

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

概要

DS28CN01は、1024ビットのEEPROMとFederal Information Publications (FIPS) 180-1/180-2およびISO/IEC 10118-3セキュアハッシュアルゴリズム (SHA-1)で実装されたチャレンジ&レスポンスの認証セキュリティと組み合わせたものです。このメモリは各32バイトの4ページとして構成されています。各メモリページに対して、データコピー防止機能とEPROMエミュレーション機能がサポートされています。各DS28CN01は、出荷時に設定され保証された固有の64ビットの登録番号を備えています。DS28CN01との通信は、業界標準のI²CおよびSMBus™対応のインターフェースを通じて実行されます。SMBusタイムアウト機能によって、バスタイムアウトのフォルト状態が検出されるとデバイスのインターフェースがリセットされます。

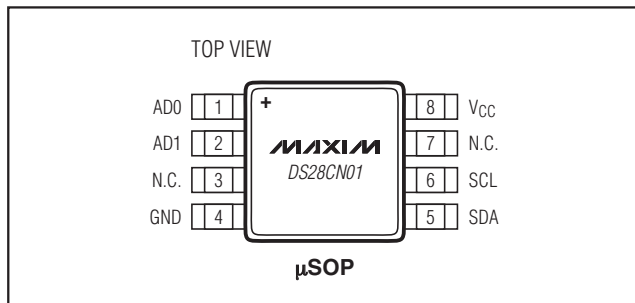
アプリケーション

PCBの固有連番
アクセサリおよびペリフェラルの識別
機器登録およびライセンス管理
ネットワークノード識別
プリンタカートリッジの設定および監視
医療用センサの認証および較正
システムの知的所有権保護

特長

- ◆ 各256ビットの4ページで区分された1024ビットのEEPROMメモリ
- ◆ SHA-1 MACを生成する専用ハードウェア高速化SHA-1エンジン
- ◆ EEPROMメモリページは個別にコピー防止またはEPROMモード(1から0への設定のみ)への移行が可能
- ◆ 書き込みアクセスには、シークレットの知識、および認証として160ビットMACの計算および伝送の能力が必要
- ◆ 出荷時に設定され試験済みの固有の64ビット登録番号によって同一製品がないため、絶対追跡が可能
- ◆ 耐久性：20万サイクル(+25°Cにおいて)
- ◆ I²CバスおよびSMBus対応にするユーザプログラマブルなシリアルインターフェース
- ◆ 100kHzと400kHzのI²C通信速度をサポート
- ◆ +5.5V耐圧のインターフェース端子
- ◆ 動作範囲：+1.62V~+5.5V、-40°C~+85°C
- ◆ 8ピンμSOPパッケージ

ピン配置



型番

PART	TEMP RANGE	PIN-PACKAGE
DS28CN01U-A00+	-40°C to +85°C	8 μSOP
DS28CN01U-A00+T	-40°C to +85°C	8 μSOP

+は鉛(Pb)フリー/RoHS準拠パッケージを表します。
T = テープ&リール

標準動作回路はデータシートの最後に記載されています。

SMBusはIntel Corp.の商標です。

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28CN01

ABSOLUTE MAXIMUM RATINGS

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

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.

ELECTRICAL CHARACTERISTICS

(T_A = -40°C to +85°C.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V _{CC}		1.62		5.50	V
Standby Current	I _{CCS}	Bus idle, V _{CC} = +5.5V			5.5	μA
Operating Current	I _{CCA}	Bus active at 400kHz, V _{CC} = +5.5V			500	μA
Power-Up Wait Time	t _{POIP}	(Note 2)			5	μs
EEPROM						
Programming Time	t _{PROG}	V _{CC} ≥ 2.0V			10	ms
		V _{CC} < 2.0V			45	
Programming Current	I _{PROG}	V _{CC} = +5.5V			1.2	mA
Endurance (Notes 3, 4, 5)	N _{CY}	At +25°C	200,000			—
		At +85°C	50,000			
Data Retention (Notes 6, 7, 8)	t _{DR}	At +85°C	40			Years
SHA-1 ENGINE						
SHA-1 Computation Time	t _{CSHA}	See full version of the data sheet.				ms
SHA-1 Computation Current	I _{LCSHA}	See full version of the data sheet.				mA
SCL, SDA, AD1, AD0 PINS (Notes 9, 10)						
Low-Level Input Voltage	V _{IL}	V _{CC} ≥ 2.0V	-0.3		0.3 × V _{CC}	V
		V _{CC} < 2.0V	-0.3		0.25 × V _{CC}	
High-Level Input Voltage	V _{IH}	V _{CC} ≥ 2.0V	0.7 × V _{CC}		V _{CCMAX} + 0.3V	V
		V _{CC} < 2.0V	0.8 × V _{CC}		V _{CCMAX} + 0.3V	
Hysteresis of Schmitt Trigger Inputs (Note 2)	V _{HYS}	V _{CC} ≥ 2.0V	0.05 × V _{CC}			V
		V _{CC} < 2.0V	0.1 × V _{CC}			
Low-Level Output Voltage at 4mA Sink Current, Open Drain	V _{OL}	V _{CC} ≥ 2.0V			0.4	V
		V _{CC} < 2.0V			0.2 × V _{CC}	

