CEC1736 开发板
用户指南
#EV19K07A

© 2023 Microchip Technology Inc. 及其子公司

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在正常使用且符合工作规范的情况下， Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。 Microchip 承诺将不断改进产品的代码保护功能。

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc. 及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc. 的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 https://www.microchip.com/en-us/support/design-help/client-supportservices。

Microchip “按原样”提供这些信息。 Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或间接的损失、损害或任何类型的开销， Microchip 概不承担任何责任，即使 Microchip 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔， Microchip 在任何情况下所承担的全部责任均不超出您为获得这些信息向 Microchip 直接支付的金额（如有）。如果将 Microchip 器件用于生命维持和 / 或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。除非另外声明，在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

有关 Microchip 质量管理体系的更多信息，请访问 www.microchip.com/quality。

商标

Microchip 的名称和徽标组合、Microchip 徽标、Adaptec、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、TimeSource、tinyAVR、UNI/O、Vectron 及 XMEGA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的注册商标。

AgileSwitch、APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、Flashtec、Hyper Speed Control、HyperLight Load、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、TrueTime和ZL均为Microchip Technology Incorporated在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、Augmented Switching、BlueSky、BodyCom、Clockstudio、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、GridTime、IdealBridge、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、IntelliMOS、Inter-Chip Connectivity、JitterBlocker、Knob-on-Display、KoD、maxCrypto、maxView、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、RTAX、RTG4、SAM-ICE、Serial Quad I/O、simpleMAP、SimpliPHY、SmartBuffer、SmartHLS、SMART-I.S.、storClad、SQI、SuperSwitcher、SuperSwitcher II、Switchtec、SynchroPHY、Total Endurance、Trusted Time、TSHARC、USBCheck、VariSense、VectorBlox、VeriPHY、ViewSpan、WiperLock、XpressConnect 和 ZENA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的商标。

SQTP 为 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 均为 Microchip Technology Inc. 在除美国外的国家或地区的注册商标。

GestIC 为 Microchip Technology Inc. 的子公司 Microchip Technology Germany II GmbH & Co. KG 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

© 2023, Microchip Technology Incorporated及其子公司版权所有。

ISBN：978-1-6683-1911-6

© 2023 Microchip Technology Inc. 及其子公司

目录

前言 4
简介 4
文档编排 4
本指南使用的约定 5
Microchip 网站 6
开发系统变更通知客户服务 6
客户支持 7
文档版本历史 7
第 1 章 简介 8
第 2 章 特性 9
2.1 CEC1736 开发板框图 9
2.2 硬件特性 9
2.3 CEC1736 开发板布局 10
第 3 章 推荐的工具和配件 11
第 4 章 为 CEC1736 开发板供电 12
第 5 章 跳线选项 13
第 6 章 运行开箱即用 （Out-of-Box， OOB）演示代码 16
第 7 章 为开发做好准备 20
7.1 使用用户的系统评估 CEC1736 21
全球销售及服务网点 22

前言

客户须知

本文档如同所有其他文档一样具有时效性。 Microchip 将不断改进工具和文档以满足客户的需求，因此实际使用中有些对话框和 / 或工具说明可能与本文档所述之内容有所不同。请访问我们的网站（www.microchip.com）获取最新文档。

文档均标记有 “DS”编号。该编号出现在每页底部的页码之前。 DS 编号的命名约定为 “DSXXXXXXXXA_CN”，其中 “XXXXXXXX”为文档编号，“A”为文档版本。

欲了解开发工具的最新信息，请参考 MPLAB® IDE 在线帮助。从 Help （帮助）菜单选择 Topics （主题），打开现有在线帮助文件列表。

简介

本文档描述了 Microchip CEC1736 开发板的使用，并详细介绍了其演示设置和执行。

本章包含使用 CEC1736 开发板前需要了解的一般信息。内容包括：

- 文档编排
- 本指南使用的约定
- Microchip 网站
- 开发系统变更通知客户服务
- 客户支持
- 文档版本历史

文档编排

本文档专为希望使用 CEC1736 开发板运行 Microchip CEC1736 演示的人员编写。本手册的内容编排如下：

- **第 1 章 “简介”** —— 说明了本指南的目的和范围。
- **第 2 章 “特性”** —— 提供了开发板特性和布局信息。
- **第 3 章 “推荐的工具和配件”** —— 介绍了演示中建议使用的工具。
- **第 4 章 “为 CEC1736 开发板供电”** —— 介绍了运行演示的步骤和图示说明。
- **第 5 章 “跳线选项”** —— 提供了开发板跳线设置信息。
- **第 6 章 “运行开箱即用 （Out-of-Box， OOB）演示代码”** —— 介绍了开发板随附的 “开箱即用”演示。
- **第 7 章 “为开发做好准备”** —— 介绍了进行用户定制开发的步骤。

© 2023 Microchip Technology Inc. 及其子公司

本指南使用的约定

本指南采用以下文档约定：

文档约定

说明	表示	示例
Arial 字体：		
斜体字	参考书目	*MPLAB® IDE User's Guide*
	需强调的文字	*…… 仅有*的编译器 ……
首字母大写	窗口	Output 窗口
	对话框	Settings 对话框
	菜单选择	选择 Enable Programmer
引用	窗口或对话框中的字段名	“Save project before build”
带右尖括号且有下划线的斜体文字	菜单路径	*File>Save*
粗体字	对话框按钮	单击 **OK**
	选项卡	单击 **Power** 选项卡
N‘Rnnnn	verilog 格式的数字，其中 N 为总位数， R 为基数， n 为其中一位。	4‘b0010， 2‘hF1
尖括号 < > 括起的文字	键盘上的按键	按下 <Enter>， <F1>
Courier New 字体：		
常规 Courier New	源代码示例	`#define START`
	文件名	`autoexec.bat`
	文件路径	`c:\mcc18\h`
	关键字	`_asm， _endasm， static`
	命令行选项	`-Opa+， -Opa-`
	二进制位值	`0， 1`
	常量	`0xFF， ‘A’`
斜体 Courier New	可变参数	*file*.o，其中 *file* 可以是任一有效文件名
方括号 [ ]	可选参数	`mcc18 [选项] file [选项]`
花括号和竖线：{ | }	选择互斥参数； “或”选择	`errorlevel {0|1}`
省略号 ...	代替重复文字	`var_name [, var_name...]`
	表示由用户提供的代码	`void main (void) { ... }`

