DS2460

EEPROM 内蔵、SHA-1 コプロセッサ

japan.maxim-ic.com

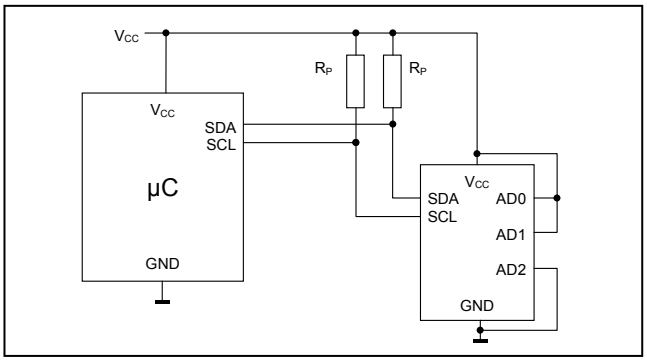
概要

EEPROM 内蔵 SHA-1 コプロセッサの DS2460 は、ISO/IEC 10118-3 セキュアハッシュアルゴリズム(SHA-1)をハードウェアによって実現したもので、SHA デバイスの認証およびディジタル署名サービスデータの検証に必要とする煩雑な SHA 計算を実行するソフトウェアの開発を不要とします。DS2460 は、一般的な I^2C インタフェースを通じてマイクロコントローラと通信します。アプリケーションには、トークン認証およびサービスデータ検証、ならびに SHA-1 結果のバイト長が 20 バイトを超えないメッセージに対するショートメッセージの暗号化と解読のために一時的に使用する暗号化キーの生成を行など多数のアクセス制御と電子決済システムが含まれます。

アプリケーション

ライセンス管理
セキュア機能の制御
システム認証
クローン防止
ドアロック
電気・ガスメータ

標準動作回路



特長

- SHA-1 MAC を生成する専用ハードウェアによる加速 SHA エンジン
- エンド機器のプロパティデータを保存するための 112 バイトのユーザ EEPROM
- I^2C ホストインタフェースが 100kHz および 400kHz の通信速度をサポート
- I^2C アドレス割当て用の 3 つのアドレス入力
- シングルバイト～8 バイトの EEPROM 書込みシーケンス
- 64 ビットの固有登録番号
- EEPROM 耐久性:200k サイクル/8 バイトブロック(25℃において)
- 最大 EEPROM 書込みサイクル:10ms
- 広い動作範囲:2.7V～5.5V、-40℃～+85℃
- すべてのピンに対する±4kV IEC 1000-4-2 ESD 保護レベル
- 8 ピン SOP (150mil)パッケージ

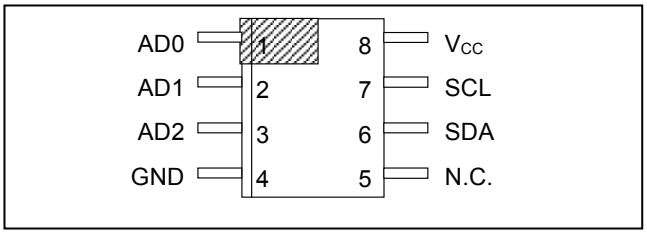
型番

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)

+は鉛フリー準拠を表します。

フルデータシートの請求:
japan.maxim-ic.com/fullds/DS2460

ピン配置



注: この製品の改訂版の中には仕様が公表されたデータシートの仕様と異なり、正誤表として扱われている場合があります。様々な販売チャネルを通し、製品に複数の改訂版が同時に存在することがあります。デバイスの正誤表に関しては、japan.maxim-ic.com/errataをご覧ください。

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.

