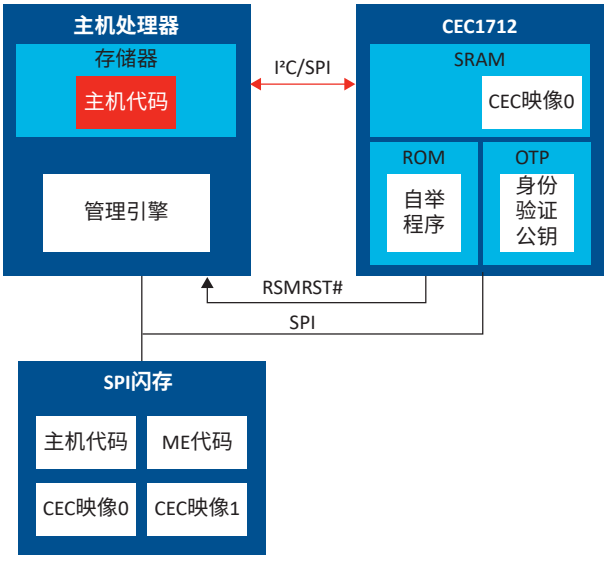
信赖您的固件

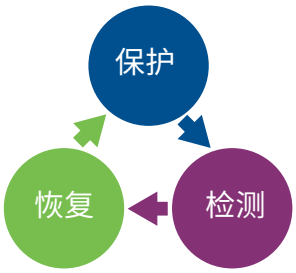
利用Soteria保障平台安全

快速且安全

Soteria是一个固件验证过程，专为CEC17xx系列加密控制器而打造。它的设计目的是在每次设备上电时协助实施安全引导过程。从SPI闪存加载的任何映像在到达主机处理器之前都要经过验证。这个过程将建立一个“信任根”，确保在设备上运行的每一行代码都是可信且真实的。在签署软件许可协议后，就可以获得Soteria。



为何必不可少？



Soteria + CEC 1712符合NIST（美国国家标准与技术研究所）SP 800-193准则中的规定。

该系统的保护机制是对主机处理器上运行的所有代码进行签名和身份验证，然后借助SHA-384加密算法检测未经授权的访问或损坏的数据。

最后，系统利用SPI闪存中的冗余映像来恢复任何已损坏或受损的代码。

工作原理

在引导过程开始时，嵌入式控制器将主机处理器保持在复位状态，从一开始就防止其运行。这样就能确保在身份验证完成之前不会在处理器上运行任何代码。SPI闪存将保存两个待验证的冗余映像。第一个映像（映像0）将加载到CEC1712的SRAM中，并使用存储在OTP中的公钥对其进行验证。如果存在损坏的数据，则将第二个映像（映像1）加载到SRAM中，并验证其数字签名。只有当其中一个映像通过身份验证后，才会释放复位线，并允许主机处理器运行代码。

要浏览支持Microchip Soteria的控制器，请访问
https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mcus/cec-32-bit-mcus

引导时间一览

下表描述了安全引导过程中每个步骤所需的时间。虽然加载映像的时间将随映像的大小而变化，但引导过程仍然非常快。在本示例中，读取、加载和解密256 KB的映像需要191.3 ms。即便是10 MB大小的映像，验证时间也不到一秒，因此增加的引导过程时间可以忽略不计。

读取报头	
读取报头并生成SHA-384哈希值	0.5 ms
验证报头签名（ECDSA ECC-P384），运行频率为48 MHz	66.0 ms
加载映像	
从SPI加载，大小为256 KB	12.3 ms
计算SHA-384哈希值	6.3 ms
验证映像签名（ECDSA ECC-P384）	66.2 ms
解密映像	
密钥交换	34.0 ms
AES-256解密	8.9 ms
总时间	**191.3 ms**

加密套件

支持Soteria的CEC1712控制器可使用多种不同的加密模式和哈希方法。此外还支持真随机数发生器和4 Kb用户可编程OTP等功能。请注意，特定器件可对OTP进行一次性编程。

CEC1712		
对称加密	**模式**	AES-128、AES-192和AES-256 ECB、CBC、OFB、CFB和CTR
哈希算法		SHA-1、SHA-256、SHA-384和SHA-512
公钥引擎	**RSA**	RSA-1024至RSA-4096
		GF（p）中192到521位
	ECC	GF（2 m）中160到571位
		Curve25519
	DSA	ECDSA、EC-KCDSA和Ed25519
		模块化算术原语
		米勒-拉宾素性测试
		真RNG
		1 Kb FIFO用于预计算
用户可编程OTP		4 Kb
现场可编程		是

要充分利用CEC1712控制器提供的大量安全功能，
请访问https://www.microchip.com/wwwproducts/en/CEC1712。