*Application Note*

# *MSPM0 MCU 中的网络安全机制*


**摘要**

MSPM0Gxx 和 MSPM0Lxx 微控制器提供了多种信息安全机制，旨在帮助开发人员实施所需的安全措施来保护代码、数据和密钥等资产。本文档介绍了这些器件中提供的安全机制及其功能和限制、运行方式，以及如何针对基本用例对它们进行配置。


## 内容



## 商标

# 1 引言

随着工业、汽车和个人电子产品应用的互联程度越来越高，并且攻击者可以使用的工具不断增加，嵌入式应用中的器件安全变得越来越重要。TI 的 MSPM0 微控制器包含各种硬件和软件安全支持技术，供工程师在开发注重安全性的应用时使用。

## 1.1 网络安全目标

一般而言，在嵌入式应用中，网络安全的主要目标是在如下方面保护关键资产：

- 机密性（对机密数据保密）
- 完整性（保护数据不被修改）
- 真实性（确保各方都是真实的）
- 可用性（确保数据和/或功能在需要时可用）
- 不可否认性（数据的来源和/或身份对其他各方都是可证明的）

这些关键目标通常适用于可能处于以下状态的资产：

- 静态（微控制器上未在使用的代码、数据或密钥）
- 使用中（微控制器上正在应用中使用的代码、数据或密钥）
- 传输中（微控制器上正在 MCU 和其他实体之间移动的代码、数据或密钥）

## 1.2 平台信息安全机制

表 1-1 列出了 MSPM0 器件中包含的信息安全机制。有关更广泛 TI 产品中信息安全机制的完整列表，请访问 TI 安全性门户。

**表 1-1. MSPM0 MCU 平台信息安全机制**

| 信息安全机制 | 器件特性 | MSPM0L | MSPM0G |
|---|---|---|---|
| 调试安全性 | 密码验证的调试访问 | 全部 | 全部 |
| | 密码验证的引导加载程序访问 | 全部 | 全部 |
| | 密码验证的主闪存批量擦除 | 全部 | 全部 |
| | 密码验证的完全恢复出厂设置 | 全部 | 全部 |
| | TI 失效分析 (FA) 启用/禁用 | 全部 | 全部 |
| | 串行线调试 (SWD) 接口的完全硬件禁用 | 全部 | 全部 |
| | 可永久锁定的器件配置数据 | 全部 | 全部 |
| | 防错器件配置数据 | 全部 | 全部 |
| | 密码存储器仅包含哈希值 (SHA2-256) | 未来 | 未来 |
| 安全启动 | 可永久锁定的主闪存（静态写保护） | 全部 | 全部 |
| | CRC-32 验证的主闪存区域 | 全部 | 全部 |
| | SHA2-256 验证的主闪存区域 | 未来 | 未来 |
| | 引导时主闪存应用程序的单点入口 | 全部 | 全部 |
| | 固件映像身份验证例程（非对称或对称） | 全部 | 全部 |
| | 用于密钥撤销和回滚保护的可锁定闪存 | 未来 | 未来 |
| | W^X（写入或执行）SRAM 边界 | 全部 | 全部 |
| 安全存储 | 静态闪存读取/执行 (RX) 防火墙 | 未来 | 未来 |
| | IP 保护（仅执行）防火墙 | 未来 | 未来 |
| | 主闪存存储体上的 W^X（写入或执行）强制执行 | 未来 | 未来 |
| | AES 易失性密钥存储区（最多四个 128 位密钥加上一个会话密钥） | 未来 | 未来 |

表 1-1. MSPM0 MCU 平台信息安全机制 (continued)

| 信息安全机制 | 器件特性 | MSPM0L | MSPM0G |
|---|---|---|---|
| **加密加速** | 硬件 AES 加速器（128 位/256 位） | 未来 | 可选 |
| | 硬件 TRNG | 未来 | 可选 |
| **器件身份** | 唯一器件标识符（96 位） | 全部 | 全部 |
| **物理安全** | 引导配置例程故障注入攻击对策 | 未来 | 未来 |

# 2 器件安全模型

MSPM0 安全模型的基础是在启动时强制执行一组用户指定的安全策略。本节概述了器件启动过程和用户指定的策略，用户可以设置这些策略来支持各种应用用例。

## 2.1 启动时的初始条件

在冷上电 (POR) 期间，器件会复位至一个安全状态。数字 IO 引脚采用高阻抗配置，所有外设功能均断开连接，NRST 引脚处于 NRST 模式，并且串行线调试 (SWD) 接口引脚处于 SWD 模式。在欠压复位释放后，串行线调试端口 (SW-DP) 最初会启用，以允许一个调试探针建立到调试子系统的初始连接。

在启动过程的这一阶段，调试探针可访问的唯一调试访问端口 (DAP) 是配置访问点 (CFG-AP) 和安全访问点 (SEC-AP)。连接的调试探针可以使用 CFG-AP 来读取通用器件信息（例如器件的通用器件型号）。SEC-AP 可用于尝试向引导配置例程传递命令消息。对器件的应用调试访问（通过 AHB-AP、ET-AP 和 PWR-AP DAP）仍会被硬件防火墙阻止。因此，器件硬件不允许在器件加电期间对处理器、EnergyTrace 状态或电源配置进行任何调试访问。

在欠压复位 (BOR) 之后，始终会生成引导复位 (BOOTRST)，从而开始执行引导配置例程。

## 2.2 引导配置例程 (BCR)

MSPM0 器件在只读存储器 (ROM) 中包含一个不可变的信任根引导配置例程。引导配置例程 (BCR) 始终是紧跟器件的 BOOTRST 之后在 Cortex-M0+ 处理器上运行的第一个代码。BCR 还会在软件调用引导加载程序 (BSL) 时运行，因为这是授权 BSL 条目所需的。BCR 的核心职责是：