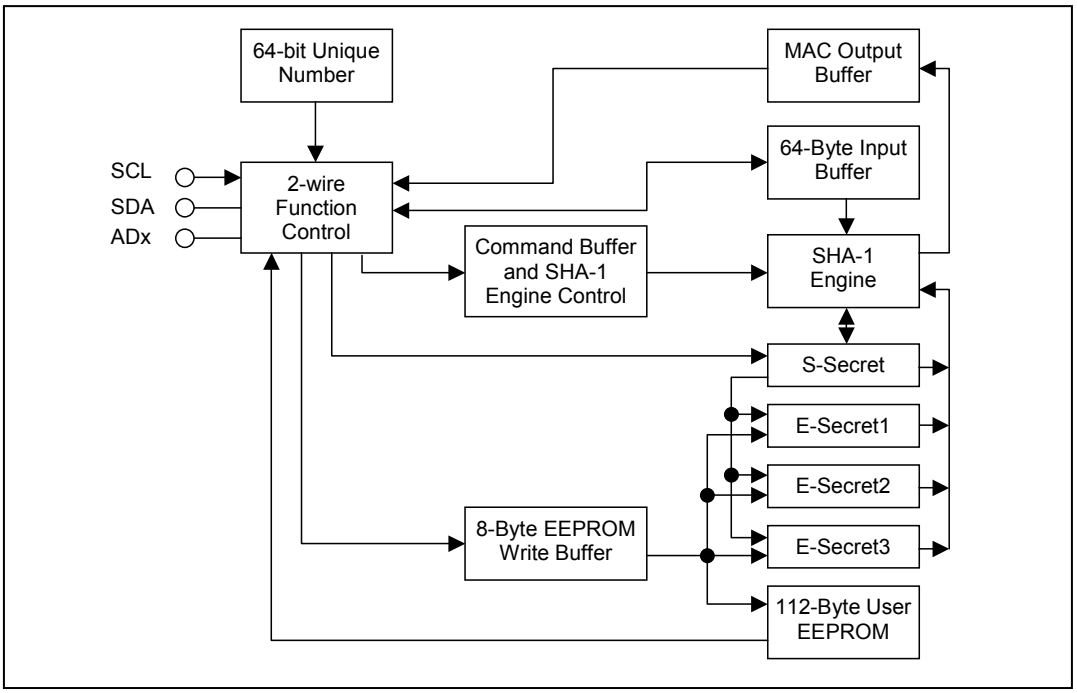
端子説明

端子	名称	機能
1	AD0	I^2C アドレス入力;VCC または GND に接続する必要があります。これらの入力によってデバイスの I^2C スレーブアドレスを決定します(図 5 参照)。
2	AD1	
3	AD2	
4	GND	グランド基準
5	NC	接続なし
6	SDA	I^2C シリアルデータ入力/出力;プルアップ抵抗器を介して V_{CC} に接続する必要があります。
7	SCL	I^2C シリアルクロック入力;プルアップ抵抗器を介して V_{CC} に接続する必要があります。
8	V_{CC}	電源入力

概要

図 1 のブロック図は、DS2460 の主要な制御セクションとメモリセクションの関係を示します。DS2460 は、その I^2C バスインタフェースを通じて標準モードまたは高速モードでホストプロセッサと通信します。3 つのアドレス端子のロジック状態が、DS2460 の I^2C スレーブアドレスを決定するため、ハブを使用せずに最大 8 個のデバイスを同一バスセグメント上で動作させることができます。詳細情報および図 2 に関しては、完全版のデータシートをご覧ください。

図 1. ブロック図



レジスタの詳細

この項および図 3 に関しては、完全版のデータシートをご覧ください。

デバイスの動作

アプリケーションにおける DS2460 の標準的な使用法には、書込み、読取り、SHA-1 エンジンの駆動、シークレットの転送、および MAC の比較などがあります。これらのアクティビティはすべて、I^2C シリアルインタフェースによって制御されます。

I^2C シリアル通信インタフェース

一般的な特性

I^2C バスでは、データライン(SDA)とクロック信号(SCL)が通信に使用されます。SDA と SCL はいずれも、双方向ラインでプルアップ抵抗器を介して正電源電圧に接続されます。通信が行われないときは、両ラインがハイです。バスに接続されたデバイスの出力段は、ワイヤド AND 機能を実行するためにオープンドレインまたはオープンコレクタを備えている必要があります。I^2C バス上のデータは、標準モードでは最大 100kbps、高速モードでは最大 400kbps のレートで転送されます。DS2460 はこれら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と定義され、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。個別にアクセスすることができるように、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。