MICROCHIP 网站

Microchip 网站 （www.microchip.com）为客户提供在线支持。客户可通过该网站方便地获取文件和信息。只要使用常用的互联网浏览器即可访问，网站提供以下内容：

- **产品支持** —— 数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持** —— 常见问题解答 （FAQ）、技术支持请求、在线讨论组以及 Microchip 顾问计划成员名单
- **Microchip 业务** —— 产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、 Microchip 销售办事处、代理商以及工厂代表列表

开发系统变更通知客户服务

Microchip 的客户通知服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请访问 Microchip 网站 www.microchip.com，点击 Customer Change Notification（变更通知客户），然后按照注册说明完成注册。

开发系统的产品类别如下：

- **编译器** ——Microchip C 编译器、汇编器、链接器及其他语言工具的最新信息。包括所有 MPLAB C 编译器、所有 MPLAB 汇编器 （包括 MPASM™ 汇编器）、所有 MPLAB 链接器 （包括 MPLINK™ 目标链接器），以及所有 MPLAB 库管理器 （包括 MPLIB™ 目标库管理器）。
- **仿真器** ——Microchip 在线仿真器的最新信息。其中包括 MPLAB REAL ICE™ 和 MPLAB ICE 2000 在线仿真器。
- **在线调试器** ——Microchip 在线调试器的最新信息。其中包括 MPLAB ICD 3 和 MPLAB ICD 4 在线调试器以及 PICkit™ 3 和 MPLAB PICkit 4 在线调试器。
- **MPLAB IDE**——关于开发系统工具的Windows®集成开发环境Microchip MPLAB IDE 的最新信息，主要针对 MPLAB IDE、 MPLAB IDE 项目管理器、 MPLAB 编辑器、 MPLAB SIM 软件模拟器以及一般编辑和调试功能。
- **编程器** ——Microchip 编程器的最新信息。其中包括生产编程器，例如 MPLAB REAL ICE 在线仿真器、 MPLAB ICD 4 在线调试器、 MPLAB PICkit 4 在线调试器以及 MPLAB PM3 器件编程器。还包括非生产用开发编程器，例如 PICkit 3 在线调试器。

© 2023 Microchip Technology Inc. 及其子公司

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师 （CAE）
- 应用工程师 （ESE）
- 技术支持

客户应联系其代理商、代表或应用工程师（ESE）寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过 http://www.microchip.com/support 获得网上技术支持。

文档版本历史

版本 A （2022 年 5 月 6 日）

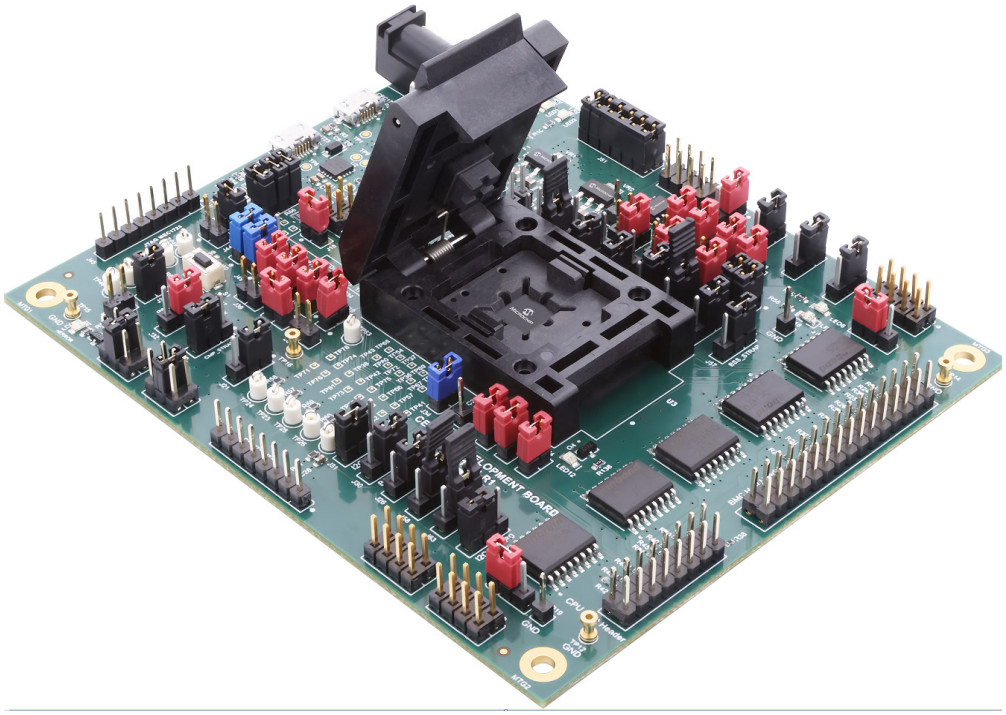
- 本文档的初始版本。

第 1 章 简介

CEC1736 开发板可用作数据中心、电信、网络以及工业和嵌入式计算市场中实时平台可信根应用的演示、开发和测试平台。它具有各种硬件选项（包括电源、用户接口、串行通信和扩展连接器），可实现实时平台可信根应用的快速原型设计和开发。