1. 将器件正常运行所需的 TI 工厂数据从 FACTORY 闪存区域加载到逻辑中，并通过 CRC-32 验证工厂数据（包括器件修整数据）的完整性
2. 将用户指定的器件配置（包括安全策略）从 NONMAIN 闪存区域加载到逻辑中，并通过 CRC-32 验证用户配置数据的完整性
3. 检查是否通过串行线调试 (SWD) 接口发送任何引导命令，对这些命令进行授权（如果适用）并进行处理（如经授权）
4. 如果启用了 BSL，检查是否存在引导加载程序 (BSL) 调用条件，如果发生有效调用，则启动 BSL
5. 在启动用户应用程序之前，检查 MAIN 闪存区域中包含用户应用程序代码的闪存部分的完整性
6. 将任何引导错误记录到 CFG-AP
7. 通过从 MAIN 闪存中的地址 0x0000.0000 获取堆栈指针并从地址 0x0000.0004 获取复位向量，触发硬件来启动应用程序

在 BCR 执行期间，AHB-AP、ET-AP 和 PWR-AP DAP 仍然无法通过 SWD 接口访问。如果用户指定的安全策略允许对器件进行调试访问，则当硬件启动用户应用程序或引导加载程序时，这些 DAP 将变为可用。

## 2.3 引导加载程序 (BSL)

MSPM0 器件还可能在只读存储器 (ROM) 中包含一个不可变的引导加载程序 (BSL)。与串行线调试 (SWD) 接口相反，BSL 提供了一种通过标准串行接口（UART 或 I2C）对器件存储器内容进行编程和验证的方法。

BSL 只能由 BCR 启动。BCR 会检查是否存在有效的 BSL 调用条件（软件调用、IO 引脚调用、空白器件调用），并验证在启动 BSL 之前是否启用了 BSL 以供使用。当 BSL 退出时，BCR 会再次运行以加载当前器件安全策略并启动用户应用程序。

BSL 始终受用户指定的 256 位密码保护，在启动 BSL 会话时，该密码必须通过 UART 或 I2C 接口传递给 BSL。如果不使用 BSL，则可以将其禁用（请参阅 BSL 启用/禁用策略）。

## 2.4 启动流程

图 2-1 显示了 MSPM0 器件的启动流程概要。

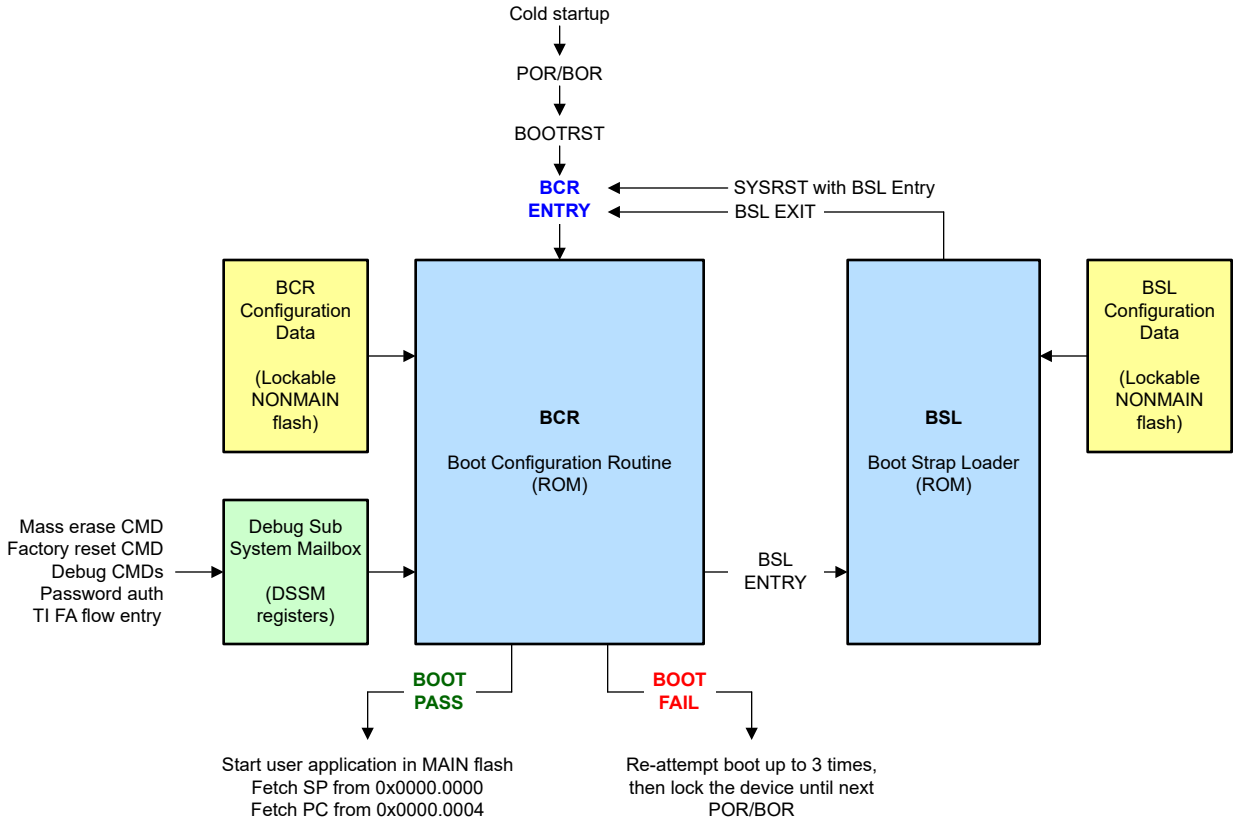


**图 2-1. 启动流程概要**

请注意，BCR 和 BSL 都在可锁定的 NONMAIN 闪存区域中包含用户指定的配置数据结构。节 2.5 中介绍了通过这些数据结构指定的这些安全策略。

## 2.5 用户指定的安全策略

MSPM0 器件包含一个专用的闪存区域，用于存储用户指定的安全和器件配置策略。该区域称为 NONMAIN 闪存区域。引导配置例程 (BCR) 和引导加载程序 (BSL) 会引用 NONMAIN 闪存区域中存储的用户指定数据以配置器件的运行。

