Application Note

*不使用启动模式开关将 **Sitara MPU HS-FS** 器件转换成 **HS-SE** 器件*

Zekun Bai, Prashant Shivhare, and Donna Xu

摘要

在汽车和工业应用中，为了保护系统安全和功能隐私，并防止应用程序映像被恶意篡改、复制或删除，大规模生产的产品通常采用高安全性芯片，这类芯片不同于通用开发中使用的芯片。Sitara 处理器提供通用 (GP) 和高安全性 (HS) 芯片类型来解决该问题。Sitara HS 芯片包含一个 OTP 标识符电子保险丝和多个硬件安全加速器，可为系统映像增加加密和解密功能，并在启动过程中进行签名验证，保护系统免受外部恶意篡改的影响。

HS 器件还具有两种表示 HS 器件状态的子类型：高安全性 - 现场安全（HS-FS）型和高安全性 - 强制安全（HS-SE）型。HS-SE 器件中的所有安全功能都启用。在开发过程中，客户必须使用 TI 提供的 Keywriter 工具将密钥编程到芯片中，将芯片从 HS-FS 转换为 HS-SE。

此编程过程通常涉及不同的方法。本应用手册总结了常用的编程方法，并提出了几种更高效并减少生产线人工干预的新方法。这些新方法无需切换启动模式。密钥编程可在单次启动模式下执行。

内容

1 简介.....2
2 使用启动模式开关进行 HS 器件刷写.....3
3 不使用启动模式开关进行 HS 器件刷写.....4
3.1 设计 1：从备用启动介质启动.....5
3.2 设计 2：从主启动介质启动.....6
4 摘要.....7

商标

1 简介

下面介绍 HS-FS 和 HS-SE 之间的差异。

HS-FS 器件

- 允许客户在 HS 器件上运行诊断代码，无需创建签名映像。
- 无安全启动
- JTAG 开路

HS-SE 器件

- 完全安全的 HS 器件
- 所有安全策略均应用
- 强制安全启动
- JTAG 关闭
- 防火墙已启用
- 所有可用的安全功能均已激活

在开发过程中，客户必须使用 Keywriter 将 HS-FS 转换为 HS-SE。

OTP Keywriter

适用于 K3 平台的 OTP 写入器开发为单个二进制文件，可在 HS-FS 器件上运行并可对客户的电子保险丝密钥进行编程。

OTP 写入器是单个映像，包含安全部分和非安全部分。

- 非安全部分或 OTP 应用程序在 R5 上运行
- 安全部分本质上是 OTP 驱动程序，在 DMSC 子系统上作为 SYSFW 的一部分运行

非安全出厂密钥配置支持：

- Keywriter 包含加密的 TI FEK 私钥
- 提供给客户的 FEK 公钥，用于加密对称密钥 (SMEK 和 BMEK)

可以使用 X509 证书输入用户可配置的参数。该 OTP 配置证书包含：

- SMPK 哈希和 FEK 加密的 SMEK、选项和 BCH
- BMPK 哈希和 FEK 加密的 BMEK、选项和 BCH
- SWREV、KEYREV (用于选择活动密钥)、KEYCNT (使用的密钥数量)
- 用于 VPP 的 GPIO (对于 16FF 器件是可选的)
- 用于唤醒 UART 的 UART 多路复用器配置
- TI FEK 私钥，使用通过 TI 对称密钥 (MEK) 获得的密钥进行加密
- 具有完整根密钥的签名证书 (克隆保护)

2 使用启动模式开关进行 HS 器件刷写

对于大规模生产的产品，使用 Keywriter 的典型启动流程是存储器 A 启动模式和存储器 B 启动模式。

下面我们举例说明：

1. 使用 SD 卡作为启动介质 (1)，并将 Keywriter 启动映像存储在 SD 卡上。使用 Nor 闪存作为启动介质 (2)，并在出厂时离线烧录服务启动映像和应用程序。
2. 将首次上电时的启动模式设置为 SD 卡。根据启动模式设置，启动 ROM 从 SD 卡读取 Keywriter，将客户密钥烧录到芯片的 OTP 区域，并将芯片从 HS-FS 转换为 HS-SE。
3. 断电并将启动模式切换为 OSPI 启动模式。
4. 再次上电，启动 ROM 从 OSPI Nor 闪存读取服务启动导映像。由于启动映像经过签名和加密，因此启动 ROM 使用启动 ROM 的 X509 标头验证并解密签名，然后正常启动内核。