此开发板具备以下功能，旨在为用户提供开箱即用体验：

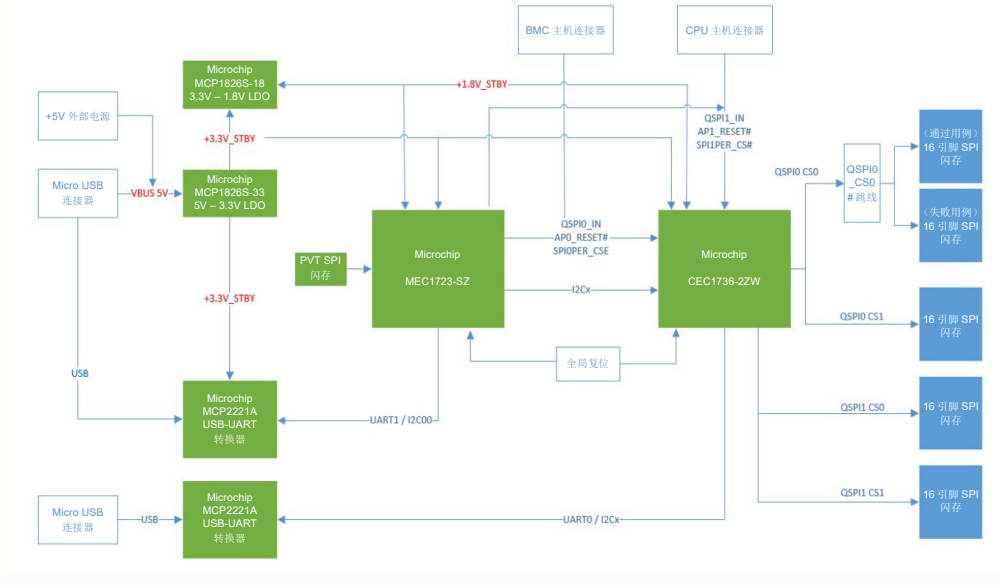
- CEC1736 OTP—— 已使用预定义 OTP 功能进行预编程，支持演示示例。
- CEC1736 内部 SPI 闪存 —— 已使用最新的 Soteria-G3 固件版本进行预编程。
- MEC1723（仿真为应用流程） —— 包含 MEC1723 开箱即用的示例固件，并且可升级以进行演示。
- CEC1736 插座 —— 用户可以使用生产 CEC1736 针对具体设计需求自行开发 OTP 功能。



© 2023 Microchip Technology Inc. 及其子公司

第 2 章 特性

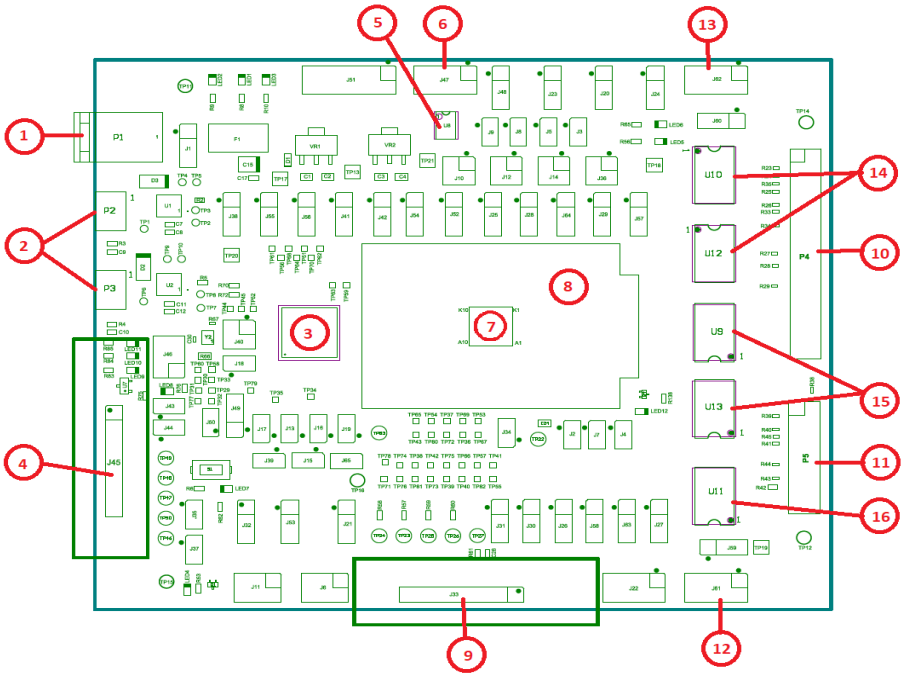
2.1 CEC1736 开发板框图



2.2 硬件特性

- CEC1736 84 引脚插座
- 4 个 16 引脚 256 Mb SPI 闪存，用于正常工作模式
- 1 个 16 引脚 256 Mb SPI 闪存，用于失败用例演示
- 1 个 USB-UART/I2C 端口，供 CEC1736 使用
- 1 个 USB-UART 端口，供 MEC1723 使用
- BMC 主机连接器
- CPU 主机连接器
- 1 个 1x8 PICKIT 4 连接器，用于 CEC1736 调试和编程
- 1 个 1x8 PICKIT 4 连接器，用于 MEC1723 调试和编程
- GPIO/I2C 连接器，用于可选的定制开发
- 开发板可通过 Micro USB 线或 +5V 电源适配器 （未随附）供电

2.3 CEC1736 开发板布局



1. 电源适配器插头（P1）—— 提供另一种开发板供电方式，即通过外部 +5V 电源适配器供电
2. USB micro-B 连接器 —— 为开发板供电，并提供接口，用于将使用 Microchip MCP2221A USB-UART/I2C 串行转换器的串行输入/输出或 I2C 连接到 CEC1736（P2）和 MEC1723 （P3）
3. Microchip MEC1723N-B0-I/SZ （U6） —— 仿真为应用处理器
4. Microchip PICKIT 4 1x8 连接器 （J45），用于 MEC1723
5. Microchip SST26VF040A SPI 闪存（U8），用于 MEC1723 私有闪存引导（可选）
6. Dediprog SF100/SF600 SPI 闪存编程连接器 （J47），连接至 U8

> **注：** J47 引脚 7 和 8 已连接，但可能会影响 Dediprog 运行。如果发生故障，请断开 SFxxx 和连接器之间的引脚 7 和引脚 8 连接

7. Microchip CEC1736-S0-I/2ZW （安装在 U3 插座中）
8. 84 引脚 2ZW 封装插座 （U3）
9. Microchip PICKIT 4 1x8 连接器 （J33），用于 CEC1736
10. BMC 主机连接器 （P4）
11. CPU 主机连接器 （P5）
12. Dediprog SF100/SF600 SPI 闪存编程连接器 （J61），连接至 U9、 U11 或 U13
13. Dediprog SF100/SF600 SPI 闪存编程连接器 （J62），连接至 U10 或 U12
14. CEC1736 QSPI1 通道上的 SPI 闪存 （U10 和 U12）
15. CEC1736 QSPI0 通道上的 SPI 闪存 （U9 和 U13）
16. CEC1736 QSPI0 CS0# 通道上的 SPI 闪存 （U11），仅用于失败用例演示

