19-6564; Rev 2; 2/13

MAXQ1741

DeepCoverセキュアマイクロコントローラ、磁気カード読取り用

概要

DeepCover®エンベデッドセキュリティソリューションは、複数層の高度な物理セキュリティによって機密データを秘匿し、可能な限り最もセキュアなキーストレージを提供します。

DeepCoverセキュアマイクロコントローラ(MAXQ1741)は、3トラック磁気ストライプリーダインタフェース、I^2Cインタフェース、2つのSPIインタフェース、および1つの汎用同期/非同期レシーバ-トランスミッタ(USART)インタフェースを内蔵した低電力マイクロコントローラです。セキュリティ機能には、AES暗号エンジン、真のハードウェア乱数発生器、電圧攻撃センサー、および自己破壊入力ピンが含まれます。シングルサイクル16ビットRISCのMAXQ® CPUがデバイスを駆動します。このデバイスは、高速ハードウェア暗号化を備えた超セキュアマイクロコントローラを磁気カードリーダのヘッド内に配置することによって、高レベルのセキュリティを磁気ストライプリーダに提供します。

このデバイスは、16KBのフラッシュメモリ、およびタンパー検出時に内容がクリアされる1152バイトの高速ワイプ不揮発性SRAM (NV SRAM)を備えています。このNV SRAMの最上位128バイトは、AESのためのデータRAMまたは作業用RAMとして使用することができます。高速ワイプ機能は、1152バイトのメモリ内の任意のデータが、任意のアプリケーションソフトウェアがアクセス可能となる前に破壊されることを保証します。要求に応じて、固有の64ビットシリアルナンバーの出荷時プログラミング、および/またはお客様の秘密鍵が使用可能です。このマイクロコントローラは、1.7V～3.6Vの広い動作電圧範囲で動作します。ユーザーアプリケーションファームウェアは、3トラック磁気ストライプインタフェースと通信します。リファレンスソフトウェアは、ISO 7811、ISO 7812、およびISO 7813に準拠したカードの読取りをサポートします。リファレンスソフトウェアのソースコードが入手可能なため、独自のカード形式に合わせたアプリケーションの調整が可能です。

超低電力ストップモードは、最高の低電力性能を提供します。このモードでは、自己破壊イベントの検出をサポートするための最小限の回路のみが動作します。主電源が存在し、マイクロコントローラがストップモードの場合、デバイスは汎用ポート端子またはシリアルインタフェースからの信号でストップモードを解除するオプションを備えています。

アプリケーション

ATM/POS端末
物理セキュリティ/ビルアクセス

特長

- **コア機能**
  - 高性能、低電力、16ビットMAXQ20C RISCコア
  - 6MHzの内蔵発振器(±10%)
  - 最大12MHzの外付け水晶をサポート
  - 動作電圧：1.7V～3.6V
  - デバッガおよびフラッシュプログラミング用の1-Wire®インタフェース
  - Cコンパイラ向けに最適化
- **セキュリティ**
  - AESハードウェアアクセラレータ
  - ハードウェアの真の乱数発生器
  - タンパー検出用の自己破壊入力
  - 永続的なローダロックアウトオプション
  - コードスクランブル
- **メモリ**
  - 16KBのフラッシュメモリ
1024バイトのメモリページセクタ
セクタ当りの消去/書込みサイクル：1000回
  - 1152バイトの高速ワイプNV SRAM、128バイトを暗号エンジンで使用可能
  - ユーザー呼び出し可能ルーチンを備えた6KBのユーティリティROM
- **I/Oおよびペリフェラル**
  - 3トラック磁気ストライプヘッドインタフェース
  - 2つのSPI通信ポート
  - USART通信ポート
  - 2つの16ビットタイマー
  - I^2C通信ポート
  - 最大16の汎用I/O端子
  - 最大8つの外部割込み端子
- **低消費電力**
  - 超低電力ストップモードの電流：3µA
  - 6MHzで3.75mA (typ)、1MHzで0.8mA (typ)
  - システムクロック分周モードを利用可能
- **追加のペリフェラル**
  - パワーオン/パワーフェイルリセット内蔵
  - 電源過電圧検出
  - 設定可能なウォッチドッグタイマ
  - ウェイクアップタイマー