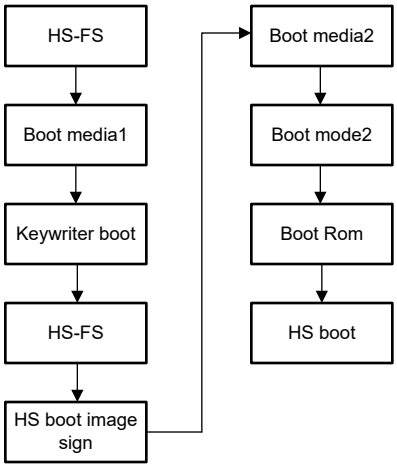

图 2-1. 使用启动模式开关的典型启动流程

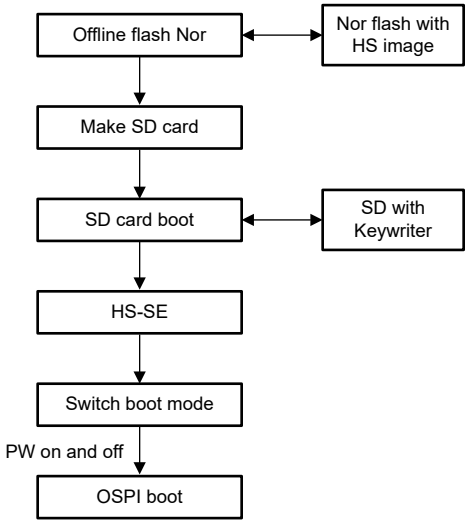

图 2-2. SD 卡为第一启动介质绍，OSPI 启动为第二启动介质

该设计相对成熟，通过在单次运行中切换启动模式，避免了许多可靠性和现场运行问题。

然而，需要与两种存储器启动模式兼容，这增加了 BOM 成本和设计复杂性。第二个问题是切换启动模式需要使用额外的夹具，使生产线复杂化。此外，这种启动模式切换通常需要人工干预，这进一步降低了生产线效率并提高了问题发生率。

3 不使用启动模式开关进行 HS 器件刷写

如果可以在支持安全启动的生产线上实现不采用夹具、且不手动烧录的 Keywriter 方法，这对于必须实现安全启动的客户很重要。TI 的处理器支持冗余启动模式和冗余 OSPI 启动偏移机制。本应用手册利用此机制提供了几种设计，以解决这一问题。

主 OSPI 偏移和备用 OSPI 偏移

OSPI 协议根据协议命令/地址/数据段的位宽（1 或 8）和数据速率（单倍数据速率 (S) 或双倍数据速率 (D)）进行描述。OSPI 启动模式支持 1S-1S-8S 模式。发出的命令和地址分别为 8 位和 24 位。为 OSPI 模式发出的读取命令为 0x8B，后跟表示地址的零和八个虚拟周期。支持的工作频率为 50MHz。在 OSPI 启动模式下，ROM 代码初始化 OSPI 模块，并从连接到所选片选的 OSPI 闪存读取映像。如果未能从闪存的偏移 0x0 正确读取映像，ROM 会尝试在偏移 0x400000 处获取映像。这是 ROM 支持的唯一冗余映像位置。ROM 代码首先将启动映像复制到片上 RAM 中，然后执行该映像。