在生产过程中，用户必须按照所需的策略配置器件的 NONMAIN 闪存区域。本节将介绍用户可通过 NONMAIN 配置存储器配置的安全策略。

NONMAIN 闪存区域分为两个不同的数据结构：

- BCR 配置（如 节 2.5.1 所述），用于设置引导配置安全策略
- BSL 配置（如 节 2.5.2 所述），用于设置引导加载程序安全策略

这两个数据结构都由自己的 32 位 CRC 摘要支持，这些摘要用作配置数据防错方案的一部分。

**备注**

BCR 和 BSL 配置结构中包含了本文档中所示之外的其他参数；本文档重点介绍了与安全性相关的参数。有关 NONMAIN 闪存区域中 BCR 和 BSL 配置结构的完整说明，请参阅相应技术参考手册中架构一章的引导配置部分。

### 2.5.1 引导配置例程 (BCR) 安全策略

BCR 安全策略由 BCR 进行解释，并包括以下参数：

- 串行线调试相关策略，如节 2.5.1.1 所述
- 引导加载程序启用和禁用策略，如节 2.5.1.2 所述
- 闪存保护和完整性策略，如节 2.5.1.3 所述

#### 2.5.1.1 串行线调试相关策略

串行线调试相关策略配置可通过器件的物理调试接口 (SWD) 获得的功能。默认情况下，TI 的 MSPM0 器件处于不受限制的状态。该状态支持轻松地进行生产编程、评估和开发。但是，不建议在大规模生产中使用这种不受限制的状态，因为它会留下很大的攻击面。为了在保持配置过程简单的同时满足各种需求，MSPM0 器件支持三个通用安全级别：无限制（级别 0）、自定义限制（级别 1）和完全限制（级别 2）。表 2-1 显示了三种通用安全级别，从限制性最低到限制性最高。

SWD 接口有 4 种主要用途需要考虑保护：

- 应用调试访问，其中包括：
  - 通过 AHB-AP 对处理器、存储器映射和外设进行完全访问
  - 通过 ET-AP 访问器件 EnergyTrace+ 状态信息
  - 通过 PWR-AP 访问器件电源状态控制以进行调试
- 批量擦除访问，其中包括：
  - 能够通过 SWD 发送一条命令来擦除 MAIN 内存区域，同时保持 NONMAIN 器件配置存储器不变
- 恢复出厂设置访问，其中包括：
  - 能够通过 SWD 发送命令来擦除 MAIN 存储器区域并将 NONMAIN 器件配置存储器恢复到 TI 出厂默认设置（0 级）
- TI 失效分析访问，其中包括：
  - TI 能够通过 SWD 启动失效分析回流（请注意，在向 TI 提供 FA 访问权限之前，TI FA 流始终强制恢复出厂设置；这确保在失效分析流程启动时，TI 没有任何机制来读取存储在器件闪存中的专有客户信息）

**表 2-1. 通用安全级别**

| Level | 场景 | SW-DP 策略 | 应用调试策略 | 批量擦除策略 | 恢复出厂设置策略 | TI FA 策略 |
|---|---|---|---|---|---|---|
| **0** | 无限制 | EN | EN | EN | EN | EN |
| **1** | 自定义限制 | EN | EN、EN（具有密码）、DIS | EN、EN（具有密码）、DIS | EN、EN（具有密码）、DIS | EN、DIS |
| **2** | 完全限制 | DIS | 无关（禁用 SW-DP 时无法访问）(1) | | | |

(1)当 SW-DP 策略是**禁用 SW-DP** 时，从 SWD 接口的角度来看，批量擦除和恢复出厂设置策略是无关的。但是，如果启用了引导加载程序 (BSL)，则批量擦除和恢复出厂设置策略会影响通过 BSL 提供的功能。有关保护 BSL 的详细信息，请参阅 BSL 安全性部分。

##### 2.5.1.1.1 SWD 安全级别 0

SWD 安全级别 0 是限制性最低的 SWD 安全状态。这是 TI 新器件的默认状态，也是器件在成功恢复出厂设置后的状态。此状态下对应用调试访问、整体擦除、恢复出厂设置和失效分析没有限制。

**何时使用此状态**

级别 0 非常适合原型设计和开发，因为它允许对器件存储器进行编程以及对处理器和外设进行调试。

**何时不应使用此状态**

大规模生产中不应使用级别 0。攻击者可以完全自由地读取器件存储器的内容、操纵器件的执行，并或许能更改闪存的内容（取决于闪存写保护方案）。

##### 2.5.1.1.2 SWD 安全级别 1

SWD 安全级别 1 允许自定义安全配置。物理调试端口 (SW-DP) 保持启用状态，并且每个功能（应用调试、批量擦除命令、恢复出厂设置命令和 TI 失效分析）都可以单独启用、禁用或（在某些情况下）通过密码身份验证启用，从而提供相当大的灵活性来根据特定用例定制器件行为。

**何时使用此状态**

级别 1 非常适合受限的原型设计/开发场景以及大规模生产场景，在这些场景中，需要保留某些 SWD 功能（例如恢复出厂设置和 TI 失效分析），同时禁用其他功能（例如应用调试）。表 2-2 中给出了级别 1 自定义配置的常见示例。

表 2-2. 级别 1 配置示例

| 级别 1 场景 | 配置 | | | |
|---|---|---|---|---|
| | 应用调试 | 批量擦除 | 恢复出厂设置 | TI FA |
| 这种场景使用用户指定的密码限制了调试访问，但保留了恢复出厂设置和 TI 失效分析。此配置允许进行现场调试（使用密码），另外还允许通过恢复出厂设置来将器件恢复到默认的“级别 0”状态。 | EN（具有密码） | DIS | EN | EN |
| 此场景不允许进行调试。它允许恢复出厂设置，但只能通过用户指定的密码来使用。这提供了一种在现场访问器件的方法，方法是在密码已知时清除 MAIN 存储器内容并将器件恢复到“级别 0”状态。重要的是，即使恢复出厂设置密码被泄露，攻击者也无法读取 MAIN 闪存中的专有信息。 | DIS | DIS | EN（具有密码） | EN |
| 此场景不允许调试，也不允许 TI 失效分析。这可防止 TI 在器件上执行恢复出厂设置和进一步的 FA 活动，除非用户在将器件返回 TI 进行 FA 之前使用自己指定的密码执行恢复出厂设置。 | DIS | DIS | EN（具有密码） | DIS |