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Output Fall Time from V _{IH(MIN)} to V _{IL(MAX)} with a Bus Capacitance from 10pF to 400pF (Notes 2, 11)	t _{OF}	V _{CC} ≥ 2.0V	20 + 0.1C _B		250	ns
		V _{CC} < 2.0V	20 + 0.1C _B		300	
Pulse Width of Spikes that are Suppressed by the Input Filter	t _{SP}	(Note 2)			50	ns
Input Current with an Input Voltage Between 0.1V _{CC} and 0.9V _{CCMAX}	I _I	(Note 12)	-10		+10	μA
Input Capacitance	C _I	(Note 2)			10	pF
SCL Clock Frequency	f _{SCL}	(Note 13)			400	kHz
Bus Timeout	t _{TIMEOUT}	CM bit = 1 (Note 13)	25		75	ms
Hold-Time (Repeated) START Condition; After this Period, the First Clock Pulse is Generated	t _{HD:STA}	(Note 14)	0.6			μs
Low Period of the SCL Clock (Note 14)	t _{LOW}	V _{CC} ≥ 2.7V	1.3			μs
		V _{CC} ≥ 2.0V	1.5			
		V _{CC} < 2.0V	1.9			
High Period of the SCL Clock	t _{HIGH}	(Note 14)	0.6			μs
Setup Time for a Repeated START Condition	t _{SU:STA}	(Note 14)	0.6			μs
Data Hold Time (Notes 15, 16)	t _{HD:DAT}	V _{CC} ≥ 2.7V	0.3		0.9	μs
		V _{CC} ≥ 2.0V	0.3		1.1	
		V _{CC} < 2.0V	0.3		1.5	
Data Setup Time	t _{SU:DAT}	(Notes 2, 14, 17)	100			ns
Setup Time for STOP Condition	t _{SU:STO}	(Note 14)	0.6			μs
Bus Free Time Between a STOP and START Condition	t _{BUF}	(Note 14)	1.3			μs
Capacitive Load for Each Bus Line	C _B	(Notes 2, 14)			400	pF

Note 1: Specifications at -40°C are guaranteed by design and characterization only and not production tested.

Note 2: Guaranteed by design, characterization, and/or simulation only and not production tested.

Note 3: This specification is valid for each 8-byte memory row.

Note 4: Write-cycle endurance is degraded as T_A increases.

Note 5: Not 100% production tested; guaranteed by reliability monitor sampling.

Note 6: Data retention is degraded as T_A increases.

Note 7: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to data sheet limit at operating temperature range is established by reliability testing.

Note 8: EEPROM writes can become nonfunctional after the data retention time is exceeded. Long-time 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 9: All values are referred to V_{IH(MIN)} and V_{IL(MAX)} levels.

Note 10: See Figure 3.

Note 11: C_B = Total capacitance of one bus line in pF. If mixed with high-speed-mode devices, faster fall times according to I²C Bus Specification v2.1 are allowed.

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28CN01

ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C.) (Note 1)**Note 12:** The DS28CN01 does not obstruct the SDA and SCL lines if V_{CC} is switched off.**Note 13:** The minimum SCL clock frequency is limited by the bus timeout feature. If the CM bit is 1 and SCL stays at the same logic level or SDA stays low for this interval, the DS28CN01 behaves as though it has sensed a STOP condition.**Note 14:** System requirement.**Note 15:** The DS28CN01 provides a hold time of at least 300ns for the SDA signal (referred to the V_{IH(MIN)} of the SCL signal) to bridge the undefined region of the falling edge of SCL.**Note 16:** The master can provide a hold time of 0ns minimum when writing to the device. This 0ns minimum is guaranteed by design, characterization, and/or simulation only, and not production tested.**Note 17:** A fast-mode I²C bus device can be used in a standard-mode I²C bus system, but the requirement t_{SU:DAT} ≥ 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 t_{RMAX} + t_{SU:DAT} = 1000 + 250 = 1250ns (according to the standard-mode I²C bus specification) before the SCL line is released.