主启动模式和备用启动模式

DMSC 是公共 ROM 的启动控制器。DMSC 执行所需的配置并将复位释放到 R5。

R5 检查主启动模式介质并检查映像完整性。如果主启动模式失败，则 R5 会改为使用备用启动模式并检查映像完整性。

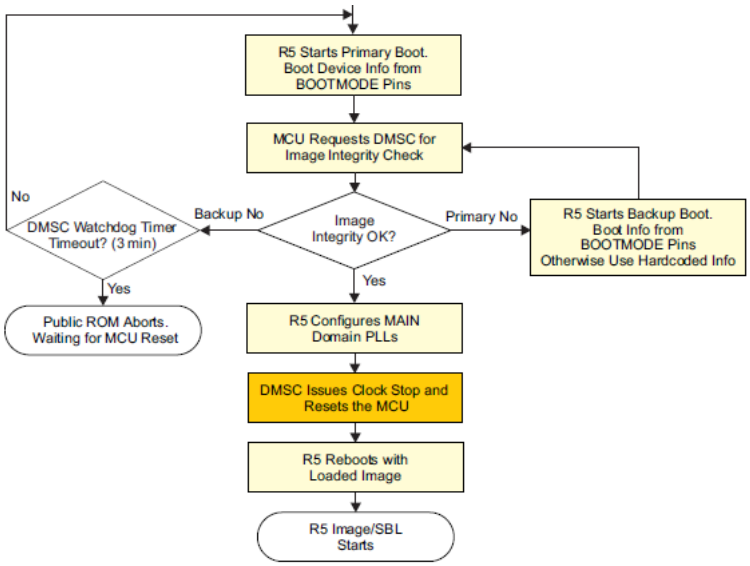

图 3-1. Sitara 主启动和备用启动流程

3.1 设计 1：从备用启动介质启动

本设计的基本理念是通过 DFU 连接到外部 PC。该 PC 存储了三个引导加载程序。第一个引导加载程序是 Keywriter，用于烧录密钥。第二个引导加载程序基于 SDK 提供的 SBL_Uniflash。SBL_Uniflash 使用客户提供的密钥预签名和加密。启动后，SBL_Uniflash 将正常的应用程序文件和 bootloader3（使用客户提供的密钥进行预签名和加密）烧录到闪存中的相关偏移处。上电时，启动 ROM 从主启动模式（即 OSPI）读取应用程序引导加载程序并启动 SOC。

要求

启动模式 => 主启动模式：OSPI、备用：UART/DFU（首选 DFU）。

闪存完全为空。更重要的是，闪存的 0x0 和 0x400000 偏移处被擦除，以便 ROM 回退到备用启动。

过程

1. 第一次 POR 时：器件状态：HS-FS。ROM 从所选备用启动介质启动 OTP Keywriter。根据 Keywriter 指南对密钥进行编程。将 HS-FS 转换为 HS-SE。
2. 在第二次 POR 时：器件状态：HS-SE。ROM 从所选备用启动介质启动闪存写入器。刷写 SDK 映像 (SBL/Applications)
3. 在第三次 POR 时：器件状态：HS-SEROM 从主启动介质 OSPI 启动。

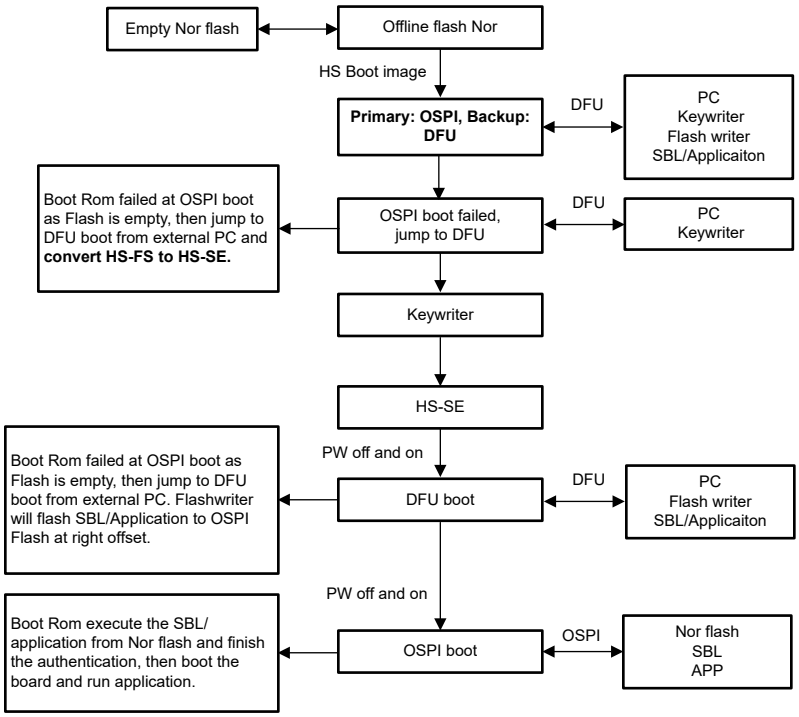

图 3-2. 从备用启动介质启动

3.2 设计 2：从主启动介质启动

本设计的基本理念是将所需文件离线烧录到 NOR 闪存的指定偏移处。这些文件包含三个引导加载程序。

- 第一个引导加载程序是位于地址 0x0 处的 Keywriter，用于烧录密钥。
- 第二个引导加载程序是位于地址 0x400000 处的闪存写入器。该闪存写入器基于单级 SBL/SPL，其唯一的工作是将 SBL 从已知位置 X 移动到主偏移 0x0 处，并且可以选择移动到冗余偏移 0x400000 处。
- 第三个引导加载程序包含来自客户的引导加载程序和应用程序（使用客户提供的密钥进行预签名和加密）。可以根据所选 NOR 闪存容量灵活配置地址，要求地址不与前两个引导加载程序重叠。

