效。

Match ROM [55h]

命令后面跟随 64 位注册号，允许主机访问多从机总线系统中某个特定的 DS2432。只有与 64 位注册号完全匹配的 DS2432 才会响应主机随后发出的存储器功能命令。所有其它从机将等待复位脉冲。这条命令既适用于单从机系统，也适用于多从机系统。

Search ROM [F0h]

系统初次上电时，总线主机可能并不知道 1-Wire总线上从机设备的数目和它们的 64 位注册号，而Search ROM命令能够使得总线主机通过排除法来检测出总线上所有从机设备的 64 位注册号。Search ROM过程其实只是简单的 3 步骤重复：读一位、读此位的补码，然后写这一位的期望值，主机对注册号的每一位数据都执行这简单的 3 步骤操作。在完全通过一次审查操作后，总线主机就能读出一台从机设备的 64 位内容。其余从机设备的注册号可经由另外的操作检测出来。关于Search ROM命令更全面的讨论，请参考Book of DS19xx iButton Standards第 5 章，并且在此章中还包括一个实例。

Skip ROM [CCh]

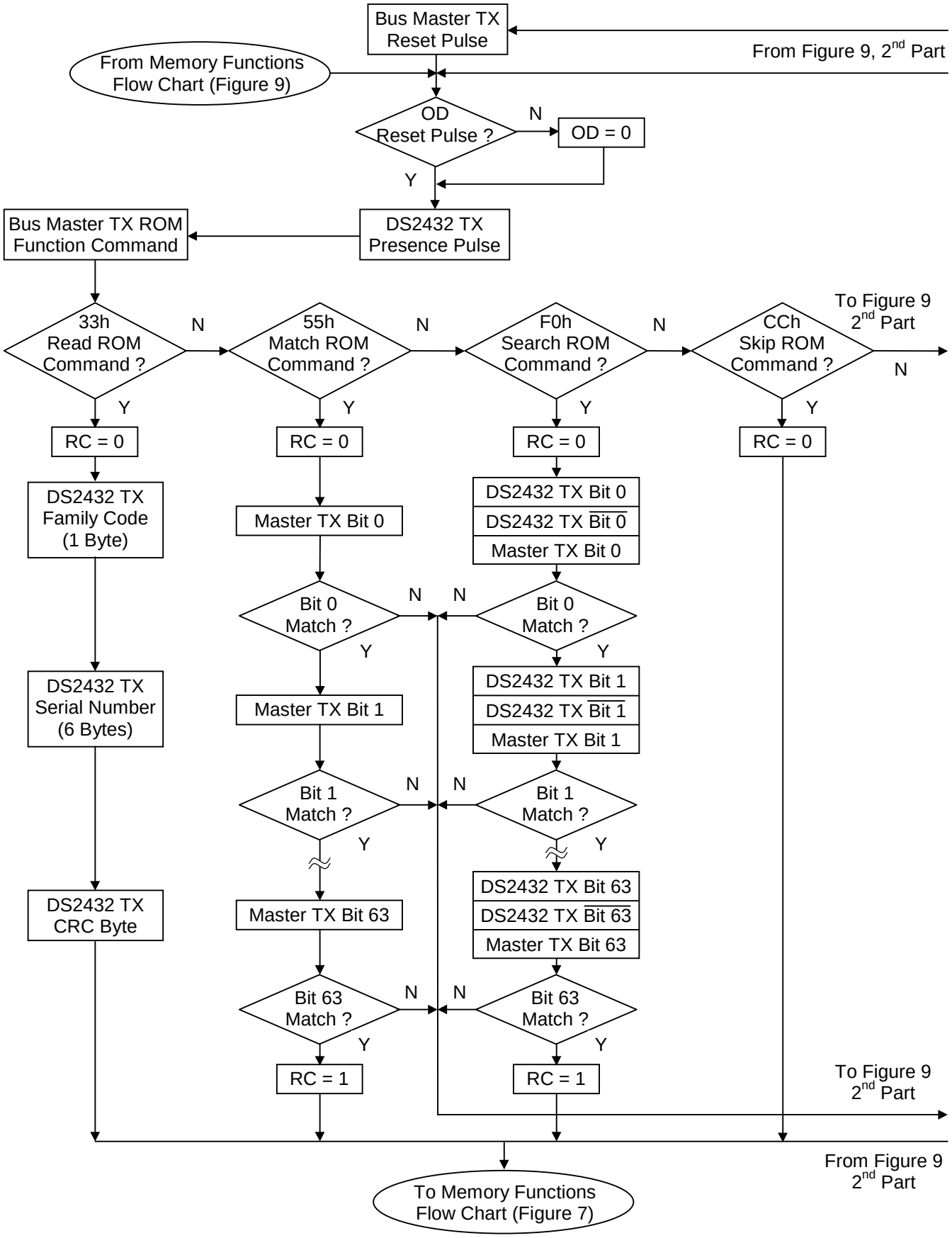
Skip ROM 命令在单从机总线系统中允许主机直接访问存储器和 SHA 功能，而无须提供 64 位注册号，节省时间。如果总线上挂接了不止一个从机设备，而且在 Skip ROM 命令后发出了一条 Read 命令，总线上的从机设备就会同时传送数据，从而引起数据冲突（漏极开路输出将产生一个线与结果）。