端子説明

端子	名称	機能
1	AD0	スレーブアドレスを選択するデバイスアドレス入力端子。スレーブアドレスビットA[1:0]を設定します。GND、SDA、SCL、またはV _{CC} のいずれかに接続する必要があります。
2	AD1	スレーブアドレスを選択するデバイスアドレス入力端子。スレーブアドレスビットA[3:2]を設定します。GND、SDA、SCL、またはV _{CC} のいずれかに接続する必要があります。
3, 7	N.C.	接続なし
4	GND	電源グランド
5	SDA	I ² C/SMBus双方向シリアルデータライン。プルアップ抵抗を介してV _{CC} に接続する必要があります。
6	SCL	I ² C/SMBusシリアルクロック入力。プルアップ抵抗を介してV _{CC} に接続する必要があります。
8	V _{CC}	電源入力

詳細

DS28CN01は、「ブロック図」に示すように、シリアルI²C/SMBusインタフェース、1KbのSHA-1セキュアEEPROM、レジスタページ、および固有の登録番号を備えています。このデバイスは、I²Cインタフェースを通じて、標準モードまたはファーストモードでホストプロセッサと通信します。ユーザはインタフェースをI²CバスモードからSMBusモードに切り替えることができます。2つの4レベルアドレス端子によって、16個のDS28CN01を同じバスセグメント上に置くことができます。

デバイスの動作

DS28CN01の読み取りと書き込みは、I²C/SMBusシリアルインタフェースを通じて制御されます。DS28CN01はさまざまな特性のメモリ領域とレジスタを備えているため、検討を要する特別なケースがいくつかあります。詳しくは、フルデータシートの「読み取りと書き込み」の項を参照してください。

シリアル通信インタフェース

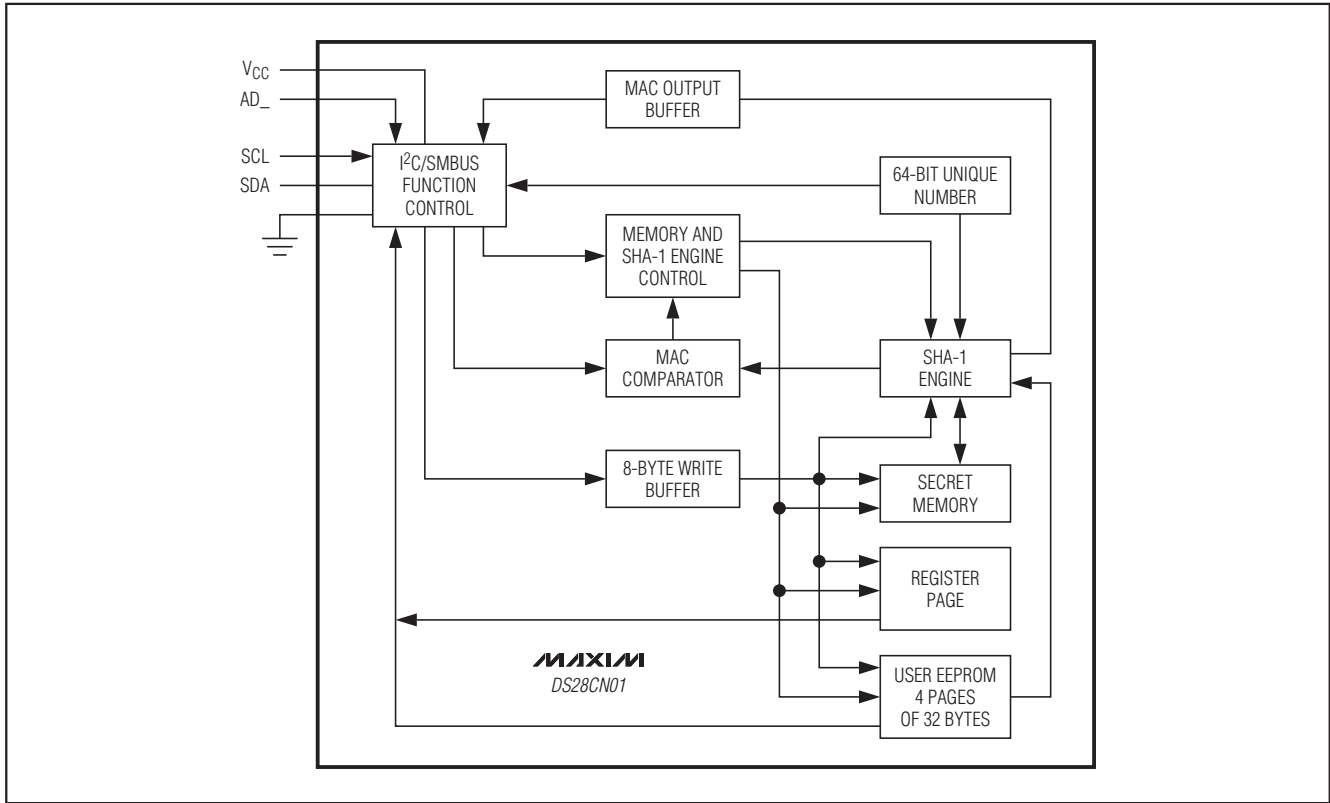
シリアルインタフェースでは、通信にデータライン(SDA)とクロック信号(SCL)が使われます。SDAとSCLはいずれも双方向ラインで、プルアップ抵抗を介して正電源電圧に接続されます。通信が行われないうち両ラインはハイになります。バスに接続されたデバイスの出力段は、ワイヤードAND機能を実行するオープンドレインまたはオープンコレクタ出力を備えている必要があります。データは、標準モードでは最高100kbps、ファーストモードでは最高400kbpsのレートで転送されます。DS28CN01はこの両モードで動作します。