データ転送は、バスがビジーでないときのみ開始することができます。マスタは、シリアルクロック(SCL)を生成し、バスアクセスを制御し、START および STOP 条件を生成し、START と STOP の間で転送されるデータバイト数を決定します(図 4)。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。各バイトの後には、マスタとスレーブを同期させるための確認応答ビットが続きます。

スレーブアドレス

DS2460 が応答するスレーブアドレスを図 5 に示します。アドレス端子 AD0、AD1、および AD2 のロジック状態がアドレスビット A0、A2、および A4 の値を決定します。これらのアドレス端子によって、デバイスは 8 つのスレーブアドレスの 1 つに応答することができます。スレーブアドレスは、スレーブアドレス/制御バイトの一部です。スレーブアドレス/制御バイト(R/$\overline{W}$)の最終ビットは、データ方向を規定します。このビットが 0 に設定されると後続データはマスタからスレーブに流れ(書込みアクセスモード)、1 に設定され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 4. I^2C プロトコルの概要

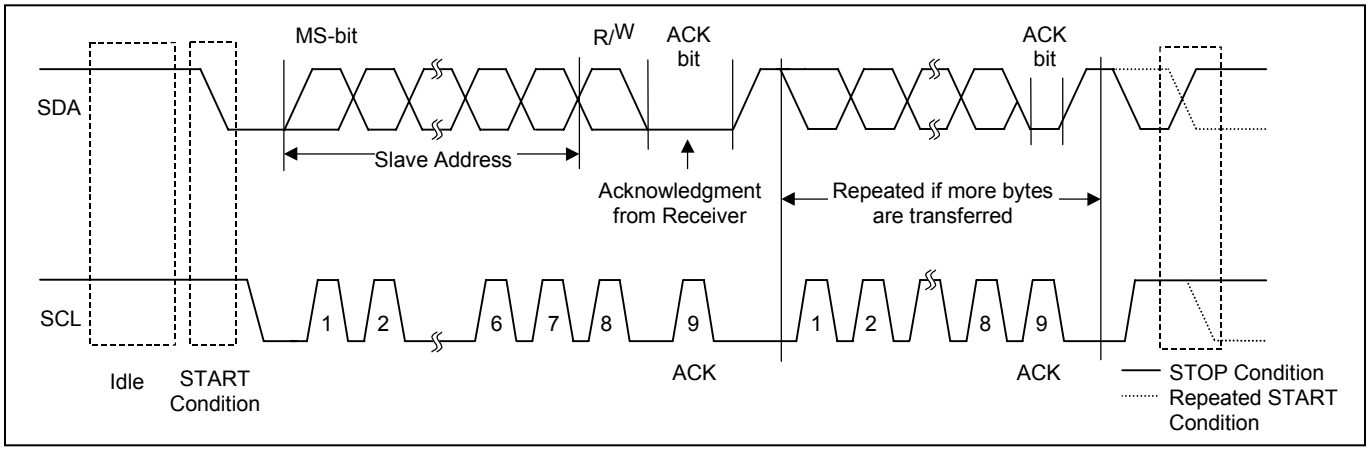
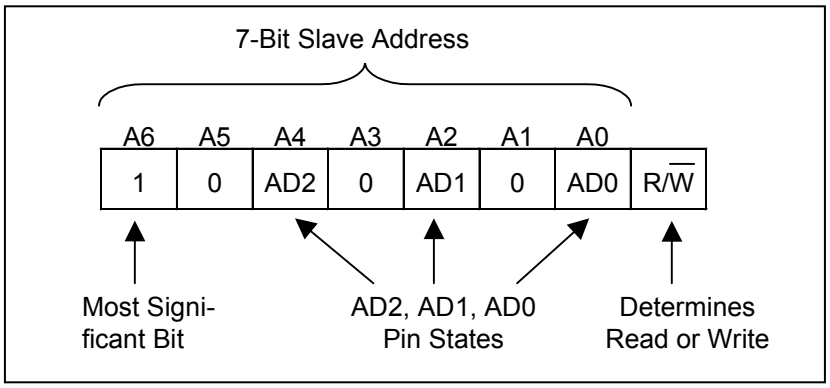