© 2023 Microchip Technology Inc. 及其子公司

第 3 章 推荐的工具和配件

使用 CEC1736 开发板进行开发时，我们建议使用以下工具：

1. Microchip MPLAB X v6.00 或更高版本
2. XC32 Pro Compiler v2.50 或更高版本
3. PICKit 4 在线调试器，可直接插入
4. ICD 4 在线调试器 + 调试器适配器板 （mD# AC102015）
5. Tera Term v4.106 或更高版本 （或首选等效工具），用于 UART 调试日志
6. （可选）Dediprog SF100 或 SF600（或首选等效工具），用于外部 SPI 闪存编程

用户可通过提交 Microchip 支持申请来获取以下 EV19K17A - CEC1736 开发板技术文档，同时需签署 “保密协议”（Non-Disclosure Agreement， NDA）。

- Altium 设计文件
- Gerber 文件
- 原理图
- 物料清单

如果有任何其他问题，请联系您的 Microchip 代表。

第 4 章 为 CEC1736 开发板供电

CEC1736 开发板可通过 USB 串行转换器的 USB micro-B 端口 （P2 和 / 或 P3）直接供电。通过 MCP1826S 稳压器，可将 USB 电压轨的 5V 输入调节为 3.3V。

（可选） CEC1736 开发板也可以通过电源插头 （P1）由外部电源供电。 5V 可调节为 3.3V，与使用 USB micro-B 端口时一样。可通过 J1 1-2 选择此选项，默认设置为 2-3，即通过 USB 供电。

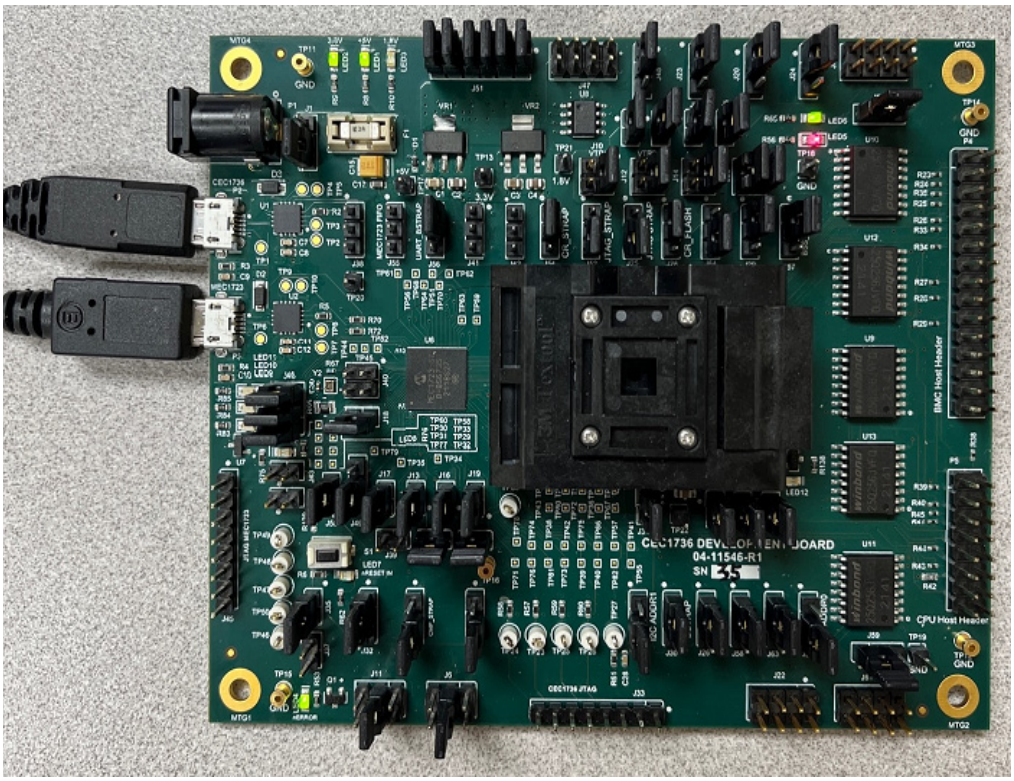
可使用旁路二极管 （D1）来测量使用 USB micro-B 端口时的系统总功耗，或者使用跳线 （J1）来测量使用外部电源时的系统总功耗。