Overdrive Skip ROM [3Ch]

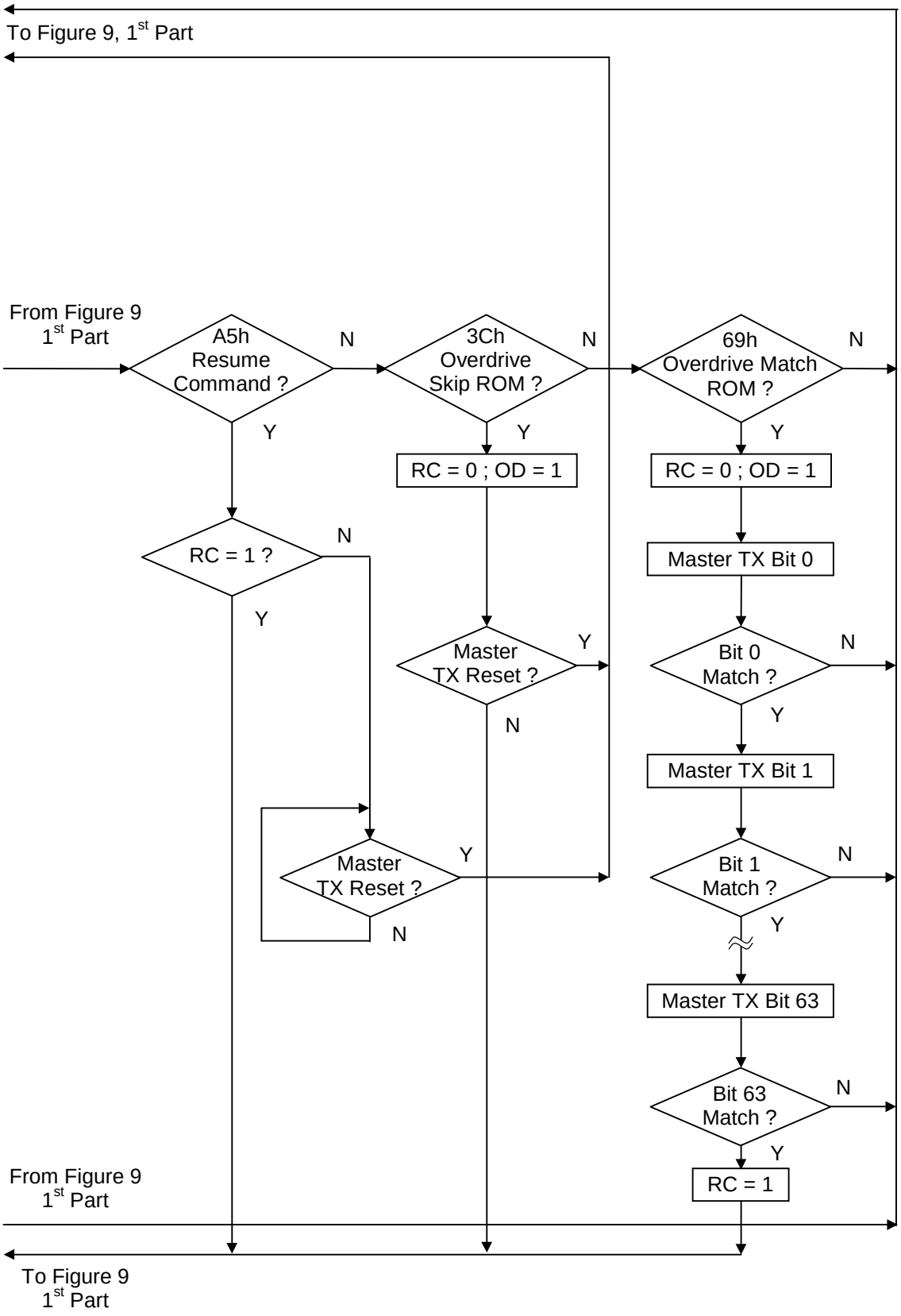
在单点总线上发出该命令的时候，总线主机不需要 64 位的注册号就可以访问存储器和 SHA 功能，从而节省了时间。不同于通常的 Skip ROM 命令， Overdrive Skip ROM 命令将 DS2432 设置成高速模式（OD = 1）。该命令代码后面的所有通信都发生在高速模式下，直到有一个最短持续 480µs 的复位脉冲把总线上的所有器件都复位到标准速率（OD = 0）。