バス上でデータを送信するデバイスはトランスミッタ、データを受信するデバイスはレシーバと定義されます。通信を制御するデバイスはマスタと呼ばれます。マスタによって制御されるデバイスはスレーブです。DS28CN01はスレーブデバイスです。

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28CNO1

ブロック図



スレーブアドレス/方向バイト

個別にアクセスするために、各デバイスはバス上の他のデバイスと競合しないスレーブアドレスを備えている必要があります。DS28CNO1が応答するスレーブアドレスを図1に示します。スレーブアドレスはスレーブアドレス/方向バイトの一部です。DS28CNO1のスレーブアドレスの上位3ビットは、101bに設定されています。AD0端子はアドレスA0とA1を制御し、AD1はA2とA3を制御します。AD0とAD1はGND、V_{CC}、SCL、またはSDA

に接続することができます。表1は、これら4つのピン状態のバイナリアドレスへの変換を示します。デバイスを選択するためには、各端子のバイナリアドレスに一致するA0～A3でアドレス指定する必要があります。

スレーブアドレス/方向バイトの最終ビット(R/W)は、データの方向を決定します。このビットを0に設定すると後続データがマスタからスレーブに流れ(書込みアクセスモード)、1に設定するとデータはスレーブからマスタに流れます(読取りアクセスモード)。