型番はデータシートの最後に記載されています。

関連部品およびこの製品とともに使用可能な推奨製品については、japan.maximintegrated.com/MAXQ1741.relatedを参照してください。

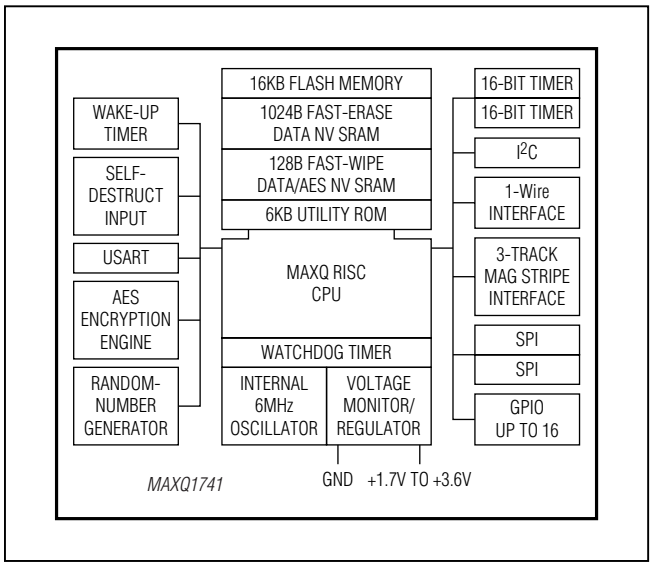
注：このデバイスの一部の改訂版には公表された仕様とは異なる内容が含まれている場合があり、正誤表の形で告知されています。様々な販売チャネルを通し、いずれのデバイスについても複数の改訂版が同時に存在する場合があります。デバイスの正誤表については、japan.maximintegrated.com/errataを参照してください。

価格、納期、発注情報についてはMaxim Direct (0120-551056)にお問い合わせいただくか、Maximのウェブサイト(japan.maximintegrated.com)をご覧ください。

MAXQ1741

DeepCoverセキュアマイクロコントローラ、磁気カード読取り用

ブロック図



詳細

MAXQ1741は、磁気カードリーダへの内蔵を目的としたMAXQ20Cベースのマイクロコントローラです。3トラック磁気カードリーダヘッドと直接インタフェース可能で、POSやATMのカードリーダのマシン/カードインタフェース部分にセキュリティ機能を追加することができます。暗号化はハードウェアAESエンジンによって提供されます。セキュリティ機能には、タンパー検出用の自己破壊入力、コードスクランブル、およびタンパー検出時のNV SRAMの高速ワイプが含まれ、過電圧状態に対する電源レール監視を備えています。16KBのフラッシュメモリは、ユーザープログラムおよび他の固定の不揮発データ用に不揮発ストレージを提供します。

このデバイスは、タンパー検出時に内容が消去される1152バイトの高速ワイプNV SRAMを備えています。NV SRAMの最上位128バイトは、AESのためのデータRAMまたは作業用RAMとして使用することができます。高速ワイプ機能は、アプリケーションソフトウェアによるアクセスが可能となる前に1152バイトのメモリ内の全データが破壊されるようにします。通信ペリフェラルには、ハードウェアI^2C、ハードウェアUSART、および2つのハードウェアSPIが含まれます。システムのプログラミングおよびアプリケーションのデバッグ用に1-Wireポートが利用可能です。