在多点总线上发出该命令时，所有支持高速模式的器件都被置为高速模式。随后，为了寻址特定的高速模式器件，必须发出一个高速模式的复位脉冲，接着运用 Match ROM 或 Search ROM 命令。这将加速搜索过程。如果总线上有多于一个支持高速模式的从机，并且 Overdrive Skip ROM 命令后接着就是 Read 命令，那么由于多个从机同时发送，总线上就会发生数据冲突（多个开漏输出下拉将产生线“与”结果）。

ROM 功能流程图 图 9



ROM 功能流程图 图 9 (续)



Overdrive Match ROM [69h]

通过 Overdrive Match ROM 命令，后接以高速模式发送的 64 位注册号，总线主机可以在多点总线上找到某个特定的 DS2432，并将它设置成高速模式。只有 64 位注册码精确匹配的 DS2432 才会响应后续的存储器或 SHA 操作命令。那些通过前面的 Overdrive Skip 或 Overdrive Match 命令已被置为高速模式的从机将继续保持高速模式。直到有一个最短持续时间 480µs 的复位脉冲发出后，所有高速模式的器件将返回常规速率。命令 Overdrive Match ROM 适用于总线上有单个或多个器件的情况。

Resume Command [A5h]

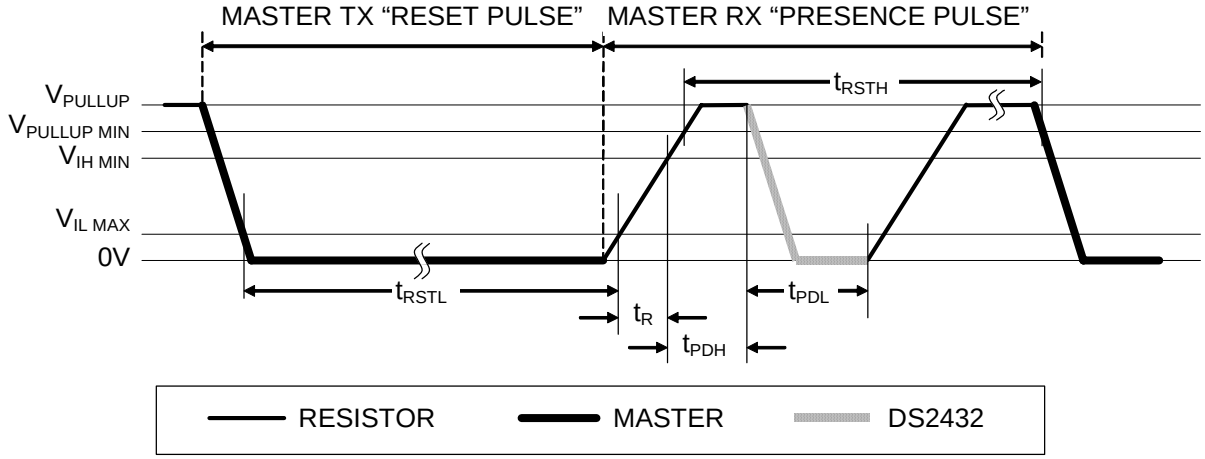
在一个典型应用中，要写满一个 32 字节的存储器页，往往需要多次访问 DS2432。这意味着在多点环境中，每次访问都要重复执行 Match ROM 命令和发送 64 位注册号。为了提高多点环境中的数据吞吐率，设置了 Resume Command 功能。该功能检测 RC 位的状态，如果置位，就直接传递控制给存储器和 SHA 功能，类似于 Skip ROM 命令。设置 RC 位的唯一方法是成功地执行 Match ROM，Search ROM 或 Overdrive Match ROM 命令。一旦设置了 RC 位，利用 Resume Command 功能就可重复访问同一器件。对于总线上另一器件的访问将清除 RC 位，以防两个或更多的器件同时响应 Resume Command 功能。