図 5. DS2460 のスレーブアドレス



I^2C の定義

以下の術語は I^2C データ転送を記述するために一般に使用されます。タイミングの基準を図 6 で定義します。

バスアイドルまたは非ビジー

SDA と SCL は、いずれも非アクティブで、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は、マスタが START 条件を生成する必要があります。START 条件は、SCL がハイ状態での SDA のハイからローへの状態変化と定義されます。有効なスレーブアドレスは、マスタによって送信され、後続の START 条件が認識される前にスレーブによって確認応答される必要があります。

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 がハイ状態での SDA のローからハイへの状態変化と定義されます。有効なスレーブアドレスは、マスタによって送信され、後続の STOP 条件が認識される前にスレーブによって確認応答される必要があります。

反復 START 条件
反復 START は、読取り対象の特定データソースまたはアドレスを選択するための読取りアクセスに一般に使用されます。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、STOP 条件の後にバスアイドル状態にはなりません。

データ有効
START および STOP 条件を除く SDA の遷移は SCL がロー状態の間にのみ行われます。SDA のデータは、SCL の全ハイパルス期間ならびに所要セットアップおよびホールド時間(SCL の立下りエッジ後 $t_{HD:DAT}$ および SCL の立上りエッジ前の $t_{SU:DAT}$ (図 6 参照))は有効かつ不変に保たれる必要があります。データの各ビットに 1 クロックパルスが対応します。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。

書込みが終了すると、SCL の次の立上りエッジで読取りが開始される前にマスタは十分なセットアップ時間(図 6 の最小 $t_{SU:DAT}$ ＋ t_R)だけ SDA ラインを解放する必要があります。スレーブは先行する 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、この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ものも含めてすべての SCL クロックパルスを生成します。

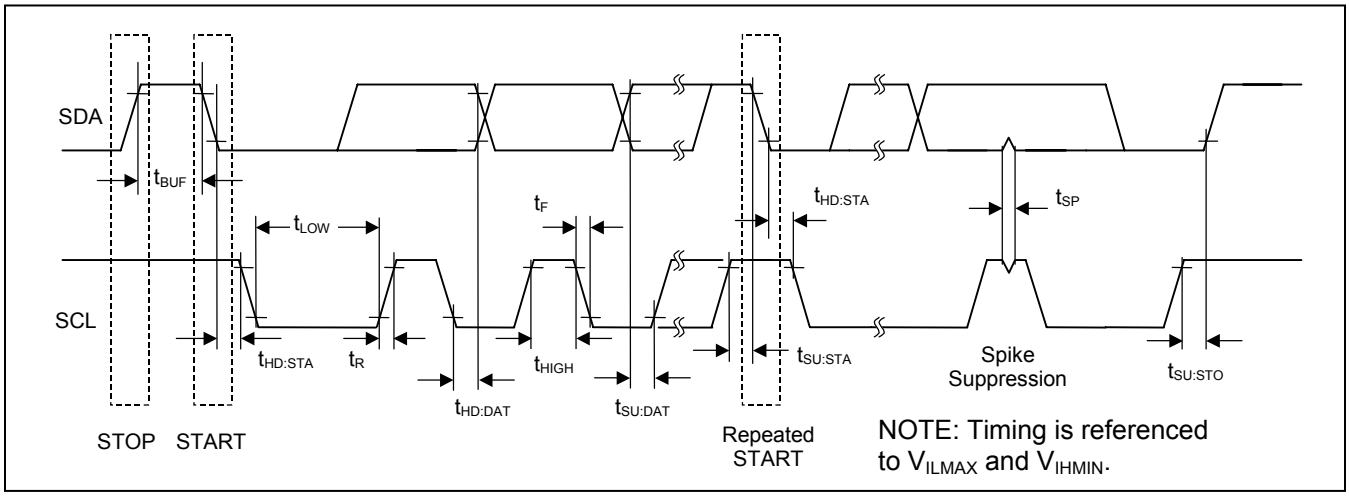
確認応答
通常、アドレス指定された受信デバイスは各バイトの受信後に確認応答を生成しなければなりません。マスタは、この確認応答ビットに対応するクロックパルスを生成する必要があります。確認応答するデバイスは、確認応答クロックパルスの間 SDA をローに駆動して、確認応答に関係するクロックパルスのハイ期間ならびに所要のセットアップおよびホールド時間(SCL の立下りエッジ後 $t_{HD:DAT}$ および SCL の立上りエッジ前の $t_{SU:DAT}$)に SDA が安定なロー状態に保たれるようにする必要があります。