**备注**

对于大多数标准生产用例，建议使用级别 1 配置。对于不需要安全启动的应用，TI 建议在生产中使用级别 1，同时保持启用恢复出厂设置（使用密码）和 TI 失效分析。在此类配置中，用户（使用密码）或 TI（通过失效分析返回流程）或许能在器件配置后将器件恢复到限制性较低的状态。在需要最大安全启动保证的用例中，可以使用限制性较高的级别 1 或级别 2 进行生产，但需要权衡的是，器件在配置后可能无法恢复到限制性较低的状态。

**何时不应使用此状态**

如果需要对器件进行完全访问，则不应在原型设计期间使用级别 1；在这种情况下，应使用级别 0。

级别 1 也不应用于需要最高限制状态且不启用 SWD 功能的大规模生产场景；在这种情况下，应改为使用级别 2，因为它直接禁用整个 SWD 物理接口，并更大限度地减少误配置的可能性。

**备注**

如果器件配置为禁用应用调试和恢复出厂设置，则用户要恢复对器件的调试访问，唯一方法是用户应用代码提供了一种机制，可将 NONMAIN 配置更改为限制性较低的状态。如果 NONMAIN 通过静态写保护锁定，则状态不可逆，用户无法重新获得调试访问。

#### 2.5.1.1.3 SWD 安全级别 2

SWD 安全级别 2 会将器件配置为最高限制状态。物理调试端口 (SW-DP) 被完全禁用，所有 SWD 可访问的功能（应用调试、批量擦除、恢复出厂设置和 TI 失效分析）都不能通过 SWD 访问，无论它们的配置如何。

当选择级别 2（SW-DP 禁用）时，应用调试配置和 TI 失效分析配置字段都是无关字段，不会影响器件配置。

如果 BSL 被禁用，则批量擦除和恢复出厂设置配置字段也是无关字段。但是，如果 BSL 被启用，那么 BSL 仍然使用批量擦除和恢复出厂设置配置字段来授权来自 BSL 接口的批量擦除或恢复出厂设置命令。

**何时使用此状态**

级别 2 只应用于大规模生产，那时无需进一步访问任何 SWD 功能且器件需要达到最大安全状态。

**何时不应使用此状态**

以下情况下不应使用级别 2：

- 未来可能需要通过 SWD 进行应用调试和/或重新编程
- 用户希望 TI 能够对器件执行失效分析
- 用户希望能够通过 SWD 发送批量擦除或恢复出厂设置命令来从闪存中删除专有信息

**备注**

器件配置为级别 2（SW-DP 禁用）后，就**无法**通过 SWD 进一步访问器件。要将器件恢复到级别 0 或级别 1 状态并恢复 SWD 访问，唯一方法是启用 BSL 和恢复出厂设置（允许发送 BSL 恢复出厂设置命令），或者用户应用程序代码中包含一种机制，可将 NONMAIN 配置更改为限制性较低的状态。在任何一种情况下，如果 NONMAIN 通过静态写保护锁定，则级别 2 状态不可逆，法重新获得 SWD 访问。

#### *2.5.1.2 引导加载程序 (BSL) 启用/禁用策略*

与串行线调试接口相反，引导加载程序 (BSL) 提供了一种通过标准串行接口（UART 或 I2C）对器件存储器进行编程和验证的方法。BSL 具有自己的配置策略，但由 BCR 确定是否启用了 BSL 以进行调用，还是要禁用 BSL（不可调用）。

由于 BSL 提供了一个额外的攻击面，如果它未在应用程序中使用，则可以在用户指定的启动安全策略中禁用它。如果在应用程序中使用 BSL，则在 BSL 配置策略中管理 BSL 安全设置（包括 BSL 访问密码）。

#### *2.5.1.3 闪存保护和完整性相关策略*

闪存保护和完整性策略规定闪存的哪些扇区被锁定而无法修改，以及启动过程中在启动用户应用程序之前要检查哪些扇区的完整性。

##### 2.5.1.3.1 锁定应用 (MAIN) 闪存

MSPM0 MCU 实现了一个静态写保护方案，以将 MAIN 闪存区域中用户定义的扇区锁定，从而防止在运行时针对相应删除执行任何编程/擦除操作。所需的静态写保护方案配置为 NONMAIN 闪存区域中启动安全策略的一部分。

**用途**

静态写保护方案支持在闪存中存储一个用户定义的、具有以下特性的固定应用程序：

- 在编程结束并被锁定后，它就无法由应用程序代码或 ROM 引导加载程序进行修改
- 如果置于闪存的开头，这会保证它始终是 ROM 引导配置例程转换到执行用户应用程序时执行的第一个代码

MSPM0 静态写保护支持这两个特性，要实现安全启动映像管理器，必须满足这些特性。

**功能**

当引导配置例程将转换到执行 MAIN 闪存中的引导加载程序或用户应用程序代码时，在 NONMAIN 中配置为写入锁定的任何扇区都将在功能上不可更改。如果应用程序代码或引导加载程序尝试对受静态保护的扇区进行任何编程或擦除，都会导致硬件闪存操作错误，并且扇区不会被修改。

静态写保护可防止应用程序代码或引导加载程序进行任何修改，但通过 SWD 接口发送的批量擦除或恢复出厂设置命令将被接受。如果不需要这种行为，可以使用唯一的密码来保护批量擦除和/或恢复出厂设置 SWD 命令，也可以同时禁用这两个命令（请参阅 SWD 策略）。要完全消除任何修改受静态写保护的 MAIN 闪存扇区的方法，必须禁用批量擦除和恢复出厂设置命令（或 SW-DP），并且 NONMAIN 引导配置存储器也必须具有静态写保护，以防止应用程序代码通过修改 NONMAIN 区域内容来更改底层写保护方案。下一节会对此进行介绍。

##### 2.5.1.3.2 锁定配置 (NONMAIN) 闪存

MSPM0 MCU 实现了一个静态写保护机制，以在运行时锁定 NONMAIN 闪存区域，从而防止对该区域进行任何编程/擦除操作。写保护方案配置为 NONMAIN 闪存区域中启动安全策略的一部分。