1- Wire 信令

为了保证数据的完整性，DS2432 具有一个严格的信号协议。该协议在一条线上定义了四种类型的信号：包括复位脉冲和在线应答脉冲的复位序列、写 0、写 1 和读数据。除了在线应答脉冲以外，所有其它信号均由总线主机发出。DS2432 能够以两种不同速率通信：标准速率和高速模式。如果没有明确设定为高速模式，DS2432 就以标准速率通信。高速模式下，所有波形均采用快速定时。

复位脉冲后面跟随一个在线应答脉冲表明DS2432 已经准备好发送或接收数据。总线主机发送（TX）一个复位脉冲（t_{RSTL}，标准速率下至少 480µs，高速模式下至少 48µs）。随后，主机将释放总线，进入接收模式 (RX)。这时 1-Wire总线通过上拉电阻被拉高。当DS2432 在数据引脚上检测到上升沿后，等待一段时间(t_{PDH}，标准速率下 15 至 60µs，高速模式下 2 至 6µs)，然后发送在线应答脉冲(t_{PDL}，标准速率下 60 至 240µs，高速模式下 8 至 24µs)。480µs或更长时间的复位脉冲将使器件退出高速模式，恢复到标准速率。如果DS2432 处于高速模式下，并且复位脉冲时间不高于 80µs，则器件保持高速模式。

