

Application Note

AM62Ax 器件的 QSPI 寻址模式注意事项



Linjun Meng, Tao Han

Central FAE

摘要

AM62Ax 处理器支持通过片上引导 ROM 从 QSPI NOR 闪存引导，该引导 ROM 在启动期间使用固定的 3 字节寻址模式。一些大容量闪存器件同时支持 3 字节和 4 字节寻址模式，并且可以在闪存持续供电时跨复位事件保留其寻址配置。在某些情况下，这种行为会导致引导 ROM 和闪存器件之间的兼容性不匹配，从而导致证书认证失败和引导中断。

本应用手册介绍了故障机制，提供了一种基于引导 ROM 日志、CCS 内存检查和 QSPI 总线分析的实用调试方法，并讨论了受影响系统的缓解策略。这些信息旨在供开发基于 AM62Ax、通过 QSPI NOR 闪存引导的工业、汽车和嵌入式系统的硬件和软件工程师使用。通过遵循本文档中提供的指导，设计人员可以在使用支持 4 字节寻址模式的闪存器件时，更高效地隔离启动故障并提高引导可靠性。

这些信息面向开发基于 AM62Ax、通过 QSPI NOR 闪存引导的工业和嵌入式系统的硬件和软件工程师，可用于提高启动可靠性并加快根本原因定位。

内容

商标.....	1
1 简介.....	3
1.1 用途.....	3
1.2 范围.....	3
2 详细说明.....	4
2.1 AM62Ax QSPI 引导概述.....	4
2.2 闪存寻址架构.....	4
2.3 引导兼容性注意事项.....	4
2.4 启动调查示例.....	6
2.5 调试方法.....	8
2.6 缓解和设计建议.....	9
3 总结.....	10
4 参考资料.....	11

插图清单

图 2-1. 3 字节寻址模式下的 QSPI 读取时序.....	5
图 2-2. 4 字节寻址模式下的 QSPI 读取时序.....	5
图 2-3. 闪存寻址模式保持对引导过程的影响.....	6
图 2-4. 引导 ROM 认证失败日志.....	7
图 2-5. 由引导 ROM 加载的内存内容.....	7
图 2-6. 启动期间的 QSPI 总线采集.....	8

表格清单

表 2-1. 引导前提条件检查清单.....	4
表 2-2. 复位行为比较.....	6

商标

Jacinto™ 和 Sitara™ 是德州仪器 (TI) 的商标。

所有商标均为其各自所有者所有。

1 简介

1.1 用途

QSPI NOR 闪存存在基于 AM62Ax 的系统中被广泛用作引导器件，因为 QSPI NOR 闪存具有紧凑的占用空间、较少的引脚数量以及简洁的引导架构。在系统开发过程中，设计人员必须理解在不同复位条件下，闪存寻址模式的行为如何与引导 ROM 的操作相互影响。

在处理器复位期间保持供电时，某些闪存器件可以保留其配置。如果保留的闪存状态与引导 ROM 的预期不同，在开始执行软件之前可能会发生启动兼容性问题。由于这些故障发生在引导 ROM 阶段，因此传统的软件调试方法难以有效确定根本原因。

本应用手册介绍了这些注意事项，并提供了诊断和缓解此类问题的实用方法。

1.2 范围

本文档适用于：

- 从 QSPI NOR 闪存引导 AM62Ax 处理器
- 支持 3 字节和 4 字节寻址模式的闪存器件
- 实现 MCU_PORz 或热复位机制的系统
- 能够跨复位事件保留配置状态的闪存器件

