CEC173x Trust Shield ファミリ

概要

CEC173x Trust Shield ファミリは、データセンター、通信、ネットワーク、組み込みコンピューティング、産業用市場において最終製品のサイバー レジリエンスを実現するリアルタイム プラットフォーム ルートオブ トラスト ソリューションです。

使いやすい Soteria-G3 ファームウェア、TPDS (Trust Platform Design Suite)、MPLAB® Harmony を含む CEC173x Trust Shield ファミリは、柔軟に設定可能なマイクロコントローラ ベースのルートオブ トラスト ソリューションの迅速な開発を可能にし、設計を短期間で市場に投入できるようにします。

CEC173x Trust Shield ファミリは、NIST 800-193 PFR、Open Compute Project® のセキュリティ ガイドライン、TCG DICE、HCD-CPP、FIPS 140-2、CAVP、サードパーティによる侵入テストに適合しています。

ターゲット アプリケーション

CEC173x Trust Shield ファミリは、外部 SPI フラッシュからブートする任意のプロセッサまたは GPU(グラフィック処理ユニット) に最適です。

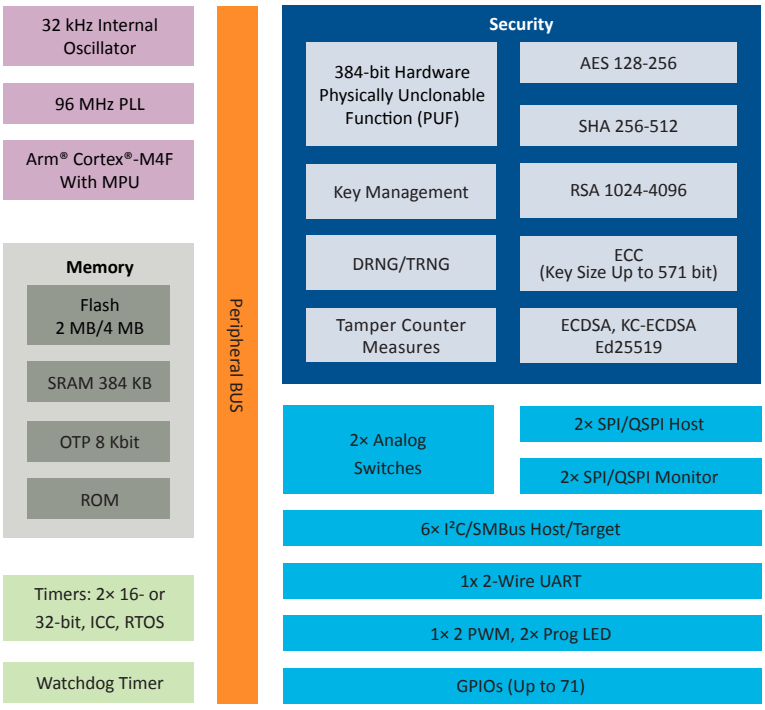
ターゲット市場

- データセンター
- 通信/5G
- 組み込みコンピューティング
- ネットワーク/IoT (Internet of Things)
- 産業用

主なセキュリティ機能

- ハードウェア CNSA セキュアブート/セキュアな更新
- リアルタイムの SPI バス監視、I²C/SMBus フィルタ処理
- 384 ビットの Physically Unclonable Function (PUF)
- デバイスとファームウェアの認証
- サイドチャンネル攻撃対策
- ライフサイクル管理と所有権移転
- 高度なハードウェア暗号スイート

CEC173× Family

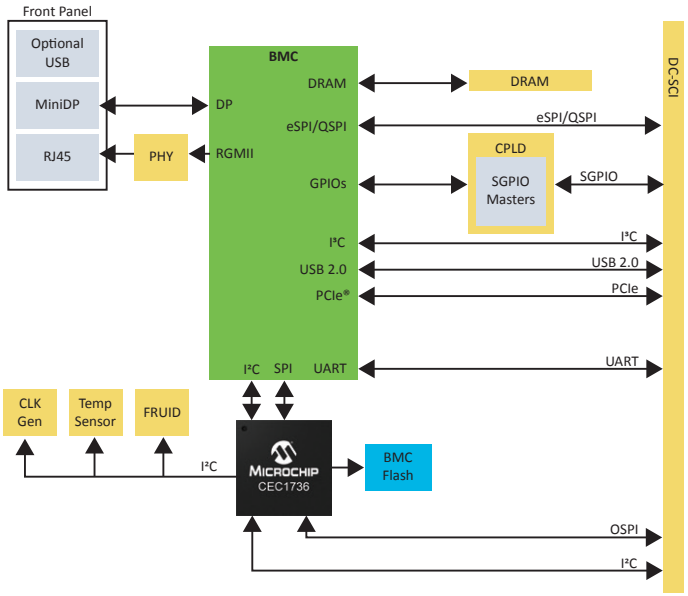


製品の特長

- 96 MHz Arm® Cortex®-M4F MPU(マイクロプロセッサ) コア
- 2 MB/4 MB フラッシュ
- 384 KB RAM
- 書き換え不可のブート ROM
- アンチヒューズ技術を備えた 8 Kb OTP
- 2× SPI/QSPI コントローラ
- 6× I2C/SMBus ホストおよびターゲット
- 1× UART、2× PWM、2× Prog LED
- 最大 71 個の GPIO
- 64 ピンおよび 84 ピンの WFBGA

OCP DC-SCM のブロック図の例

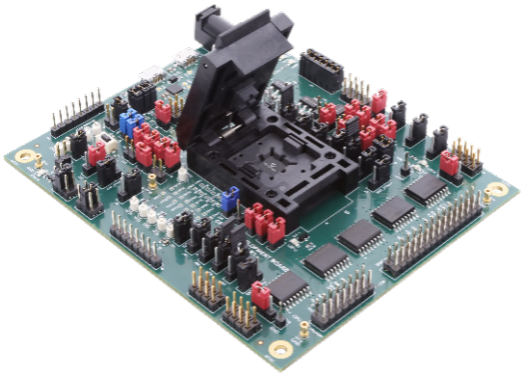
以下の図は、データセンター セキュア制御モジュールの例において、CEC173x ファミリが次世代のリアルタイム プラットフォーム ルートオブ トラストをもたらす方法を示しています。



開発を始める

CEC1736 の開発は以下の使いやすいツールでサポートされています。

CEC1736 開発ボード - EV19K07A



https://www.microchip.com/en-us/Development-Tool/EV19k07a---CEC1736-Development-Board

- TPDS (Trust Platform Design Suite)
- Soteria-G3 ファームウェア
- MPLAB Harmony v3

ご購入先と詳細情報

以下の CEC173x の製品ページにシリコンの詳細情報を記載しています。CEC1736 と CEC1734 は、64 ピンおよび 84 ピン WFBGA パッケージで提供しています。

https://www.microchip.com/en-us/product/CEC1736

https://www.microchip.com/en-us/product/CEC1734