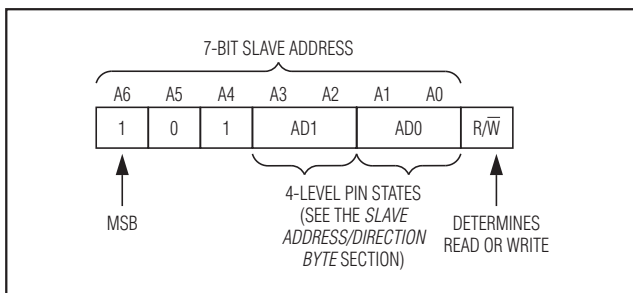


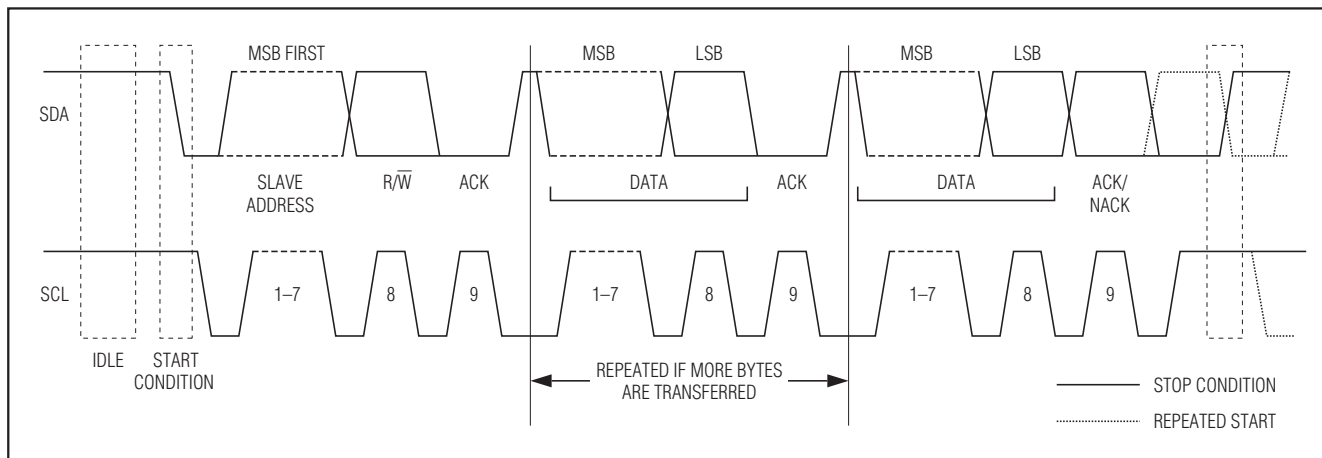
図1. スレーブアドレス

表1. 端子状態からバイナリ値への変換

AD1	A3	A2	AD0	A1	A0
GND	0	0	GND	0	0
V _{CC}	0	1	V _{CC}	0	1
SCL	1	0	SCL	1	0
SDA	1	1	SDA	1	1

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28C01

図2. I²C/SMBusプロトコルの概要I²C/SMBusプロトコル

データ転送は、バスがビジーでないときにのみ開始することができます。マスタは、SCLの生成、バスアクセスの制御、START条件およびSTOP条件の生成、およびSTARTとSTOPの間にSDAライン上に転送されるバイト数の決定を行います。データは、最上位ビットを先頭にバイト単位で転送されます。各バイトの後に、マスタとスレーブの間の同期を可能にする確認応答ビットが続きます。データ転送の間、クロックラインがハイのときはSDAが不変に保たれる必要があります。SCLがハイの間にSDAラインが変化すると、この変化はSTARTまたはSTOPと解釈されます。プロトコルを図2に示します。詳細なタイミングリファレンスについては、図3を参照してください。

バスアイドルまたは非ビジー

SDAとSCLはともに非アクティブ、すなわちロジックハイ状態にあります。

START条件

スレーブとの通信を開始するために、マスタはSTART条件を生成する必要があります。START条件は、SCLがハイに保たれている間にSDAがハイからローになる状態変化と定義されます。

STOP条件

スレーブとの通信を終了するために、マスタはSTOP条件を生成する必要があります。STOP条件は、SCLがハイに保たれている間にSDAがローからハイになる状態変化と定義されます。