スレーブによる非確認応答
スレーブデバイスは、MAC 計算や EEPROM 書込みサイクルのようなリアルタイム機能を実行中であるなどの理由で、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、スレーブデバイスはそのスレーブアドレスを確認応答せずに SDA ラインをハイの状態に保ちます。

通信準備の整ったスレーブデバイスは少なくともそのスレーブアドレスを確認応答します。しかし、しばらくしてスレーブはコマンドやアクセスモードが無効であるなどの理由でデータ受入れを拒否したり、MAC の非一致を伝達するために拒否したりする場合があります。この場合、スレーブデバイスは拒否するバイトのいずれにも確認応答せずに SDA をハイの状態に保ちます。いずれにせよ、スレーブが確認応答しなかった場合は、マスタがまず反復 START 条件または STOP 条件に続いて START 条件を生成して新たなデータ転送を開始する必要があります。

マスタによる非確認応答
マスタは、データを受信する際のある時点でデータの終了をスレーブデバイスに伝達する必要があります。この実現のために、マスタはスレーブから受信した最終バイトを確認応答しません。これに対し、スレーブは SDA を解放するため、マスタは STOP 条件を生成することができます。

図 6. I^2C タイミング図



読取りと書込み
この項では、さまざまなレジスタおよび EEPROM の読取りと書込み動作について説明しています。詳細に関しては、完全版のデータシートをご覧ください。

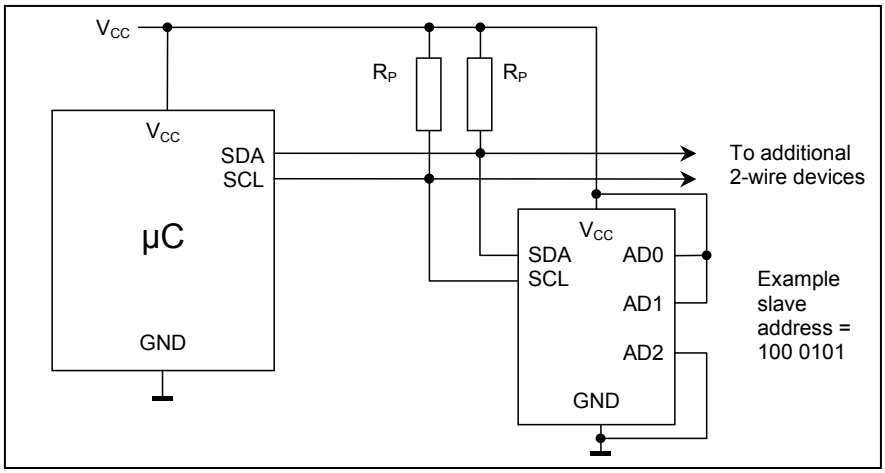
SHA-1 エンジン制御
この項では、SHA-1 エンジンのユーザの観点と動作方法を説明しています。詳細および図 7～9 および表 1 と 2 に関しては、完全版のデータシートをご覧ください。

SHA-1 の計算アルゴリズム
SHA計算の以下の説明は、NISTのウェブサイト(www.itl.nist.gov/fipspubs/fip180-1.htm)からダウンロード可能なSecure Hash Standard SHA-1ドキュメントを改作したものです。詳細に関しては、完全版のデータシートをご覧ください。

アプリケーション情報

SDA および SCL のプルアップ抵抗器
SDA は、ハイのロジックレベルを実現するためのプルアップ抵抗器を必要とする DS2460 のオープンドレイン出力(図 10)です。DS2460 では SCL を入力としてのみを使用するため(クロック伸張なし)、マスタはプルアップ抵抗器付きオープンドレイン/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。