开发板上电后， LED1 （+5V）、 LED2 （+3.3V）和 LED3 （+1.8V）应点亮。

根据 MEC1723 固件应用的状态，LED9、LED10 和 LED11 可能会闪烁，这表明正在加载和执行 MEC1723 固件。

LED4、LED5、LED6 和 LED12 也会闪烁，表明正在加载和执行 CEC1736 Soteria 固件。

上电情况如下图所示：



© 2023 Microchip Technology Inc. 及其子公司

第 5 章 跳线选项

下面概括了 CEC1736 开发板使用的几种跳线：

跳线选项

跳线	说明	详细信息
J1	开发板电源选择	1-2：外部 5V 适配器 （P1）供电 **2-3 （默认）：** Micro-USB 端口 （P2 和 P3）供电
J2	将 VTR 电源连接至 CEC1736	**IN （默认）：** 连接 VTR 电源 OUT：断开 VTR 电源
J3	将 +3.3V 电源连接至 MEC1723	**IN （默认）：** 连接 +3.3V 电源 OUT：断开 +3.3V 电源
J4	将 VTR_PLL 电源连接至 CEC1736	**IN （默认）：** 连接 VTR_PLL 电源 OUT：断开 VTR_PLL 电源
J5	将 +1.8V 电源连接至 MEC1723	**IN （默认）：** 连接 +1.8V 电源 OUT：断开 +1.8V 电源
J6	MCP2221A 的 CEC1736 I2C SCL 选择	1-2：I2C10 **3-4 （默认）：** I2C06 5-6：I2C00
J7	将 VTR_ANALOG 电源连接至 CEC1736	**IN （默认）：** 连接 VTR_ANALOG 电源 OUT：断开 VTR_ANALOG 电源
J8	将 +3.3V 电源连接至 CEC1736	**IN （默认）：** 连接 +3.3V 电源 OUT：断开 +3.3V 电源
J9	将 +1.8V 电源连接至 CEC1736	**IN （默认）：** 连接 +1.8V 电源 OUT：断开 +1.8V 电源
J10	CEC1736 的 VTR1 电源选择	**1-2 （默认）：** 连接 +3.3V 电源 3-4：断开 +1.8V 电源
J11	MCP2221A 的 CEC1736 I2C SDA 选择	1-2：I2C10 **3-4 （默认）：** I2C06 5-6：I2C00
J12	CEC1736 的 VTR2 电源选择	**1-2 （默认）：** 连接 +3.3V 电源 3-4：断开 +1.8V 电源
J13	将 VTR_REG 电源连接至 MEC1723	**IN （默认）：** 连接 VTR_REG 电源 OUT：断开 VTR_REG 电源
J14	MEC1723 的 VTR2 电源选择	**1-2 （默认）：** 连接 +3.3V 电源 3-4：断开 +1.8V 电源
J15	将 VTR_PLL 电源连接至 MEC1723	**IN （默认）：** 连接 VTR_PLL 电源 OUT：断开 VTR_PLL 电源
J16	将 VTR_ANALOG 电源连接至 MEC1723	**IN （默认）：** 连接 VTR_ANALOG 电源 OUT：断开 VTR_ANALOG 电源
J17	将 VTR1 电源连接至 MEC1723	**IN （默认）：** 连接 VTR1 电源 OUT：断开 VTR1 电源
J18	将 VBAT 电源连接至 MEC1723	**IN （默认）：** 连接 VBAT 电源 OUT：断开 VBAT 电源
J19	将 VTR3 电源连接至 MEC1723	**IN （默认）：** 连接 VTR3 电源 OUT：断开 VTR3 电源
J20	CEC1736 GPIO012/nEXTRST 上 / 下拉电阻选择	**1-2 （默认）：** 拉高至 VTR_REG 2-3：下拉

跳线选项

跳线	说明	详细信息
J21	CEC1736 GPIO106/AP0_nRESET 上 / 下拉电阻选择	**1-2（默认）：**拉高至 VTR_REG 2-3：下拉
J22	CEC1736 GPIO 连接器	用于调试
J23	CEC1736 GPIO1316/AP1_nRESET 上 / 下拉电阻选择	**1-2（默认）：**拉高至 VTR_REG 2-3：下拉
J24	CEC1736 nRESET_IN 引脚	**1-2（默认）：**正常工作 2-3：CEC1736 保持复位
J25	CEC1736 JTAG _STRAP 引脚	1-2：进入边界扫描模式 **2-3（默认）：**正常工作
J26	CEC1736 GPIO055 配置选项	无关
J27	CEC1736 I2C_ADDR0 配置	1-2：拉高至 VTR_REG **2-3（默认）：**下拉
J28	CEC1736 CR_FLASH 配置	**1-2（默认）：**正常工作 2-3：从危机恢复闪存元件引导
J29	CEC1736 GPIO124 配置选项	无关
J30	CEC1736 BSTRAP 配置	**1-2（默认）：**正常工作 2-3：从 I2C 或 UART 危机端口引导
J31	CEC1736 I2C_ADDR1 配置	1-2：拉高至 VTR_REG **2-3（默认）：**下拉
J32	CEC1736 RESET_IN# 延迟电路电源	**1-2（默认）：**连接 +3.3V 电源 2-3：连接 VTR_REG 电源
J33	CEC1736 PICKIT 4 1x8 连接器	用于调试
J34	CEC1736 32KHz 单端电源	**IN（默认）：**连接振荡器 OUT：断开振荡器
J35	CEC1736 RESET_IN# 延迟电路	**IN（默认）：**连接延迟电路 OUT：断开延迟电路
J36	CEC1736 GPIO157/LED1 和 GPIO156/LED0 引脚连接	**1-2（默认）：**将 GPIO157 连接至 LED5 **3-4（默认）：**将 GPIO156 连接至 LED6
J37	CEC1736 RESET_IN# 引脚接地	IN：CEC1736 保持复位 **OUT（默认）：**正常工作
J38	CEC1736 UART0 调试头	用于调试
J39	ME1723 测试时钟输出连接器	用于调试
J40	MEC1723 32KHz 单端输入选择（可选）	1-2：连接至 32KHZ_IN 引脚 2-3：连接至 XTAL2
J41	MEC1723 I2C02 通道连接器	用于调试
J42	MEC1723 I2C07 通道连接器	用于调试
J43	MEC1723 RESET_IN# 延迟电路	IN：连接延迟电路 **OUT（默认）：**断开延迟电路
J44	MEC1723 RESET_IN# 引脚接地	IN：MEC1723 保持复位 **OUT（默认）：**正常工作
J45	MEC1723 PICKIT 4 1x8 连接器	用于调试
J46	MEC1723 GPIO156/LED0、GPIO157/LED1 和 GPIO153/LED2 引脚连接	**1-2（默认）：**将 GPIO156 连接至 LED9 **3-4（默认）：**将 GPIO157 连接至 LED10 **5-6（默认）：**将 GPIO153 连接至 LED11
J47	Dediprog SPI 编程连接器	用于 U8 PVT SPI 闪存编程
J48	U8 SPI 闪存电源选择	**1-2（默认）：**连接至开发板 +3.3V 电源 2-3：连接 Dediprog +3.3V 电源
J49	MEC1723 XTAL2 选择	**1-2（默认）：**连接至 2 引脚晶振 2-3：连接至单端 32 KHz 时钟源