初始化时序“复位脉冲和在线应答脉冲” 图 10

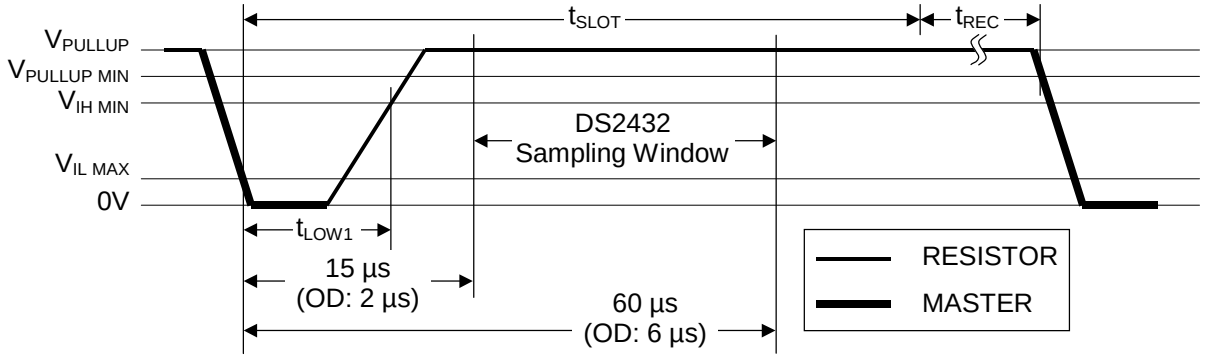


读/写时隙

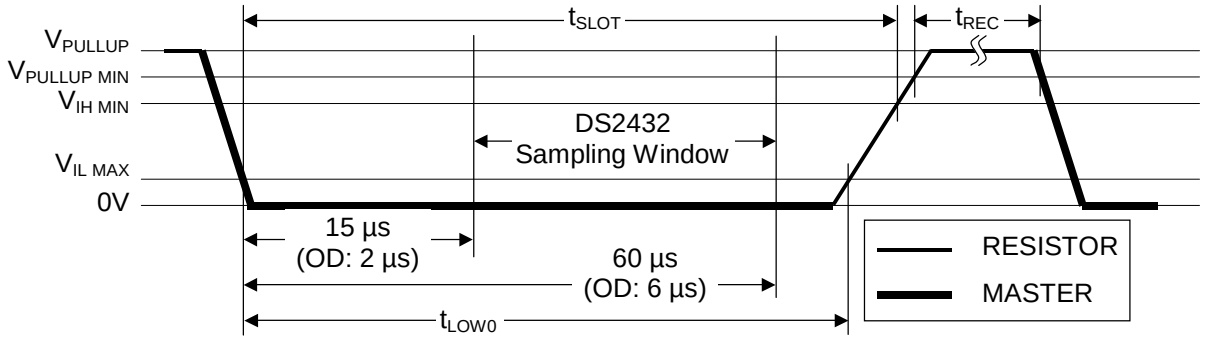
读、写时隙的定义如图 11 所示。主机通过拉低数据线来启动所有时隙。数据线的下降沿通过触发内部延迟电路使 DS2432 与主机同步。在写时隙中，延迟电路可确定什么时候 DS2432 采样数据线。对读数据时隙来说，如果发送的是“0”，那么延迟电路将决定 DS2432 数据线保持为低的时间。如果数据位是“1”，则 DS2432 无需将数据线拉低。

读/写时序图 图 11

Write-one Time Slot

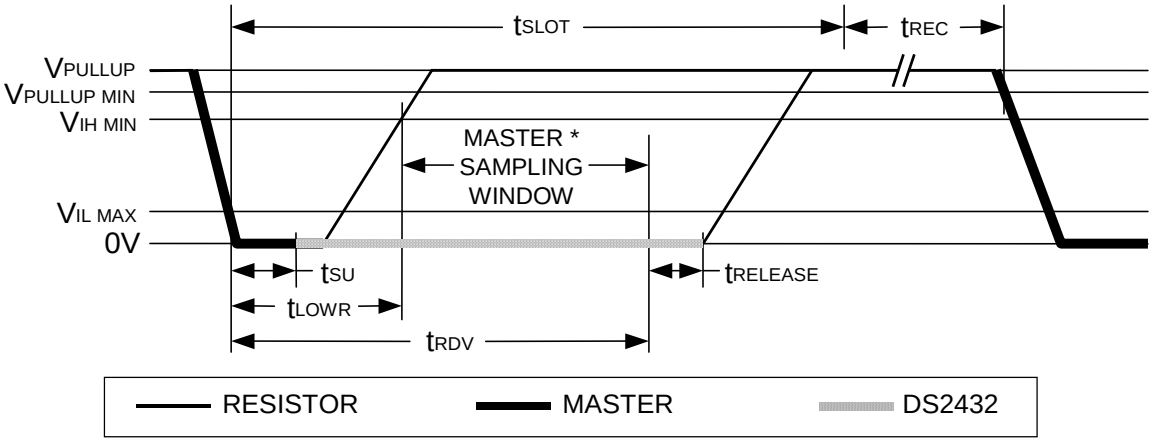


Write-zero Time Slot



读/写时序图 图 11 （续）

Read-data Time Slot



* 主机的最佳采样点应尽可能靠近t_{RDV}，不要超出t_{RDV}。执行读 1 时隙时，这样做会给上拉电阻留出足够的时间以将总线恢复为高电平。执行读 0 时隙时，这将确保在最快的 1-Wire器件释放总线前 ($t_{RELEASE}$ = 0) 执行读操作。

CRC 生成

DS2432 有两种类型的循环冗余校验（CRC）。其中一种类型是 8 位的，在出厂时就已经计算好了，并用激光写入 64 位ROM的最高字节中。该CRC的等价多项式是$X^8 + X^5 + X^4 + 1$。为了确定ROM数据是否被无差错地读取，总线主机可用 64 位ROM的前 56 位计算CRC值，并将其与从 DS2432 读来的值相比较。读ROM的时候，接收到的是 8 位CRC校验码的原码形式（未求反的）。

另一种 CRC 校验为 16 位，这种 CRC 校验用于检测执行存储器和 SHA-1 功能命令时的错误，详细信息 (包括图 12)请参考完整的数据资料。

ABSOLUTE MAXIMUM RATINGS*

Voltage on Any Pin Relative to Ground	-0.5V to +5.5V
Operating Temperature	-40°C to +85°C
Storage Temperature	-55°C to +125°C
Soldering Temperature	See J-STD-020A specification

* 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.