**用途**

默认情况下，TI 的 NONMAIN 配置存储器（包含用户指定的启动安全策略和引导加载程序策略）不受写保护。这样一来，用户就可以在配置期间擦除 NONMAIN，并使用将用于大规模生产的用户指定策略重新编程。

在许多情况下，配置存储器最好在配置完毕后锁定。锁定配置存储器的好处是可以防止引导加载程序或应用程序代码本身对安全策略、引导加载程序策略和静态写保护策略进行任何未经授权的修改。在大多数应用中，大规模生产的器件无需修改配置存储器，即使在器件固件更新时也是如此。

**功能**

当配置为受保护时，整个 NONMAIN 区域都将被写锁定，并且在引导配置例程将执行传递给引导加载程序或 MAIN 闪存中的用户应用程序代码时在功能上不可更改。如果应用程序代码或引导加载程序尝试对 NONMAIN 进行任何编程或擦除，都会导致硬件闪存操作错误，并且扇区不会被修改。

静态写保护可防止应用程序代码或引导加载程序进行任何修改，但通过 SWD 接口发送的恢复出厂设置命令仍会被接受。如果不需要这种行为，可以使用唯一的密码来保护恢复出厂设置 SWD 命令，或者完全禁用该命令（请参阅 SWD 策略）。要完全消除任何修改 NONMAIN 配置存储器的方法，必须禁用恢复出厂设置命令和 TI FA（或 SW-DP）。

**备注**

当 NONMAIN 受到静态写保护并且禁用了恢复出厂设置命令和 TI FA（或 SW-DP）时，NONMAIN 相当于不可改变的只读存储器，并且不再能够通过任何方式更改器件配置。此外，如果任何 MAIN 存储器区域扇区配置了静态保护，则这些扇区也不能通过任何方式进行修改，可能会被视为不可更改。

#### 2.5.1.3.3 验证应用 (MAIN) 闪存的完整性

BCR 支持在将执行从 BCR（位于 ROM 中）转移到用户应用程序（位于 MAIN 闪存中）之前，检查 MAIN 闪存中用户指定地址范围的数据完整性。

**用途**

完整性检查可用作额外的步骤，以确保在引导 ROM（通常是安全启动映像管理器）之后首先运行的代码具有与预期值匹配的 CRC 摘要。此完整性检查降低了闪存中关键代码（可能负责验证其余用户应用软件映像）的任何意外损坏可能会造成安全漏洞的可能性。

**功能**

可以将起始地址、长度和 ISO-3309 CRC-32 摘要配置到 NONMAIN 配置存储器中。在引导过程中，BCR 将计算 MAIN 闪存中指定范围的 CRC-32 摘要，并根据配置的（预期）摘要来验证计算的摘要。如果这些值匹配，则会启动用户应用程序。如果这些值不匹配，则不会启动用户应用程序，结果会导致灾难性的引导错误。

### 2.5.2 引导加载程序 (BSL) 安全策略

BSL 安全策略在调用时由引导加载程序解释，并包含以下参数：

- BSL 访问密码，如 节 2.5.2.1 所述
- BSL 读取策略，如 节 2.5.2.2 所述
- BSL 安全警报策略（篡改检测），如 节 2.5.2.3 所述

#### *2.5.2.1 BSL 访问密码*

对 BSL 的访问始终受到用户指定的 256 位密码保护。无法选择禁用密码。必须在调用后向 BSL 提供密码，才能获得权限来访问大多数的 BSL 功能。如果未提供密码，则允许的 BSL 命令只有*获取身份*和*启动应用程序*。

如果向 BSL 提供了错误的密码，BSL 会暂停 2 秒，随后可以再尝试发送正确的密码。在三次密码尝试失败后，安全警报功能将被激活（请参阅 节 2.5.2.3）。

#### *2.5.2.2 BSL 读取策略*

BSL 可选择支持出于调试和/或诊断目的读取器件存储器（在通过正确密码匹配获得 BSL 访问权限后）。默认情况下，为了安全起见，会禁用此功能，以防止他人从器件中提取敏感代码和/或数据。禁用 BSL 读取策略后，可通过 BSL 接口向主机提供的唯一信息是最小段长度为 1KB 的存储器段 CRC32 摘要。如果需要直接读取器件存储器，可在 BSL 配置中启用该功能。

#### *2.5.2.3 BSL 安全警报策略*

BSL 提供了一种警报机制，用于在怀疑发生篡改时采取措施。具体而言，如果在一个 BSL 会话期间 3 次将错误的密码传递给 BSL，则会激活安全警报，并且 BSL 可能会根据指定的安全警报策略以三种不同的方式之一进行响应：

1. 发出恢复出厂设置命令（擦除 MAIN 闪存并重置 NONMAIN 闪存区域）。
2. 禁用 BSL（保持 MAIN 闪存不变，但重新配置 NONMAIN 以阻止访问 BSL）。
3. 忽略（不修改配置并允许继续密码尝试）。

**备注**

选项 1 和 2 要求 NONMAIN 闪存区域未受静态写保护（请参阅 节 2.5.1.3.2）。

选择选项 1 时，配置为受静态写保护的任何 MAIN 存储器区域（请参阅 节 2.5.1.3.1）将不会在恢复出厂设置期间被擦除。

### 2.5.3 配置数据错误抵抗

MSPM0 器件采用多种机制来降低因 NONMAIN 配置存储器中出现数据错误而导致安全性丧失的可能性。

#### *2.5.3.1 由 CRC 支持的配置数据*

NONMAIN 存储器中的 BCR 配置数据和 BSL 配置数据结构各自包含一个 CRC32 值，该值对应于相应结构的 CRC32 摘要。在器件启动过程中，BCR 将计算数据结构的 CRC 摘要，并将其与存储的 CRC 值进行比较，确认匹配后才会信任并使用这些结构中包含的数据。

**BCR 配置 CRC 故障处理**

如果 BCR 配置数据（包含 SWD 策略、BSL 启用/禁用策略以及闪存保护和完整性检查策略）在启动期间未能通过 CRC 检查，则会产生灾难性的启动错误并施加以下限制：