在首次上电期间，程序从地址 0x0 处的 Keywriter 执行，将芯片从 HS-FS 转换为 HS-SE。在第二次上电期间，启动 ROM 无法验证地址 0x0 处的 Keywriter，它会跳转到地址 0x400000 以执行闪存写入器。该程序会将客户的服务启动程序和（使用客户提供的密钥进行预签名和加密）烧录到闪存中的地址 0x0，覆盖之前的 Keywriter 文件。此时，再次上电后，启动 ROM 通常从地址 0x0 读取业务启动程序和应用程序，完成密钥签名验证和解密，然后完成启动并启动 SOC。

要求

启动模式 => 主启动模式：OSPI、备用：（无关）

使用相关偏移处的三个文件部分离线刷写闪存。

过程

1. 第一次 POR 时：器件状态：HS-FS。ROM 从 NOR 闪存 0x0 偏移处启动 OTP Keywriter。根据 Keywriter 指南对密钥进行编程。将 HS-FS 转换为 HS-SE。
2. 在第二次 POR 时：器件状态：HS-SEROM 从 NOR 闪存 0x400000 偏移处启动闪存写入器。将 SDK 映像 (SBL/Applications) 刷写到 0x0、0x8000。
3. 在第三次 POR 时：器件状态：HS-SEROM 从 0x0 偏移处启动客户引导加载程序和应用程序并启动电路板。

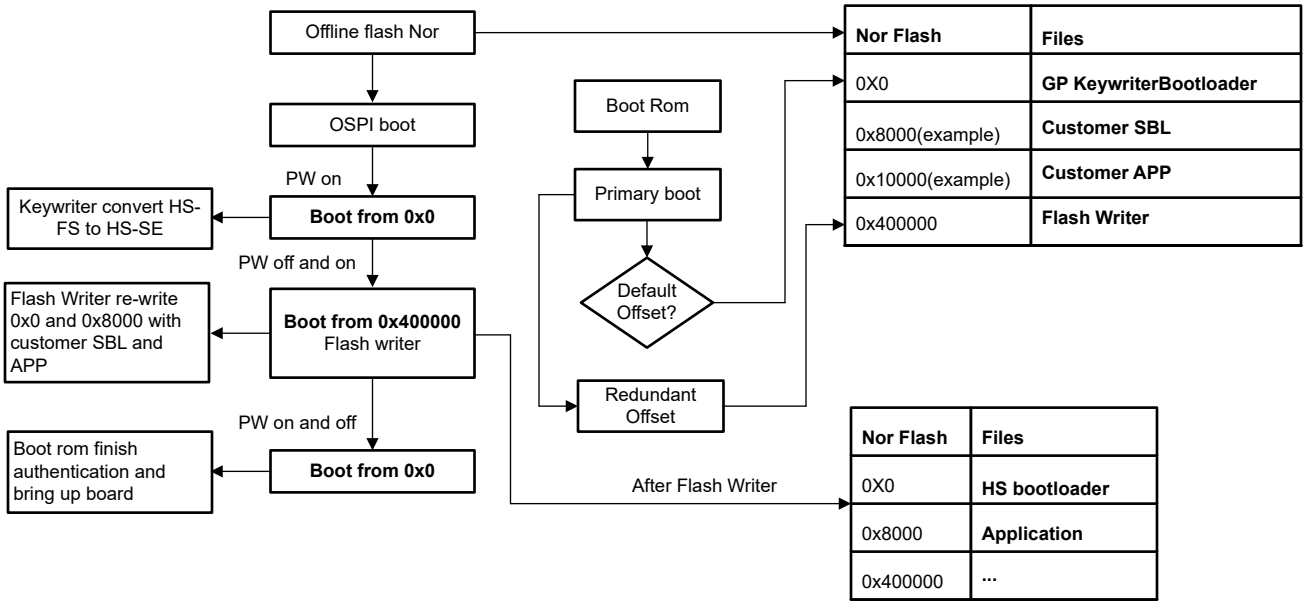

图 3-3. 从主启动介质启动

4 摘要

本应用手册介绍了客户常用的密钥烧录过程，具体涉及切换启动模式以烧录密钥，并实现业务文件的正常启动。

本文档还提供了两种实用的新方法。这些方法无需切换启动模式。但这些方法利用芯片的冗余启动模式，通过多次下电上电来实现密钥烧录和业务文件启动。这种方法的主要优点是简化了生产流程并减少了人工干预。此外，客户的硬件设计不再需要支持多种启动模式，这进一步简化了设计并降低了系统 BOM 成本。请注意，这些只是建议，客户必须对其进行全面测试。

重要通知和免责声明

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、与某特定用途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安全、安保法规或其他要求。

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 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 TI 销售条款)、TI 通用质量指南 或 ti.com 上其他适用条款或 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。 除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

最后更新日期：2025 年 10 月