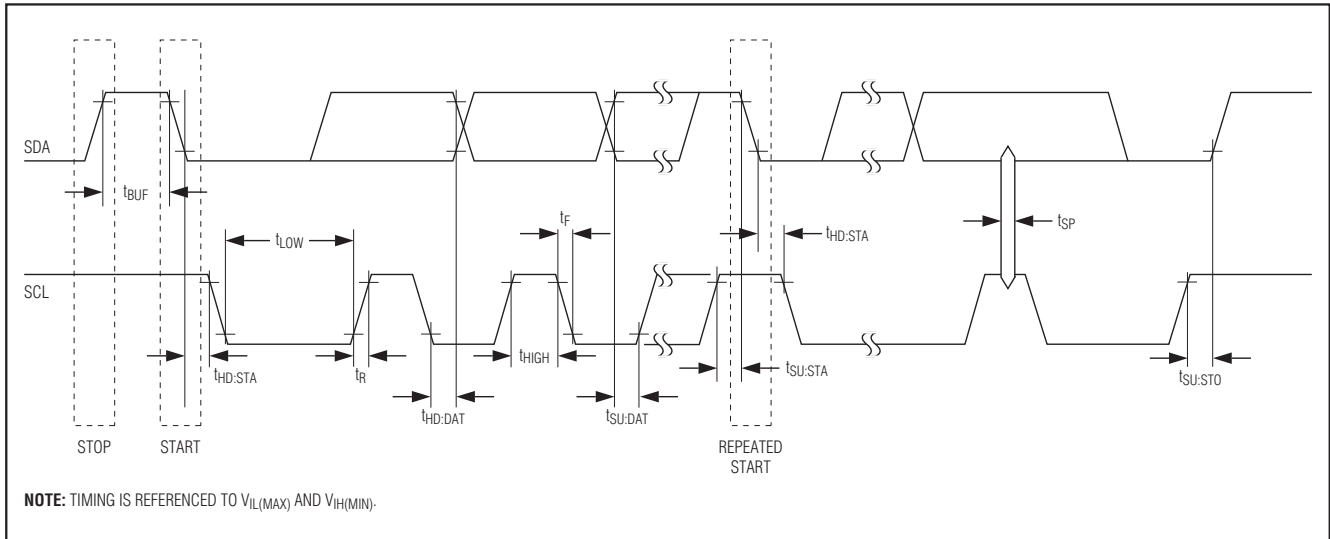
反復START条件

反復STARTは、一般に直前の書込みアクセスで読み取るメモリアドレスを指定した後の読取りアクセスに利用されます。マスタは、データ転送の最後に反復START条件を使用して、現在のデータ転送に続いて新たなデータ転送を直ちに開始することができます。反復START条件は、通常のSTART条件と同様に生成されますが、直前のSTOP条件がありません。

データ有効

STARTおよびSTOP条件を除くと、SDAの遷移はSCLがロー状態の間のみ発生します。SDAのデータは、SCLのハイパルスの全期間と必要なセットアップおよびホールド時間(SCLの立下りエッジ後の $t_{HD:DAT}$ とSCLの立上りエッジ前の $t_{SU:DAT}$ 、図3参照)にわたって、有効かつ不変の状態を保つ必要があります。データの1ビットにつき1クロックパルスが生成されます。データは、SCLパルスの立上りエッジの間に受信デバイスにシフトインされます。

書込みを終了すると、マスタは読取りを開始するためにSCLの次の立上りエッジ前に十分なセットアップ時間(図3の最小 $t_{SU:DAT} + t_R$)にわたってSDAラインを解放する必要があります。スレーブは直前のSCLパルスの立下りエッジでSDAの各データビットをシフトアウトし、データビットは現在のSCLパルスの立上りエッジで有効になります。マスタは、スレーブからの読取りに必要なクロックパルスを含む、すべてのSCLクロックパルスを生成します。

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM図3. I²C/SMBusのタイミング図

スレーブによる確認応答

通常、アドレスを指定されたスレーブデバイスは、各バイトの受信後に確認応答を生成しなければなりません。マスタは各確認応答ビットに対してクロックパルスを生成する必要があります。確認応答するスレーブは、SDAラインが確認応答クロックパルスのハイ期間中安定したローに保たれるよう、このクロックパルスの中にSDAラインをプルダウンする必要があります。セットアップ時間とホールド時間の $t_{SU:DAT}$ と $t_{HD:DAT}$ が考慮されなければなりません。

マスタによる確認応答

スレーブからの読取りを続けるために、マスタは各バイトの受信後に確認応答を生成しなければなりません。マスタは各確認応答ビットに対してクロックパルスを生成する必要があります。確認応答するマスタは、SDAラインが確認応答クロックパルスのハイ期間中に安定したローに保たれるよう、このクロックパルスの中にSDAラインをプルダウンする必要があります。セットアップ時間とホールド時間の $t_{SU:DAT}$ と $t_{HD:DAT}$ が考慮されなければなりません。

スレーブによる非確認応答

スレーブデバイスは、アクセスモードが無効である、SHA-1エンジンが動作している、またはEEPROMの書

込みサイクルが進行中である、などの理由のいずれかによってデータを送受信することができない場合があります。この場合、DS28CN01は確認に関係したクロックパルスのハイの期間中にSDAをハイのままにして拒否するバイトを確認応答しません。DS28CN01が確認応答しない状況の詳細リストについては、フルデータシートの「読取りと書込み」の項を参照してください。

マスタによる非確認応答

データを受信しているある時期に、マスタは読取りを終了する必要があります。これを実行する際、マスタは確認応答に関係したクロックパルスのハイの期間中にSDAをハイのままにして、スレーブから受信した最終バイトを確認応答しません。これに応じてスレーブは送信を中止するため、マスタはSTOP条件を生成することができます。