- 错误原因将作为引导诊断记录在 CFG-AP 中
- BSL 将不会被调用，即使它配置为要启用
- 用户应用程序不会启动
- 应用程序调试访问不会启用
- 如果启用了或使用密码启用了，则会执行待处理的 SWD 恢复出厂设置命令
- 如果已启用，则会执行待处理的 TI 失效分析流程条目
- 启动过程将最多重试 3 次
  - 如果第 2 次或第 3 次尝试通过，器件将正常启动
  - 如果第 3 次尝试仍未通过，则在下一次 BOR 或 POR 之前不会再进行启动尝试

此 CRC 校验的好处是，在启动过程中可以明确地检测配置数据中是否存在任何位翻转，例如静态写保护配置（安全启动的支柱）。故障处理程序会明确阻止 BSL 和用户应用程序运行，唯一受支持的选项（SWD 恢复出厂设置和 TI FA）受 16 位模式匹配字段保护。

**BSL 配置 CRC 故障处理**

如果 BSL 配置数据（包含 BSL 密码和 BSL 策略）在 BSL 调用期间未通过 CRC 检查，则会导致灾难性的启动错误并施加以下限制：

- 错误原因作为引导诊断记录在 CFG-AP 中
- BSL 不会被调用，即使它配置为要启用
- 用户应用程序不会启动
- 应用程序调试访问不会启用
- 启动过程最多会重试 3 次
  - 如果第 2 次或第 3 次尝试通过，器件将正常启动
  - 如果第 3 次尝试仍未通过，则在下一次 BOR 或 POR 之前不会再进行启动尝试

此 CRC 校验的好处是，在调用过程中可以明确地检测 BSL 配置数据中是否存在任何位翻转。故障处理程序会阻止 BSL 使用可能导致安全性丧失的无效数据启动。

**TI 出厂修整数据 CRC 故障处理**

除了用户指定的配置数据外，如果 TI 出厂修整在启动期间未能通过 CRC 检查，也会导致灾难性的启动错误并具有以下限制：

- 错误原因将作为引导诊断记录在 CFG-AP 中
- BSL 将不会被调用，即使它配置为要启用

- 用户应用程序不会启动
- 应用程序调试访问不会启用
- 如果已启用，则会执行待处理的 TI 失效分析流程条目
- 启动过程将最多重试 3 次
  - 如果第 2 次或第 3 次尝试通过，器件将正常启动
  - 如果第 3 次尝试仍未通过，则在下一次 BOR 或 POR 之前不会再进行启动尝试

#### *2.5.3.2 16 位关键字段模式匹配*

BCR 配置存储器中的关键策略（如 SWD 安全策略）会在 NONMAIN 存储器中实现为 16 位模式匹配字段，并具有以下特性：

- 需要精确的模式匹配，才能启用较低的安全状态
- 如果 16 位字段中的任何值与确切定义的模式不匹配，都会导致相应参数处于最高安全状态

这种行为可防止 single-bit 翻转导致器件进入比最初指定更低的安全状态。

# 3 安全启动

MSPM0 器件支持结合使用软硬件功能来对应用软件进行身份验证（安全启动）。虽然并非所有 MSPM0 器件都提供安全存储来保护对称密钥不受软件攻击，但这些器件都支持基于非对称和对称的身份验证方案。

MSPM0 架构包括实现安全启动所需的几个关键硬件特性：

- 可锁定闪存，用于存储固定的身份验证固件和身份验证密钥
- 引导期间的单点入口，可确保安全启动映像管理器始终是 BCR 之后运行的首个应用程序

MSPM0 软件开发套件 (SDK) 包括启动映像管理器 (BIM) 参考应用，用于在 MSPM0 MCU 上实现安全启动。此参考应用可轻松配置并预置到 MSPM0 器件中。

## 3.1 安全启动身份验证流程

需要完成以下配置步骤来准备器件，以便支持安全启动：

1. 必须配置启动映像管理器固件并将其编程到 MAIN 闪存中，其中复位矢量 0x0000.0004 指向启动映像管理器的开始
2. 启动映像管理器所需的任何身份验证密钥材料都必须编程到 MAIN 闪存中，与启动映像管理器相邻
3. 器件 NONMAIN 配置存储器必须使用以下特性进行编程：
   a. 包含启动映像管理器固件和密钥材料的 MAIN 闪存扇区必须配置为静态写保护以防止遭到修改。
   b. NONMAIN 闪存扇区必须配置为静态写保护以防止遭到修改。
   c. 建议使用密码保护或禁用批量擦除和恢复出厂设置命令（使用上述配置设置禁用恢复出厂设置将导致 NONMAIN 配置以及包含启动映像管理器和身份验证密钥的扇区永久锁定）。
   d. 建议启用 MAIN 闪存完整性检查，并将地址范围设置为包括启动映像管理器和身份验证密钥。

配置完成，并且将已签名的固件编程到器件中后，器件上电的安全启动流程如下所示：

1. 在上电期间，器件处于最大安全状态。如果器件配置有效，BCR 将检查器件配置存储器的完整性，并相应地加载用户指定的策略。
2. BCR 将计算与包含 BIM 和密钥材料的 MAIN 闪存相对应的 CRC 值。如果 CRC 校验通过，BCR 将转换到执行第一个用户代码（启动映像管理器）。
3. 启动映像管理器将计算剩余应用程序代码的摘要：
   a. 在非对称身份验证的情况下，应用程序代码的安全哈希 (SHA2-256) 摘要将在软件中计算
   b. 在对称身份验证的情况下，与应用程序代码相对应的 CMAC 消息身份验证代码将使用身份验证密钥计算
4. 启动映像管理器将根据提供的签名验证摘要：
   a. 在非对称身份验证的情况下，数字签名将在软件中使用椭圆曲线数字签名算法 (ECDSA) 进行解密，并将结果与计算的哈希值进行比较
   b. 在对称身份验证的情况下，计算出的 CMAC 将与数字签名中的 CMAC 进行比较
5. 如果应用程序代码摘要与签名相匹配，则会启动应用程序代码，否则将调用用户指定的故障处理程序。

## 3.2 非对称与对称安全启动

虽然 MSPM0 SDK 中提供的启动映像管理器支持非对称和对称安全启动，但对于给定的应用，应仔细权衡这两种实现方案。表 3-1 给出了这两种替代方案之间的权衡。