DC ELECTRICAL CHARACTERISTICS (V_{PUP} =2.8V to 5.25V; -40°C to +85°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
1-Wire Input High	V_{IH}	2.2			V	1, 7
1-Wire Input Low	V_{IL}	-0.3		TBD	V	1, 8
1-Wire Output Low @ 4 mA	V_{OL}			0.4	V	1
1-Wire Output High	V_{OH}		V_{PUP}		V	1, 2
Input Load Current	I_L		5		µA	3
Programming Current	I_{LPROG}		500		µA	9
SHA-1 Computation Current	I_{CSHA}	See full version of data sheet.				

CAPACITANCE (t_A = 25°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
1-Wire I/O	$C_{IN/OUT}$		100	800	pF	5

ENDURANCE (V_{PUP} =5.0V; T_A = 25°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Write/Erase Cycles	N_{CYCLE}	50k			—	
Data Retention	t_{DRET}	10			years	

AC ELECTRICAL CHARACTERISTICS REGULAR SPEED (V_{PUP}=2.8V to 5.25V; -40°C to +85°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Time Slot	t_{SLOT}	60		120	µs	
Write 1 Low Time	t_{LOW1}	1		15	µs	
Write 0 Low Time	t_{LOW0}	60		120	µs	
Read Low Time	t_{LOWR}	1		15	µs	
Read Data Valid	t_{RDV}		15		µs	10
Release Time	$t_{RELEASE}$	0	15	45	µs	
Read Data Setup	t_{SU}			1	µs	4
Recovery Time	t_{REC}	1			µs	
Reset High Time	t_{RSTH}	480			µs	
Reset Low Time	t_{RSTL}	480			µs	6
Presence Detect High	t_{PDHIGH}	15		60	µs	
Presence Detect Low	t_{PDLOW}	60		240	µs	
Programming Time	t_{PROG}			10	ms	
SHA Computation Time	t_{CSHA}	See full version of data sheet.				

AC ELECTRICAL CHARACTERISTICS
OVERDRIVE SPEED

(V_{PUP}=2.8V to 5.25V; -40°C to +85°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Time Slot	t_{SLOT}	6		16	µs	
Write 1 Low Time	t_{LOW1}	1		2	µs	
Write 0 Low Time	t_{LOW0}	6		16	µs	
Read Low Time	t_{LOWR}	1		2	µs	
Read Data Valid	t_{RDV}		2		µs	10
Release Time	$t_{RELEASE}$	0	1.5	4	µs	
Read Data Setup	t_{SU}			1	µs	4
Recovery Time	t_{REC}	1			µs	
Reset High Time	t_{RSTH}	48			µs	
Reset Low Time	t_{RSTL}	48		80	µs	
Presence Detect High	t_{PDHIGH}	2		6	µs	
Presence Detect Low	t_{PDLOW}	8		24	µs	
Programming Time	t_{PROG}			10	ms	
SHA Computation Time	t_{CSHA}	See full version of data sheet.				

NOTES:

1. All voltages are referenced to ground.
2. V_{PUP} = external pull-up voltage.
3. Input load is to ground.
4. Read data setup time refers to the time the host must pull the 1-Wire bus low to read a bit. Data is guaranteed to be valid within 1 µs of this falling edge.
5. Capacitance on the data pin could be 800 pF when power is first applied. If a 5 kΩ resistor is used to pull up the data line to V_{PUP}, 5 µs after power has been applied the parasite capacitance will not affect normal communications.
6. The reset low time (t_{RSTL}) should be restricted to a maximum of 960 µs, to allow interrupt signaling, otherwise, it could mask or conceal interrupt pulses.
7. V_{IH} is a function of the external pull-up resistor and V_{PUP}.
8. Under certain low voltage conditions V_{ILMAX} may have to be reduced to as much as 0.5V to always guarantee a Presence Pulse. V_{IL} is a function of V_{PUP} and the reset low time.
9. During write operations to the EEPROM the voltage on the 1-Wire bus must not fall below 2.8V. The EEPROM write cycle takes max. 10 ms.
10. The optimal sampling point for the master is as close as possible to the end time of the t_{RDV} period without exceeding t_{RDV}. For the case of a Read-one time slot, this maximizes the amount of time for the pull-up resistor to recover the line to a high level. For a Read-zero time slot it ensures that a read will occur before the fastest 1-Wire device releases the line ($t_{RELEASE}$ = 0).