2 详细说明

2.1 AM62Ax QSPI 引导概述

2.1.1 引导前提条件

在引导 ROM 能够成功访问 QSPI 闪存之前，必须满足以下条件。

表 2-1. 引导前提条件检查清单

条目	要求
参考时钟	有效的 MCU_OSC0_XI 输入
启动配置	配置为 QSPI 引导的 BOOTMODE
QSPI	与闪存器件实现功能通信

在启动调试期间，必须首先验证这些条件是否满足。

2.1.2 引导 ROM 读取序列

复位释放后，AM62Ax 引导 ROM 执行以下序列：

1. 使用命令 0x9F 读取闪存 JEDEC ID。
2. 发出 Quad Output Fast Read 命令 0x6B。
3. 从地址 0x000000 开始，读取 tiboot3.bin。
4. 验证证书和镜像标头。
5. 将执行权转移到下一个引导阶段。

引导 ROM 使用固定的通信参数：

- 读取命令：0x6B
- 传输模式：1S-1S-4S
- 地址阶段：3 字节
- 虚拟周期：8
- 时钟频率：50MHz

这些参数在引导 ROM 实现中经过硬编码，无法通过软件修改。

2.2 闪存寻址架构

2.2.1 3 字节寻址模式

在 3 字节寻址模式下，闪存器件使用 3 字节地址阶段，并支持访问前 16MB 的内存空间。

大多数 QSPI NOR 闪存器件在上电或硬件复位后会自动进入 3 字节寻址模式。

2.2.2 4 字节寻址模式

高容量闪存器件通常支持 4 字节寻址模式，从而将可寻址内存扩展到前 16MB 之外。

通常通过软件命令进入此模式，并在显式退出该模式或发生复位之前保持有效。

2.2.3 状态保持行为

配置寄存器的行为因闪存供应商和器件系列而异。

对于某些器件，只要保持供电，配置状态就会保持不变。

对于没有独立 RESET# 引脚的闪存器件，如果未移除闪存电源，则在 MCU_PORz 复位后，寻址模式可能保持不变。

2.3 引导兼容性注意事项

2.3.1 引导 ROM 的预期

在启动期间，AM62Ax 引导 ROM 始终假定闪存器件在 3 字节寻址模式下运行。

引导 ROM 发出命令 0x6B，后跟固定的 3 字节地址阶段和 8 个虚拟周期。引导 ROM 不提供任何检测闪存器件当前寻址模式的机制。

2.3.2 寻址模式不匹配机制

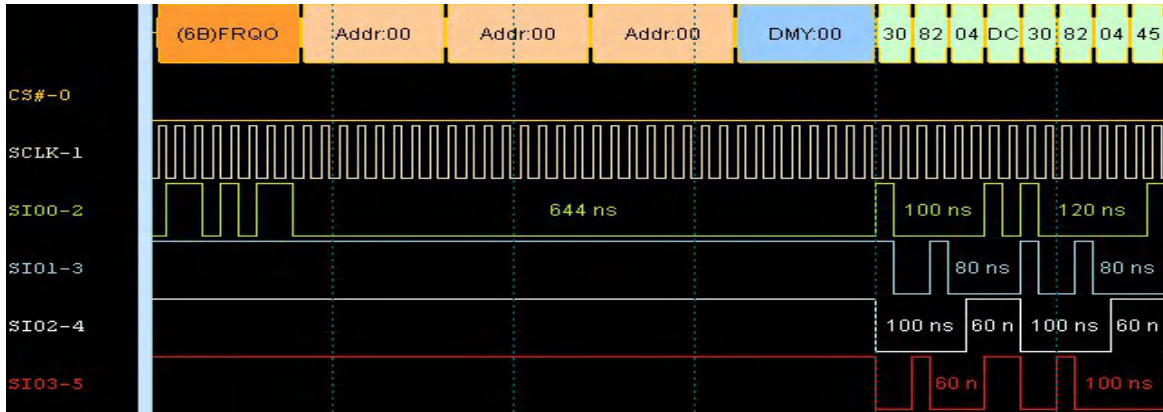


图 2-1. 3 字节寻址模式下的 QSPI 读取时序