**表 3-1. 安全启动算法比较**

| 参数 | 非对称 (SHA2 + ECDSA) | 对称 (CMAC) |
|---|---|---|
| 身份验证用时 | 较长，因为使用软件哈希计算和公钥算法 | 较短，因为算法简单并且能够在可用时利用硬件 AES 加速 |
| 代码大小 | 较大，因为使用 SHA 和 ECDSA 算法 | 较小，尤其是在目标器件上提供 AES 加速时 |
| 密钥完整性 | 公钥必须配置到器件中，并且必须是不可更改的 | 共享密钥必须配置到器件中，并且必须是不可更改的 |
| 密钥机密性 | 公钥没有保密要求，也不需要保护公钥免受应用程序代码漏洞的影响 | 共享密钥必须保密，并且在不使用时应打包，并应使用静态读取防火墙（如果目标器件支持）进行保护，以保护共享密钥免受应用程序代码漏洞的影响 |

在大多数情况下，TI 建议采用非对称实现方案。如果代码大小受限且/或身份验证用时必须保持最短，则可以使用对称实现方案，但必须谨慎管理共享密钥。并非所有器件都提供了安全存储来保护共享对称密钥免受软件漏洞的影响。

# 4 加解密加速

某些 MSPM0 MCU 提供针对高级加密标准 (AES) 的硬件加速功能，以及用于为加密生成真正随机数 (TRNG) 的硬件。请参阅特定于器件的数据表以确定器件是否具有 AES 加速器或 TRNG，或参阅附录 A。

## 4.1 硬件 AES 加速

某些 MSPM0 器件包括针对高级加密标准 (AES) 的硬件加速。请参阅特定于器件的数据表，以确定特定器件是否包含 AES 硬件加速。

### 4.1.1 概述

AES 加速器模块根据高级加密标准 (AES) 在硬件中使用 128 位或 256 位密钥对 128 位数据块进行加密和解密。AES 是 FIPS PUB 197 中指定的对称密钥块加密算法。

AES 加速器的特性包括：

- AES 128 位块加密和解密
- DMA 触发器支持自动执行 NIST SP 800-38 中定义的 ECB、CBC、OFB 和 CFB 块加密模式
- 通过加密预先计算的（nonce || 计数器）块以及使用生成的密钥流加速纯文本异或，支持对 CTR 加密模式进行加速
- 支持对 CBC-MAC 标签计算（具有零初始化矢量的 CBC DMA 模式）进行加速
- 动态密钥扩展进行加密和解密
- 用于解密的离线密钥生成
- 用于存储所有密钥长度的初始密钥的影子寄存器
- 8 位字节或 32 位字访问，以提供关键数据、输入数据和输出数据
- AES 就绪中断
- 在运行和睡眠模式下受支持（请参阅器件技术参考手册的*工作模式*部分）

AES 加速器硬件由 128 位状态存储器和相关的输入/输出寄存器、AES 加密/解密内核和控制逻辑、256 位 AES 密钥存储器和相关的输入寄存器组成。图 4-1 中显示了 AES 硬件。

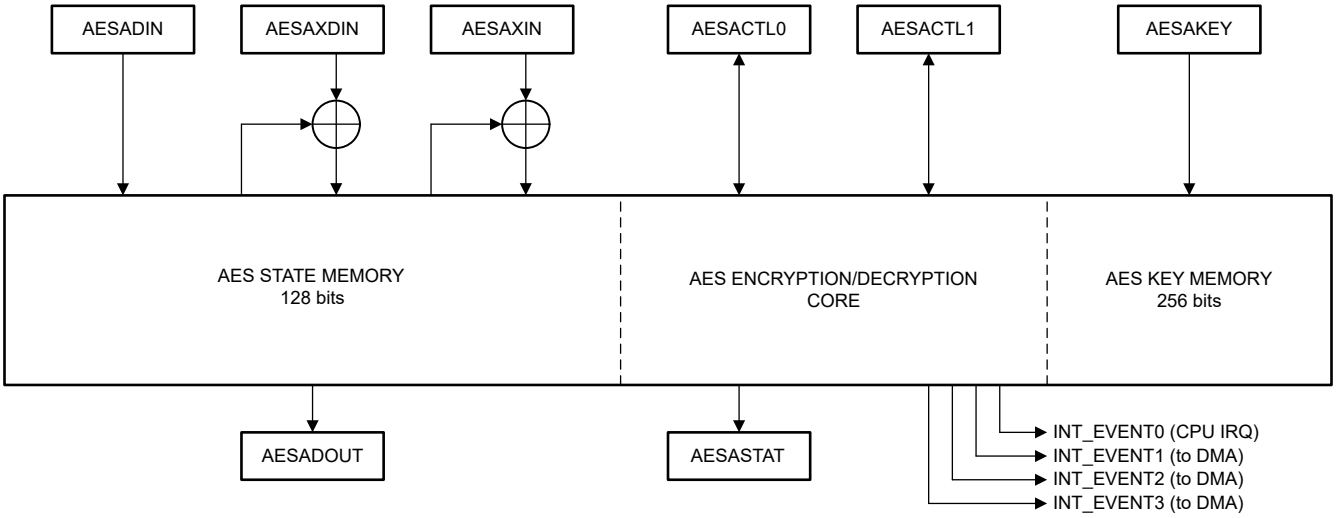


**图 4-1. AES 加速器框图**

### 4.1.2 AES 性能

AES 加速器可对 128 位块进行快速加密和解密。表 4-1 中以块加密和块解密（使用预先生成的解密密钥）的周期和执行时间形式给出了 AES 加速器性能。

表 4-1. AES 硬件加速器关键性能指标

| AES 密钥长度 | 加密 (OPx==0x0) | | | 解密 (OPx==0x3) | | |
|---|---|---|---|---|---|---|
| | 周期数 | 时间 (32MHz) | 时间 (80MHz) | 周期数 | 时间 (32MHz) | 时间 (80MHz) |
| 128 位 | 168 | 5.25 µs | 2.10 µs | 168 | 5.25 µs | 2.10 µs |
| 256 位 | 234 | 7.31 µs | 2.93 µs | 234 | 7.31 µs | 2.93 µs |