マイクロプロセッサ

MAXQ20Cコアは、個別の16ビットプログラムおよびデータアドレスバスを備えたハーバードメモリアーキテクチャをサポートします。固定16ビット命令ワードが標準ですが、データは8または16ビット構成が可能です。MAXQコアはパイプライン化されたプロセッサとして実装されているため、MHz当り1MIPSに近い性能を発揮します。レジスタモジュールの周囲に16ビットデータパスが実装され、個々のレジスタモジュールが特定の機能をコアに提供します。アキュムレータモジュールは16の16ビットレジスタで構成され、算術論理ユニット(ALU)と密結合されています。プログラムフローは設定可能なソフトスタックによってサポートされます。

命令の実行は、機能レジスタモジュール間または機能レジスタモジュールとメモリ間のデータ転送によって起動されます。データ移動には送信元モジュールと送信先モジュールのみが関与するため、回路切り替え動作はアクティブなモジュールのみに限定されます。電力を意識したアプリケーションの場合、この方式によって消費電力が局所的となりスイッチングノイズが最小限に抑えられます。モジュール型アーキテクチャは、組み込みアプリケーションで使用されるマイクロプロセッサにとって重要な最大の柔軟性と再利用性も提供します。

MAXQの命令セットは非常に高い直交性を備えています。すべての算術および論理演算は、任意のレジスタをアキュムレータと組み合わせて使用することが可能です。任意のレジスタ間のデータ移動がサポートされています。メモリへのアクセスは、自動インクリメント/デクリメント機能を備えた特定のデータポインタレジスタを介して行われます。

メモリ

このマイクロコントローラは、複数のメモリタイプを内蔵しています。

- 16KBフラッシュメモリ
- 1152バイト高速ワイプNV SRAM（AESエンジンが使用する128バイトを含む）
- 6KBユーティリティROM
- RAMベースのソフトウェアスタック

NV SRAMはDRSイベントによってクリアされます。AES機能を使用していない場合、128バイトのメモリは汎用メモリとして使用可能です。AESエンジンを起動すると、このメモリに保存されているデータは無効化されます。

MAXQ1741

DeepCoverセキュアマイクロコントローラ、磁気カード読取り用

補足資料

このデバイスの全機能を完全に使用するために、設計者は以下のドキュメントを入手する必要があります。このデータシートには、端子説明、機能の概要、および電気的仕様が記載されています。正誤表には公表されている仕様との差異が記載されています。ユーザーガイドは製品の特長および動作についての詳しい情報を提供しています。

- このMAXQ1741のデータシート(電気的/タイミング仕様および端子説明が記載されています)
- リビジョン固有のMAXQ1741の正誤表
- 「MAXQ174X User's Guide」(プログラミングを含む、コア機能および動作についての詳細情報が記載されています)

開発およびテクニカルサポート

以下のものを含む、このマイクロコントローラ用の非常に汎用的な、低価格の各種開発ツールがMaximおよびサードパーティサプライヤから提供されています。

- コンパイラ
- インサーキットエミュレータ
- 統合開発環境(IDE)

開発ツールベンダーの一部が記載されたリストについては、**japan.maximintegrated.com/MAXQ_tools**を参照してください。

テクニカルサポートについては、**https://support.maximintegrated.com/jp/micro**をご覧ください。

型番

PART	TEMP RANGE	OPERATING VOLTAGE (V)	FLASH MEMORY (KB)	DATA MEMORY (KB)	PIN-PACKAGE
MAXQ1741-FBX+	-40°C to +85°C	1.70 to 3.6	16	1	28 TQFN-EP*
MAXQ1741-DNS+	-40°C to +85°C	1.70 to 3.6	16	1	Bare die

注：詳細については「MAXQ174X User's Guide」を参照してください。
+は鉛(Pb)フリー/RoHS準拠パッケージを表します。
*EP = エクスポーズドパッド。

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(フットプリント)は**japan.maximintegrated.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を注意してください。

パッケージタイプ	パッケージコード	外形図No.	ランドパターンNo.
28 TQFN-EP	T2844+1	21-0139	90-0035

注：この資料はフルデータシートの要約版です。フルデータシートは**japan.maximintegrated.com/MAXQ1741**からご請求ください。「**フルデータシートを請求する**」をクリックしてください。