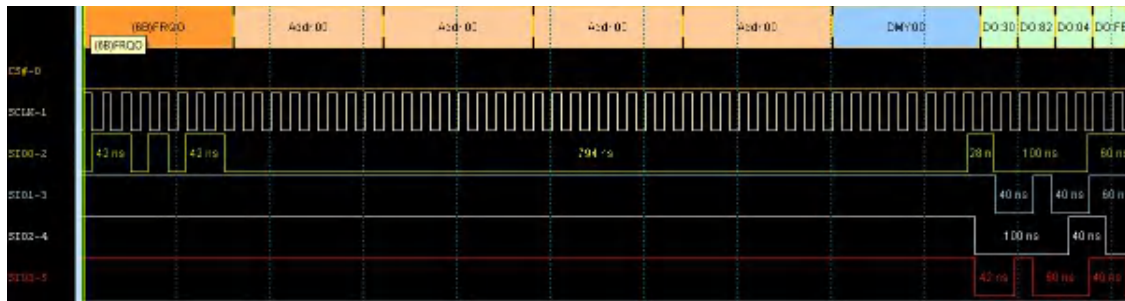


图 2-2. 4 字节寻址模式下的 QSPI 读取时序

当闪存仍配置为 4 字节寻址模式时，引导 ROM 所生成的事务会被以不同于预期协议的方式解释。

引导 ROM 传输：

命令 + 3 字节地址 + 虚拟周期 + 数据

然而，配置为 4 字节寻址模式的闪存器件会将同一事务解释为：

闪存会将引导 ROM 虚拟周期的最后 1 个字节解释为第 4 个地址字节。

因此，引导 ROM 虚拟周期的一部分被解释为地址信息，导致闪存数据输出相对于引导 ROM 采样点发生偏移。

2.3.3 启动影响

寻址模式不匹配会在引导 ROM 加载的镜像中引入数据位移。

在所研究的系统中，镜像内容发生了 1 个字节的偏移。因此，tiboot3.bin 中所包含的证书标头不再位于预期的偏移位置，导致证书认证失败，尽管原始镜像和证书仍然有效。

最终的失败序列如图 2-3 所示。

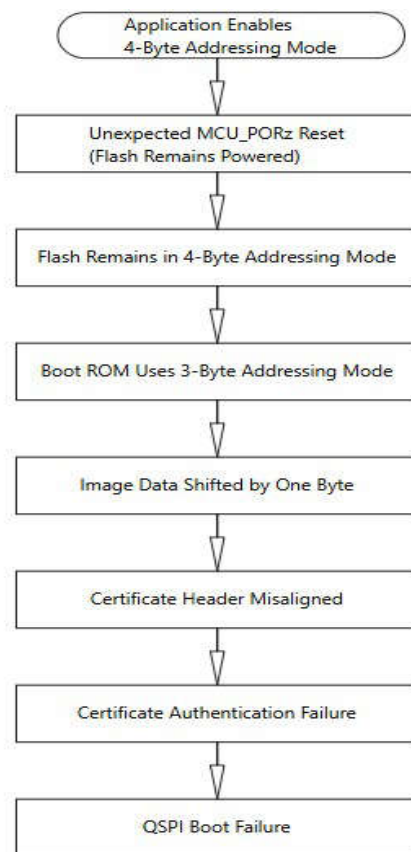


图 2-3. 闪存寻址模式保持对引导过程的影响

2.4 启动调查示例

2.4.1 外部故障症状

所研究的平台表现出以下行为，如表 2-2 所示。

表 2-2. 复位行为比较

复位条件	结果
冷启动	引导成功
Linux 重新引导	引导成功
MCU_PORz 复位	启动失败

当 UART 引导被配置为备用引导源时，器件在 QSPI 引导失败后会自动切换至 UART 引导。

此行为提供了外部迹象，表明故障发生在引导 ROM 阶段。

2.4.2 引导 ROM 日志分析

图 2-4 显示了引导 ROM 解码后的故障日志。

```
Warning Log:
Log Max Index Size: 21
Log current entry: 4
Log buffer: 0x43c3e480
0: main.c:1397 ecode: 0x2010018, ts: 445
"Main_derPanic()!!!"
1: main.c:1752 ecode: 0xffffffff, ts: 450
"derOneParse() failed"
2: main.c:1397 ecode: 0x2010018, ts: 679
"Main_derPanic()!!!"
3: main.c:1752 ecode: 0xffffffff, ts: 683
"derOneParse() failed"
```

