19-6564; Rev 2; 2/13

MAXQ1741

用于磁卡读卡器的DeepCover安全微控制器

概述

DeepCover™嵌入式安全方案采用多重先进的物理安全机制保护敏感数据，提供最高等级的密钥存储安全保护。

DeepCover安全微控制器(MAXQ1741)是低功耗微控制器，集成三轨磁条读卡器接口、I²C接口、两个SPI接口和一个通用同步/异步收发器接口(USART)。安全功能包括AES加密引擎、硬件随机数发生器、电压攻击检测器和自毁输入引脚。单周期16位RISC MAXQ® CPU提供强大的器件支持，通过在磁卡读卡器内部安装超级安全微控制器(内置高速硬件加密引擎)，为磁条读卡器提供高度可靠的安全保护。

器件提供16KB闪存和1152字节快速擦除非易失SRAM (NV SRAM)，一旦检测到篡改操作立即将其内容清零。NV SRAM的最高128个字节可以用作数据RAM或支持AES的工作RAM。快速擦除功能确保在任何软件访问器件之前擦除1152字节存储器中的所有数据。可根据用户要求提供工厂预置的64位唯一序列号和/或用户密钥。微控制器工作在1.7V至3.6V较宽的电源范围，提供带有三轨磁条读卡器接口的用户应用固件。参考程序支持ISO 7811、ISO 7812和ISO 7813标准读卡器。提供参考设计的源程序，可以根据定制读卡器的格式进行调整。

超低功耗停止模式提供极低功耗性能，停止模式下只有少数支持自毁检测事件的电路处于供电状态。当主电源上电、微控制器处于停止模式时，器件可以通过通用端口引脚或串口触发，退出停止模式。

应用

ATM/POS终端

安全设施/楼宇门禁

特性

- ♦ 核心功能
  - ✧ 高性能、低功耗、16位MAXQ20C RISC核
  - ✧ 6MHz内部振荡器(±10%)
  - ✧ 支持最高12MHz外部晶振
  - ✧ 1.7V至3.6V供电
  - ✧ 1-Wire®接口支持调试和闪存编程
  - ✧ 优化C编译器
- ♦ 安全
  - ✧ AES硬件加速器
  - ✧ 硬件随机数发生器
  - ✧ 自毁输入用于篡改检测
  - ✧ 可选择永久闭锁装载器
  - ✧ 扰码
- ♦ 存储器
  - ✧ 16KB闪存存储器
    - 1024字节存储器页扇区
    - 每个分区具有1000擦除/写次数
  - ✧ 1152字节可快速擦除NV SRAM、加密引擎使用128字节
  - ✧ 6KB固定用途ROM支持用户程序
- ♦ I/O和外设
  - ✧ 三轨磁条读卡器接口
  - ✧ 两个SPI通信端口
  - ✧ USART通信端口
  - ✧ 两个16位定时器
  - ✧ I²C通信端口
  - ✧ 多达16个通用I/O引脚
  - ✧ 8个外部中断引脚
- ♦ 低功耗
  - ✧ 低功耗停止模式下仅消耗3µA电流
  - ✧ 3工作在6MHz时消耗3.75mA (典型值)电流，1MHz时消耗0.8mA (典型值)电流
  - ✧ 可以工作在分频后的系统时钟
- ♦ 附加外设
  - ✧ 内置上电复位/电源失效复位
  - ✧ 电源过压检测
  - ✧ 可编程看门狗定时器
  - ✧ 唤醒定时器

定购信息在数据资料的最后给出。

相关型号以及配合该器件使用的推荐产品，请参见：china.maximintegrated.com/MAXQ1741.related。

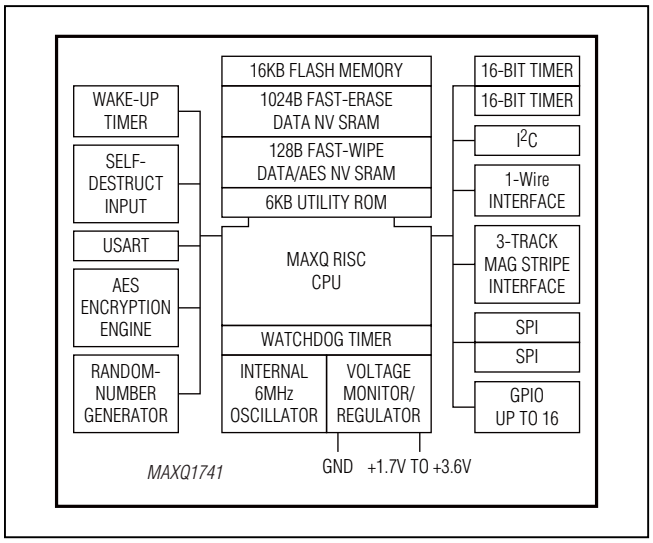
***注：**该器件的部分版本与公布的技术资料有出入，请参见勘误表。不同的销售渠道可同时提供多个版本的器件。关于器件勘误表的信息，请参见：china.maximintegrated.com/errata。*