© 2023 Microchip Technology Inc. 及其子公司

跳线选项

跳线	说明	详细信息
J50	MEC1723 XTAL1 选择	**IN （默认）：**连接至 2 引脚晶振 OUT：使用单端 32 KHz 时钟源，悬空
J51	U8 SPI 闪存隔离跳线	**1-2 （默认）：**连接 U8 SPI_CLK **3-4 （默认）：**连接 U8 SPI_IO0 **5-6 （默认）：**连接 U8 SPI_IO1 **7-8 （默认）：**连接 U8 SPI_CS# **9-10 （默认）：**连接 U8 SPI_IO2 **11-12 （默认）：**连接 U8 SPI_IO3
J52	MEC1723 JTAG _STRAP 引脚	1-2：进入边界扫描模式 **2-3 （默认）：**正常工作
J53	MEC1723 CMP_STRAP 引脚	无关
J54	MEC1723 CR_STRAP 引脚	**1-2 （默认）：**通过 CEC1736 从 SHD_SPI 闪存引导 2-3：从 PVT_SPI 闪存 （U8）引导
J55	MEC1723 UART0 调试头	用于调试
J56	MEC1723 UART_BSTRAP 引脚	**1-2 （默认）：**正常工作 2-3：从 UART 危机端口引导
J57	MEC1723 BSS_STRAP 引脚	**1-2 （默认）：**正常工作 2-3：在此应用中不引导
J58	CEC1736 QSPI0 CS0 通过 / 失败用例选择，用于演示目的	**1-2 （默认）：**通过 U9 演示正常通过用例 2-3：通过 U11 演示失败用例
J59	CEC1736 闪存总线 1 电源选择	**1-2 （默认）：**连接至开发板 +3.3V 电源 2-3：连接 Dediprog +3.3V 电源
J60	CEC1736 闪存总线 2 电源选择	**1-2 （默认）：**连接至开发板 +3.3V 电源 2-3：连接 Dediprog +3.3V 电源
J61	Dediprog SPI 编程连接器	用于 U9、 U11 或 U13 SPI 闪存编程
J62	Dediprog SPI 编程连接器	用于 U10 或 U12 SPI 闪存编程
J63	U9/U11 或 U13 SPI 闪存编程选择	**1-2 （默认）：**连接至 U9/U11，通过 J58 选择 2-3：连接至 U13
J64	U10 或 U12 SPI 闪存编程选择	**1-2 （默认）：**连接至 U10 2-3：连接至 U12
J65	CEC1736 AP0_RESET# 连接至 MEC1723 RESET_IN#	**IN （默认）：**连接 OUT：断开

第 6 章 运行开箱即用 （Out-of-Box， OOB）演示代码

CEC1736 开发板可演示以下 CEC1736 关键功能，旨在提供良好的开箱即用体验。

为此，此开发板随附已安装预定义 OTP 设置和 Soteria-G3 固件 SPI 映像的预编程 CEC1736。

目前提供的演示如下。更多演示正在创建中，将通过固件升级提供。

1. 映像验证演示
   - **AP 映像**

     MEC1723 向 CEC1736 发送验证 AP 映像的 I2C 命令，以显示当前状态，并输出至 UART 日志；然后配置为无效映像位置，并复位 CEC1736。验证将会失败，随后会执行黄金映像恢复操作。所有步骤和状态都将输出至 UART 日志。

   - Soteria-G3 映像

     MEC1723 向 CEC1736 发送 I2C 命令，以获取 Soteria-G3 映像验证状态，并输出至 UART 日志；然后将 CEC1736 标记 0 设置配置为无效映像位置，并复位 CEC1736，标记 0 中的无效映像验证将会失败，随后会加载 Soteria-G3 固件标记 1 中的良好映像。所有步骤和状态都将输出至 UART 日志。

2. SPI MON （监视）滤波演示
   - 操作码违例

     在 AP_CFG 引导后的操作码设置中配置读取和写入权限，但禁止擦除权限；然后，MEC1723（AP 主机）会对 AP0 SPI 闪存中的任意存储单元执行擦除操作，CEC1736 将检测 OPCODE 违例，并复位 MEC1723，所有步骤和状态都将输出至 UART 日志。

   - 运行时违例

     配置为禁止对在 AP_CFG 设置中的受保护存储区执行读操作；然后， MEC1723（AP 主机）会对 AP0 SPI 闪存上的受保护区域执行读操作。CEC1736 将检测该读干预运行时违例，并复位 MEC1723。所有步骤和状态都将输出至 UART 日志。

   - 运行时验证

     配置为在 AP_CFG 引导前操作码设置中允许读取、写入和擦除权限；然后，MEC1723（AP 主机）会依次读取 AP0 SPI 闪存中的字节匹配映像和非关键型散列匹配映像，读回映像验证状态为 “Good to Go”，然后破坏非关键型散列匹配映像，并再次读取映像验证状态。此时，它应指示 “FW is bad”。所有步骤和状态都将输出至 UART 日志。

© 2023 Microchip Technology Inc. 及其子公司

- 证明 （SPDM）演示

  MEC1723 会向 CEC1736 发送从内部闪存提取整个认证链的一系列 I2C 命令，然后进行校验，向 CEC1736 发送取回 NONCE 数据及其签名的“质询验证”命令，并验证 NONCE 数据的签名。所有步骤、状态和数据都将输出至 UART 日志。

3. 撤销演示

- 密钥撤回

  此演示将展示密钥撤回后， EMC1723 加载映像失败的情形；所有步骤和状态都将输出至 UART 日志。

- 回滚保护

  此演示将展示更新 FW 版本后， EMC1723 加载映像失败的情形；所有步骤和状态都将输出至 UART 日志。

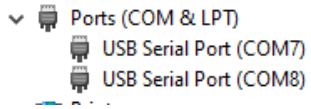
注： 根据计划，将随附演示 #1，并将其编程到开发板中。演示 #2、#3、#4 及未来其他开发演示在创建完成后将会包含在通过 SDE 发布的单独 OOB 主机代码示例包中。