图 2-4. 引导 ROM 认证失败日志

使用 TI ROM 引导日志转储实用程序，采集并解码引导 ROM 故障日志。

解码后的日志报告了证书认证失败。

尽管此消息最初表明可能存在镜像签名或证书生成问题，但后续验证确认原始 **tiboot3.bin** 镜像和证书有效。因此，认证失败被视为症状，而非根本原因。

2.4.3 使用 CCS 进行内存验证

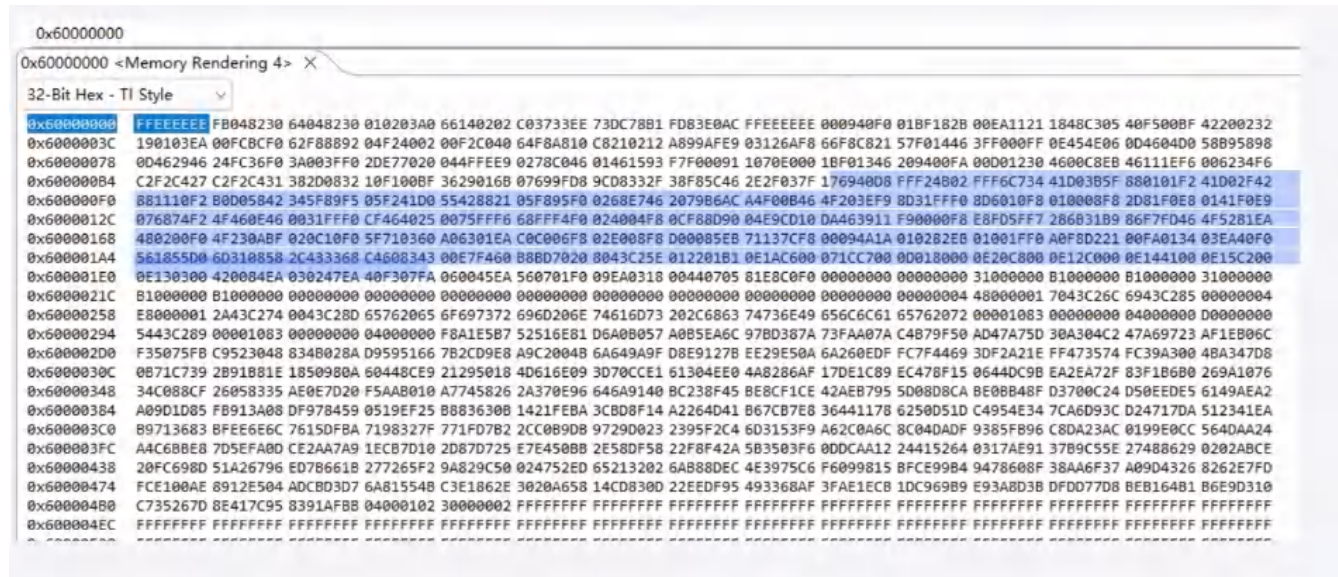


图 2-5. 由引导 ROM 加载的内存内容

将故障系统连接至 CCS，并检查由引导 ROM 加载的内存内容。

预期的证书标识符未出现在预期的偏移位置。内存中的前几个字节与原始 **tiboot3.bin** 镜像中的对应字节不同。与一次成功启动的案例对比显示，证书标头的第 1 个字节发生了 1 字节的位移。