本文是英文数据资料的译文，文中可能存在翻译上的不准确或错误。如需进一步确认，请在您的设计中参考英文资料。
有关价格、供货及订购信息，请联络Maxim亚洲销售中心：10800 852 1249 (北中国区)，10800 152 1249 (南中国区)，或访问Maxim的中文网站：china.maximintegrated.com。

MAXQ1741

用于磁卡读卡器的DeepCover安全微控制器

方框图



详细说明

MAXQ1741是基于MAXQ20C的微控制器，用于集成至读卡器。器件可直接连接至3轨读卡器，在机器/磁卡接口上为POS或ATM读卡器提供安全性。由硬件AES引擎提供加密。安全特性包括自毁输入(用于篡改检测)、扰码、在检测到篡改时快速擦除NV SRAM，以及电源轨监测(过压条件)。16KB闪存为用户程序及其它静态、非易失数据提供非易失存储。

器件提供1152字节快速擦除NV SRAM，一旦检测到篡改操作立即将其内容清除。NV SRAM的最高128个字节可以用作数据RAM或支持AES的工作RAM。快速擦除功能确保在任何软件访问器件之前擦除1152字节存储器中的所有数据。通信外设包括硬件I²C、硬件USART和两路硬件SPI。提供一个1-Wire端口，用于系统编程和应用程序调试。

微处理器

MAXQ20C内核支持Harvard存储架构，具有独立的16位程序和数据地址总线。使用固定的16位指令字，但数据可为8或16位。MAXQ内核设计为流水线处理器，性能达到1MIPS/MHz。16位数据通路围绕寄存器模块设计，每个寄存器模块为内核提供特定功能。累加器模块包括十六个16位寄存器，与算术逻辑单元(ALU)紧密配合。程序流由可配置的软堆栈支持。

功能寄存器模块之间或功能寄存器模块与存储器之间的数据传输触发指令执行。由于数据流动仅涉及源和目标模块，所以电路切换动作仅限于活动模块。对于功率敏感应用，这种方法减少了功耗并最大程度降低切换噪声。模块式结构也提供了最大程度的灵活性和可复用性，对于嵌入式应用中的微处理器非常重要。

MAXQ指令集设计为高度正交。全部算术和逻辑操作可以采用任意寄存器结合累加器。数据可以在任意寄存器之间流动。通过支持自动递增/递减的专用数据指针寄存器访问存储器。

存储器

微控制器包括多种类型的存储器：

- 16KB闪存
- 1152字节快速擦除NV SRAM，包括128字节供AES引擎使用的存储器
- 6KB固定用途ROM
- 基于RAM的软堆栈

NV SRAM由DRS事件清零。如果不使用AES功能，128字节存储器可作为通用存储器；启动AES引擎将造成存储在该存储区域的数据作废。图3所示为存储器映射。

MAXQ1741

用于磁卡读卡器的DeepCover安全微控制器

其它文档

设计人员需参考以下文档，以充分使用该器件的全部功能。数据资料(包括引脚说明、特性和电气规范)、勘误表包含了与已发布版本的电气规格差异。用户指南提供了器件特性和工作的详细信息。

- MAXQ1741数据资料，含有电气/定时规格和引脚说明。
- 版本相关的MAXQ1741修订勘误表。
- *MAXQ174X用户指南*，含有关于内核功能和工作的详细信息，包括编程。

开发和技术支持

Maxim及第三方供应商可提供适用于该微控制器的各种多功能、高性价比开发工具，包括：

- 编译器
- 在线仿真器
- 集成开发环境(IDC)

部分开发工具供应商的列表可从网站查找：**china.maximintegrated.com/MAXQ_tools**。

技术支持请参见**https://support.maximintegrated.com/micro**。

定购信息

器件	温度范围	工作电压(V)	闪存(KB)	数据存储器(KB)	引脚–封装
MAXQ1741-FBX+	-40°C至+85°C	1.70至3.6	16	1	28 TQFN-EP*
MAXQ1741-DNS+	-40°C至+85°C	1.70至3.6	16	1	Bare die

***注：**更多信息请参见MAXQ174X用户指南。*
+表示无铅(Pb)/符合RoHS标准的封装。
**EP = 裸焊盘。*

封装信息

如需最近的封装外形信息和焊盘布局(占位面积)，请查询**china.maximintegrated.com/packages**。请注意，封装编码中的“+”、“#”或“–”仅表示RoHS状态。封装图中可能包含不同的尾缀字符，但封装图只与封装有关，与RoHS状态无关。

封装类型	封装编码	外形编号	焊盘布局编号
28 TQFN-EP	T2844+1	**21-0139**	**90-0035**

注意：该文件是完整数据资料的缩略版。其他产品信息仅在完整版的数据资料中。如需申请完整版，请浏览**china.maximintegrated.com/MAXQ1741**并点击**申请数据资料全文**。