データメモリとレジスタ

図4と5および表2を含むこの項については、完全版のデータシートを参照してください。

読取りと書込み

この項ではEEPROMおよび各種レジスタの読取りと書込み動作を説明します。表3~13を含む詳細については、フルデータシートを参照してください。

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28CN01

SHA-1の計算アルゴリズム

SHA-1計算についてのここでの説明は、NISTのウェブサイトからダウンロードすることが可能なセキュアハッシュ規格SHA-1ドキュメントを改作したものです。詳細については、完全版のデータシートを参照してください。

アプリケーション情報

SDAおよびSCLのプルアップ抵抗

SDAは、ハイロジックレベルを実現するためにプルアップ抵抗を必要とするDS28CN01のオープンドレイン出力です（「標準動作回路」を参照）。DS28CN01ではSCLを入力としてのみ使用するため（クロック伸縮なし）、マスタはプルアップ抵抗付きのオープンドレイン/コレクタ出力またはプッシュプル出力のいずれかによってSCLを駆動することができます。

プルアップ抵抗R_pの大きさ

I²Cの仕様によると、スレーブデバイスは+0.4VのV_{OL}で少なくとも3mAをシンク可能である必要があります。SMBusの仕様では、+0.4Vで4mAの電流シンク能力を必要とします。DS28CN01は、全動作電圧範囲にわたって+0.4VのV_{OL}で少なくとも4mAをシンクすることができます。

このDC特性によってプルアップ抵抗の最小値が決まります。すなわち、R_{pMIN} = (V_{CC} - 0.4V)/4mAです。+5.5Vの最大動作電圧の場合、プルアップ抵抗の最小値は1.275kΩです。図6の「Minimum R_p」ラインは、最小プルアップ抵抗が動作（プルアップ）電圧によってどのように変化するかを示しています。

I²Cシステムでは、立上り時間と立下り時間はプルアップ電圧の30%~70%の範囲で測定されます。最大バス容量C_Bは400pFです。最大立上り時間は、300nsを超えない必要があります。最大立上り時間を仮定すると、所定の容量C_Bにおける最大抵抗値は、R_{pMAX} = 300ns / (C_B × ln(7/3))として求められます。400pFのバス容量では、最大プルアップ抵抗は885Ωとなります。

立上り時間仕様と400pFのバス容量を満たすために必要な885Ωのプルアップ抵抗は、+5.5VにおけるR_{pMIN}よりも小さいため、異なるアプローチが必要です。図6の「Maximum Load」ラインは、所定の動作電圧における最小プルアップ抵抗（「Minimum R_p」ライン）を計算した後、300nsの立上り時間を生じるそれぞれのバス容量を計算することによって生成されます。

プルアップ電圧が+4V以下の場合にのみ、400pFの最大許容バス容量を維持することができます。300pFに減少させたバス容量は、動作電圧の全範囲で許容されます。この電圧での対応するプルアップ抵抗の値を「Minimum R_p」ラインで示しています。