## 4.2 硬件真随机数发生器 (TRNG)

某些 MSPM0 器件包含硬件真随机数生成器 (TRNG) 模块。TRNG 可用于轻松生成真随机种子值，这些值可用于播种确定性随机位发生器 (DRBG)。

TRNG 模块基于器件内部的模拟熵源来提供 32 位真随机输出。TRNG 本地提供了一个专用稳压器，用于防止电源操控攻击。

集成健康测试提供了 TRNG 模拟和数字组件的加电自检，并通过统计自检提供持续监控。

TRNG 适用于构建 TRNG + DRBG 系统，该系统可以通过用于加密随机数生成器的 NIST SP800-22 统计测试套件。图 4-2 中显示了 TRNG 的方框图。

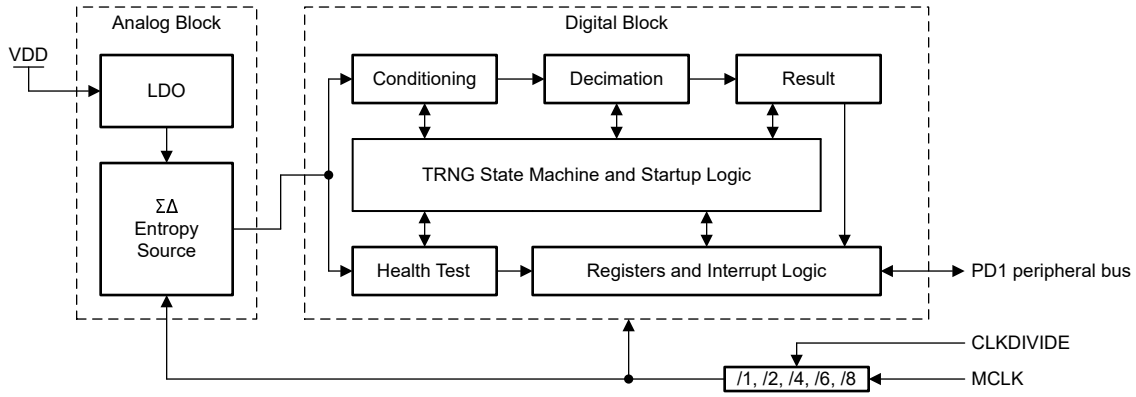


图 4-2. TRNG 方框图

有关 TRNG 操作的更多信息，请参考器件系列技术参考手册。

# 5 器件标识

所有 MSPM0 器件都包含一个特定于器件的 96 位识别码（器件 ID），该识别码可由应用软件读取。有关器件 ID 的更多信息，请参阅技术参考手册和器件数据表。

TI 设计的器件 ID 对于每个发运的器件都是唯一的，因此可用于识别特定器件或将其与任何其他器件区分开来。虽然器件 ID 是唯一的，但它不是加密随机值，因为一些位对应于器件特性，例如器件型号和产品版本。

# 6 总结

MSPM0 MCU 中提供的信息安全机制为希望向新应用添加更多网络安全功能的 MCU 客户提供了独特的功能和价值组合。以同等价位提供的独特功能（例如密码验证的应用调试、批量擦除和恢复出厂设置）支持各种开发和生产用例，同时保持配置简单明了。

## 7 参考文献


- TI 安全电子书 (SWPB021)
- TI 安全性门户 ( 链接 )
- MSPM0G 技术参考手册 (SLAU846)
- MSPM0L 技术参考手册 (SLAU847)


## 8 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

| 日期 | 修订版本 | 说明 |
|---|---|---|
| 2023 年 1 月 | * | 初始发行版 |

# A 各子系列提供的信息安全机制

表 A-1 中列出了给定 MSPM0 子系列中包含的信息安全机制。请注意，某些功能是为未来的 MSPM0 器件计划的，可能并未包含在表中所示的器件系列中。

**表 A-1. MSPM0 子系列提供的信息安全机制**

| 信息安全机制 | 信息安全机制 | MSPM0L110x | MSPM0L13xx | MSPM0G110x | MSPM0G150x | MSPM0G3x0x |
|---|---|---|---|---|---|---|
| 调试安全性 | 密码验证的调试访问 | 是 | | | | |
| | 密码验证的引导加载程序访问 | 是 | | | | |
| | 密码验证的主闪存批量擦除 | 是 | | | | |
| | 密码验证的完全恢复出厂设置 | 是 | | | | |
| | TI 失效分析 (FA) 启用/禁用 | 是 | | | | |
| | 串行线调试 (SWD) 接口的完全硬件禁用 | 是 | | | | |
| | 可永久锁定的器件配置数据 | 是 | | | | |
| | 防错器件配置数据 | 是 | | | | |
| | 密码存储器仅包含哈希值 (SHA2-256) | 否 | | | | |
| 安全启动 | 可永久锁定的主闪存（静态写保护） | 是 | | | | |
| | CRC-32 验证的主闪存区域 | 是 | | | | |
| | SHA2-256 验证的主闪存区域 | 否 | | | | |
| | 引导时主闪存应用程序的单点入口 | 是 | | | | |
| | 固件映像身份验证例程（非对称或对称） | 是 | | | | |
| | 用于密钥撤销和回滚保护的可锁定闪存 | 否 | | | | |
| | SRAM W^X（写入或执行）边界强制执行 | 是 | | | | |
| 安全存储 | 静态闪存读取/执行 (RX) 防火墙 | 否 | | | | |
| | IP 保护（仅执行）防火墙 | 否 | | | | |
| | 主闪存存储体上的 W^X（写入或执行）强制执行 | 否 | | | | |
| | AES 易失性密钥存储区（最多四个 128 位密钥加上一个会话密钥） | 否 | | | | |
| 加密加速 | 硬件 AES 加速器（128 位/256 位） | 否 | | | 是 | |
| | 硬件 TRNG | 否 | | | 是 | |
| 器件身份 | 唯一器件标识符（96 位） | 是 | | | | |
| 物理安全 | 引导配置例程故障注入攻击对策 | 否 | | | | |

# 重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265