注： 详细信息请参见 OOB 演示代码发布包应用笔记。

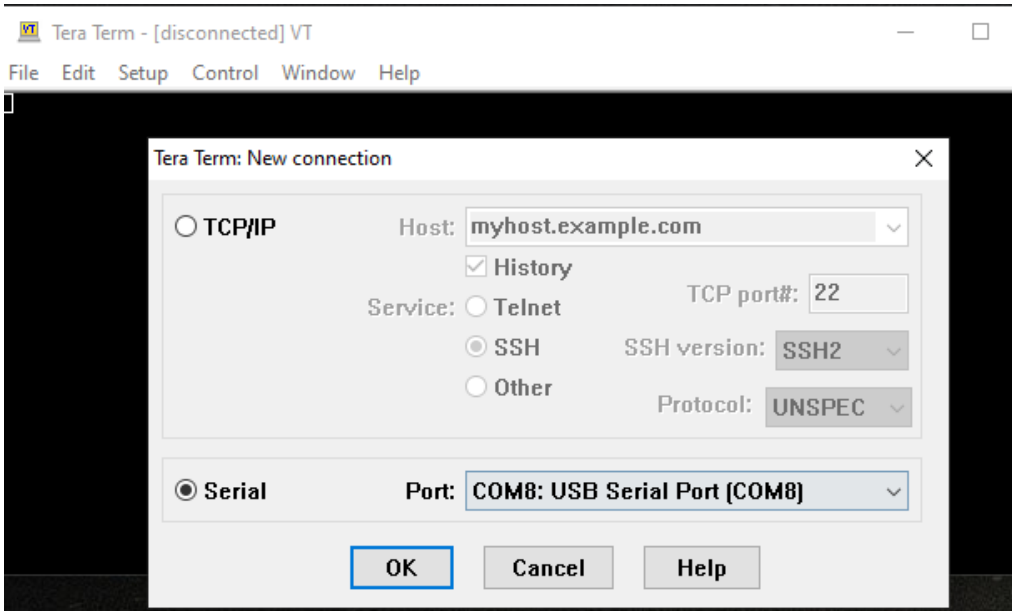
注： 如欲获取任何更新信息，请联系您的 Microchip 代表。

以下示例按步骤说明开发板初次上电后的 CEC1736 串行 UART 日志：

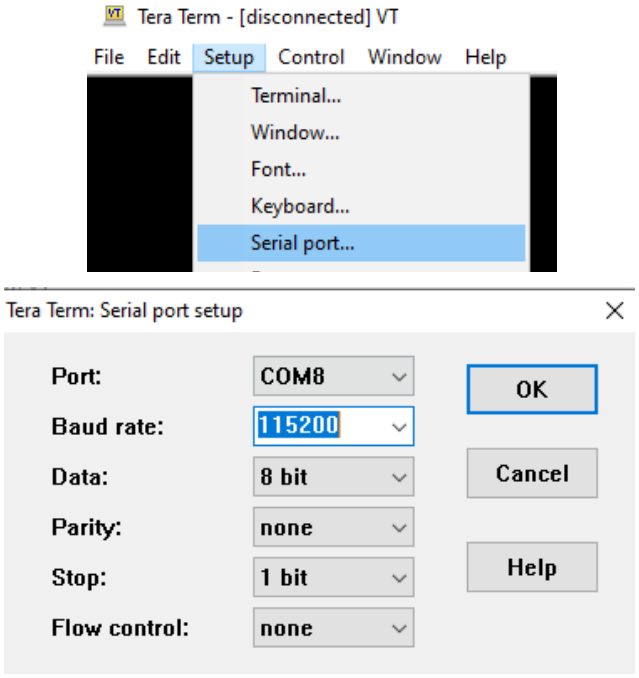
1. 用 Micro USB 线连接 PC USB 端口和 CEC1736 开发板上的 P2 Micro USB 端口（用于 CEC1736），如第 4 章中所示。
2. 用 Micro USB 线连接 PC USB 端口和 CEC1736 开发板上的 P3 Micro USB 端口（用于 MEC1723），如第 4 章中所示。
3. 所连接的 PC Windows 设备管理器应检测到 2 个 USB 串口 （例如：COM7 和 COM8，如下所示）。



4. 打开 “Tera Term” 终端程序，然后选择新的 “Serial”（串行） COM 端口 （例如：COM8）。



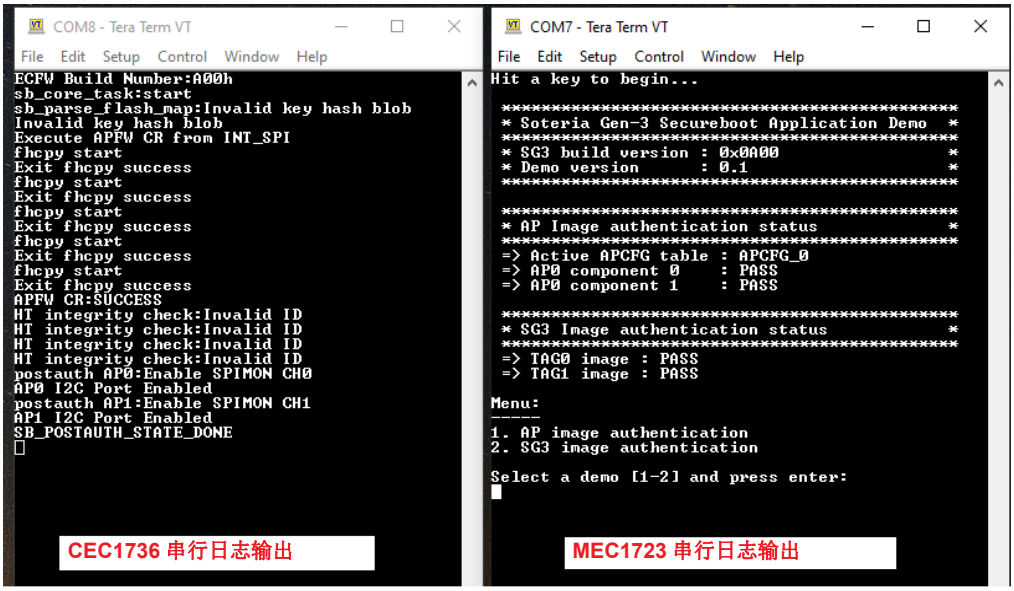
5. 转至 “Setup”（设置）-> “Serial port”（串口），然后选择 “115200-8-n-1-n”。



6. 打开另一个 Tera Term，使用相同的 115200-8-n-1-n 设置来设置 COM7。
7. 由于开发板上电时已执行 CEC1736 Soteria-G3 固件，所以在上述设置之后，初始 UART 日志就会丢失。我们可以使用 S1 开关来复位 CEC1736，然后就会出现相应的 UART 日志，如下图所示。