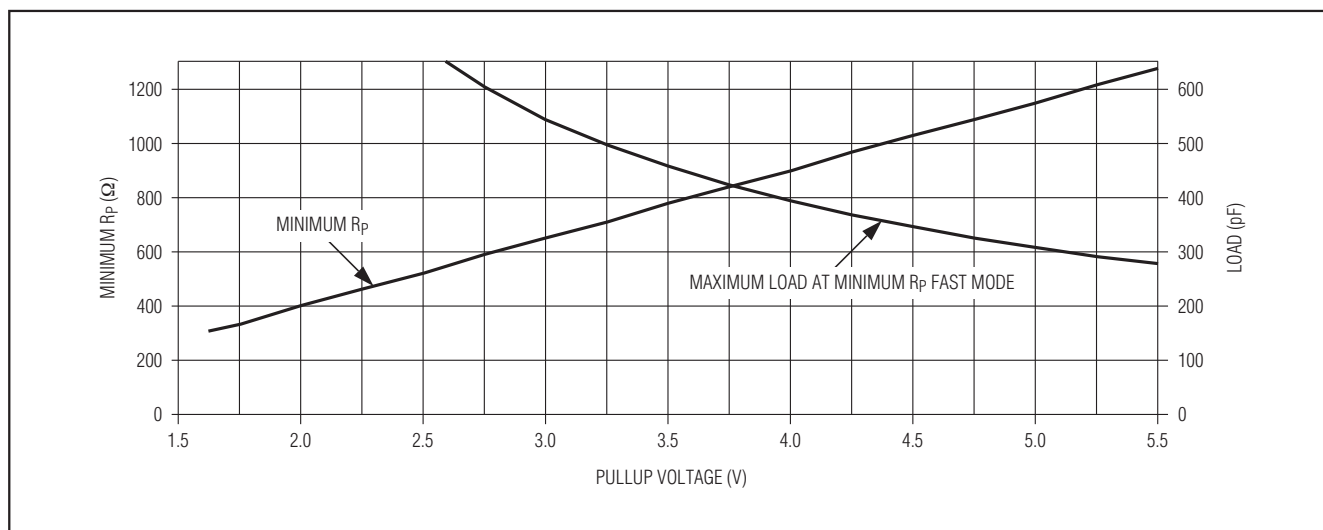
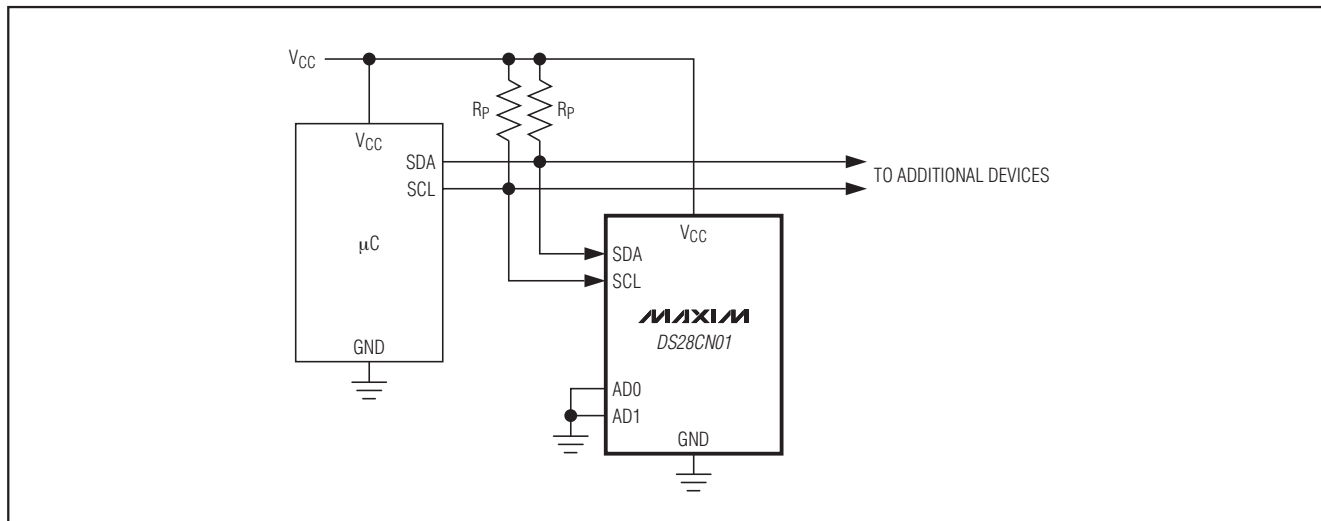


図6. I²Cファーストモードプルアップ抵抗の選択チャート

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

標準動作回路



パッケージ

最新のパッケージ図面情報およびランドパターンは、japan.maxim-ic.com/packagesを参照してください。なお、パッケージコードに含まれる「+」、「#」、または「-」はRoHS対応状況を表したものでしかありません。パッケージ図面はパッケージそのものに関するものでRoHS対応状況とは関係がなく、図面によってパッケージコードが異なることがある点に注意してください。

パッケージタイプ	パッケージコード	ドキュメントNo.
8 μ SOP	U8+3	21-0036

要約版

SHA-1エンジン付き、1Kb I²C/SMBus EEPROM

DS28CN01

改訂履歴

版数	改訂日	説明	改訂ページ
0	6/07	初版	—
1	4/09	最新のテンプレート式データシートを作成	すべて
2	11/09	「Electrical Characteristics (電気的特性)」の中のBus Timeoutの仕様に「CM bit = 1」という条件を追加	3

マキシム・ジャパン株式会社

〒169-0051東京都新宿区西早稲田3-30-16 (ホリゾン1ビル)
TEL. (03)3232-6141 FAX. (03)3232-6149

Maximは完全にMaxim製品に組込まれた回路以外の回路の使用について一切責任を負いかねます。回路特許ライセンスは明言されていません。Maximは随時予告なく回路及び仕様を変更する権利を留保します。

10 **Maxim Integrated Products, 120 San Gabriel Drive, Sunnyvale, CA 94086 408-737-7600**