図 10. アプリケーションの回路図



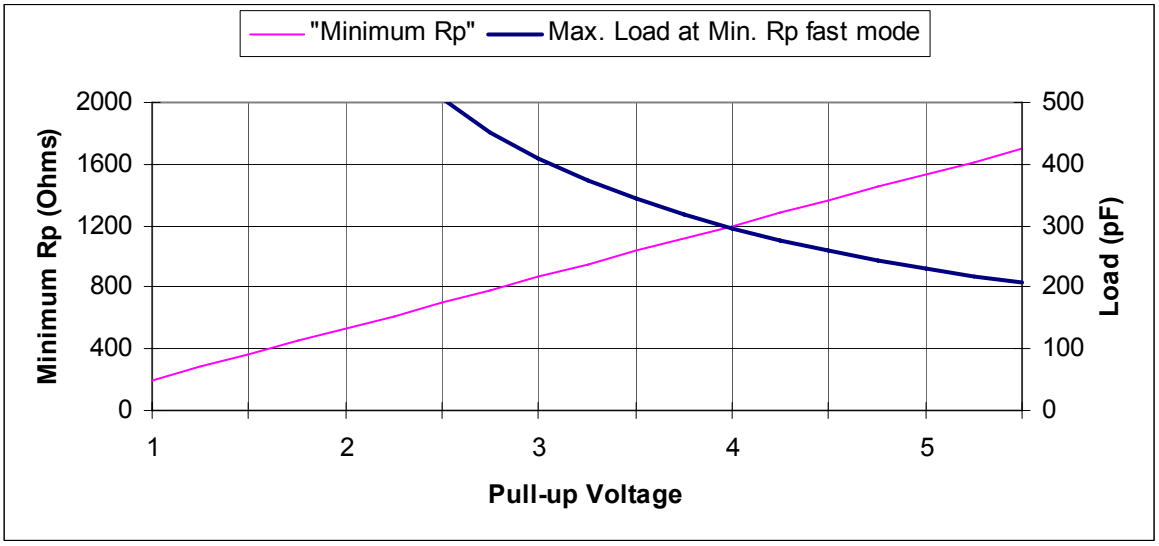
プルアップ抵抗器 R_P の算定
I^2C 仕様によると、スレーブデバイスは 0.4V の V_{OL} において少なくとも 3mA をシンクすることができなければなりません。この DC 条件は、プルアップ抵抗器の最小値を決定します。すなわち、**$R_{PMIN} = (V_{CC} - 0.4V)/3mA$**。動作電圧が 5.5V の場合、プルアップ抵抗器の最小値は 1.7kΩ です。図 11 の「Minimum R_P」ラインは、最小プルアップ抵抗器が動作(プルアップ)電圧によって変化する様子を示します。

I^2C 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%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 を超えてはなりません。最大立上り時間を仮定すると、与えられた任意の容量 C_B での最大抵抗器の値が **$R_{PMAX} = 300ns/(C_B*ln(7/3))$**から計算されます。400pF のバス容量では、最大プルアップ抵抗器が 885Ω となります。

400pF のバス容量において立上り時間仕様を満たすのに必要と思われる 885Ω のプルアップ抵抗器は 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 11 の「Max. Load…」ラインは、まず所定の動作電圧における最小プルアップ抵抗器(「Minimum R_P」ライン)を計算した後で立上り時間が 300ns となる各バス容量を計算することによって生成されます。

3V 以下のプルアップ電圧に対してのみ、400pF の最大許容バス容量が保たれます。4V 以下のプルアップ電圧に対しては、300pF の低減バス容量が許容されます。高速動作では、いかなるプルアップ電圧においてもバス容量が 200pF を超えてはなりません。電圧に対応するプルアップ抵抗器の値を「Minimum R_P」ラインで示します。

図 11. I^2C 高速プルアップ抵抗器の選択図



パッケージ

(このデータシートに掲載されているパッケージ仕様は、最新版が反映されているとは限りません。最新のパッケージ情報は、japan.maxim-ic.com/DallasPackInfoをご参照下さい。)