注： 下述日志仅为示例，实际结果将取决于测试环境以及所使用的 Soteria-G3 固件发行版本。

© 2023 Microchip Technology Inc. 及其子公司

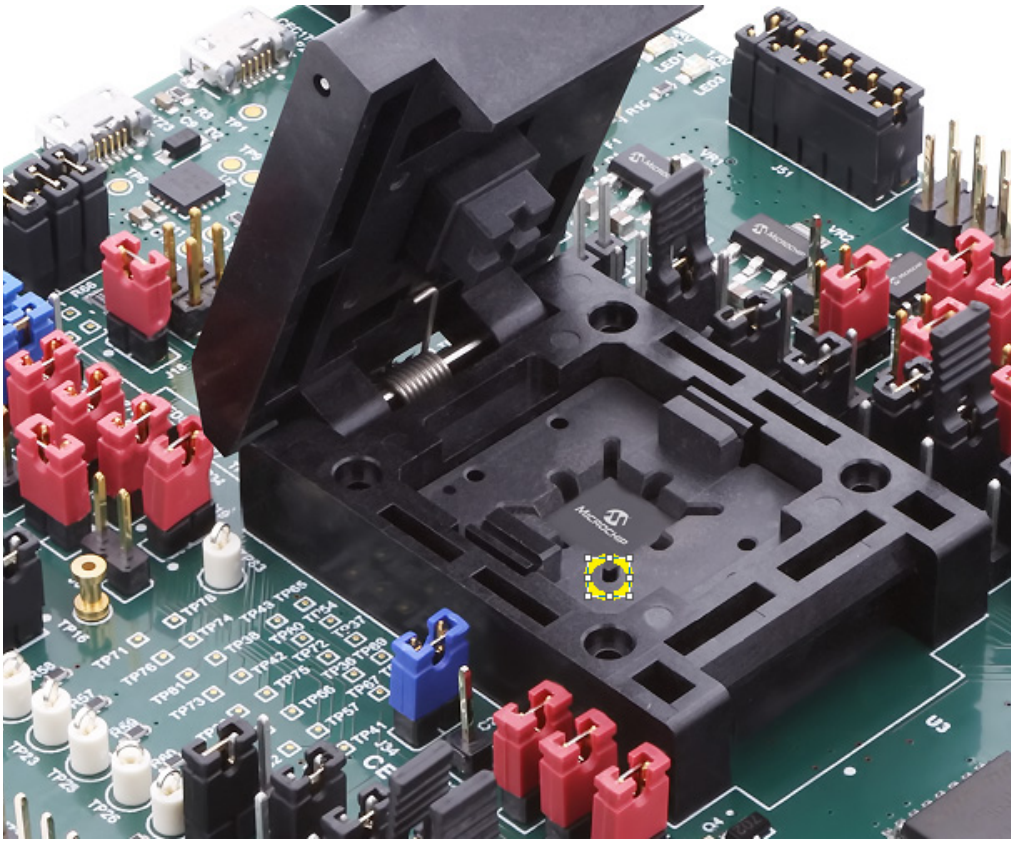

COM8 - Tera Term VT
File Edit Setup Control Window Help
ECFW Build Number:A00h
sb_core_task:start
sb_parse_flash_map:Invalid key hash blob
Invalid key hash blob
Execute APFW CR from INT_SPI
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
APFW CR:SUCCESS
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
postauth AP0:Enable SPIMON CH0
AP0 I2C Port Enabled
postauth AP1:Enable SPIMON CH1
AP1 I2C Port Enabled
SB_POSTAUTH_STATE_DONE
CEC1736 串行日志输出
COM7 - Tera Term VT
File Edit Setup Control Window Help
Hit a key to begin...
* Soteria Gen-3 Secureboot Application Demo *
* SG3 build version : 0x0A00 *
* Demo version : 0.1 *
* AP Image authentication status *
=> Active APCFG table : APCFG_0
=> AP0 component 0 : PASS
=> AP0 component 1 : PASS
* SG3 Image authentication status *
=> TAG0 image : PASS
=> TAG1 image : PASS
Menu:
1. AP image authentication
2. SG3 image authentication
Select a demo [1-2] and press enter:
MEC1723 串行日志输出

第 7 章 为开发做好准备

在演示和评估阶段后，用户可使用此开发板来定制安全特性。

首先，用户需要创建自己的 QTP 包，以申请 CEC1736-S0-I/2ZW （84 引脚封装）器件的生产版本订单。

然后，用户可以将新的定制 CEC1736 插入开发板插座。请确保器件上的小黑点指向插座引脚 1，如下图中的黄色标记所示。



- 其余开发步骤和操作详情，请参见Microchip可信平台设计套件（Trust Platform Design Suite， TPDS）（支持 CEC1736 的版本）。
- 有关使用工具配置 CEC1736 的详细信息，请参见 “可信平台设计套件快速入门指南”。
- 有关使用工具开发和定制 CEC1736 外设（如 UART、SPI、LED 和 PWM 等）的详细信息，请参见 “MPLAB Harmony v3 用户指南”。
- 如需获取可信平台设计套件（TPDS）、MPLAB Harmony v3 和相关用户指南，请联系您当地的 Microchip 代表。需要签署 “保密协议”（NDA）。

© 2023 Microchip Technology Inc. 及其子公司

7.1 使用用户的系统评估 CEC1736

用户可考虑将 CEC1736 开发板连接至系统，以便进一步评估和进行产品开发。

CEC1736 开发板设计了禁用 MEC1723 的方法，具体操作如下：

- 移除 J65，以便断开 CEC1736 AP0_RESET# 引脚与 MEC1723 RESET_IN# 引脚的连接
- 在 J43 和 J44 之间连接跳线，使 MEC1723 保持复位状态，且所有连接的引脚都处于输入模式和三态。
- 将 P4 （BMC 主机连接器）连接至平台 AP0 接口
  - CEC1736 QSPI0_IN 总线连接至 AP0 QMSPI 总线
  - CEC1736 AP0_RESET# 引脚连接至 AP0 复位引脚
  - CEC1736 I2C 通道连接至 AP0 I2C 通道
  - 设计中需要的其他可选功能信号
- 如果使用了双通道，则将 P5 （CPU 主机连接器）连接至平台 AP1 接口
  - CEC1736 QSPI1_IN 总线连接至 AP1 QMSPI 总线
  - CEC1736 AP1_RESET# 引脚连接至 AP1 复位引脚
  - 设计中需要的其他可选功能信号

全球销售及服务网点

美洲

公司总部 Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277
技术支持：
http://www.microchip.com/support
网址：www.microchip.com

亚特兰大 Atlanta
Duluth, GA
Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾 Philippines - Manila
Tel: 63-2-634-9065

新加坡 Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利 Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4485-5910
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-72400

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Ra'anana
Tel: 972-9-744-7705

意大利 Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利 Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7288-4388

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙 Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820

© 2023 Microchip Technology Inc. 及其子公司