这一观察结果表明，镜像损坏发生在证书验证开始之前。

2.4.4 镜像比较

对以下内容进行了比较：

- 原始 tiboot3.bin 镜像
- 引导 ROM 加载的内存内容

该比较显示，整个镜像均发生了一致的 1 字节位移。

由于证书标头必须位于固定偏移位置，因此位移直接导致了认证失败。

2.4.5 QSPI 总线分析

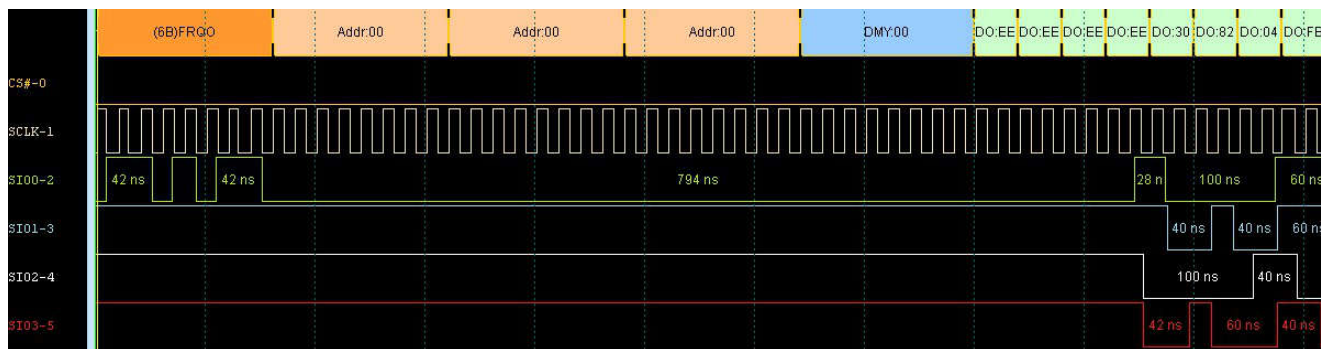


图 2-6. 启动期间的 QSPI 总线采集

逻辑分析仪的采集结果证实：

- 引导 ROM 使用 3 字节地址阶段传输了命令 0x6B。
- 闪存器件保持在 4 字节寻址模式。
- 闪存数据输出比预期晚 1 个字节。
- 观察到的位移与 CCS 内存检查期间所识别到的偏移一致。

这一关联性提供了直接证据，表明认证失败的原因在于闪存读取损坏，而非证书生成或镜像签名错误。

2.4.6 根本原因确认

以下证据综合表明：

- 引导 ROM 日志分析
- CCS 内存检查
- 镜像比较
- QSPI 总线分析

确认启动失败源于引导 ROM 与闪存器件之间的寻址模式不匹配。

引导 ROM 始终使用 3 字节地址阶段访问闪存，而闪存器件在 MCU_PORz 复位后仍配置为 4 字节寻址模式。这种不匹配在镜像数据流中引入了 1 个字节的位移，并最终导致了证书认证失败。

2.5 调试方法

在引导 ROM 阶段发生启动故障时，建议使用以下方法。

- 第 1 步：采集引导 ROM 日志
 - 确定器件是否进入备用引导模式，并使用相应的 TI 实用程序收集引导 ROM 日志。
- 第 2 步：确认身份验证错误
 - 确定所报告的认证失败是由证书问题还是镜像数据损坏引起的。
- 第 3 步：检查由引导 ROM 加载的内存
 - 使用 CCS 检查由引导 ROM 填充的内存内容。
- 第 4 步：与原始 tiboot3.bin 进行比较
 - 验证由引导 ROM 加载的镜像是否与已编程的镜像完全匹配。

5. 第 5 步：分析 QSPI 总线时序
 - 使用逻辑分析仪采集 QSPI 事务并验证协议时序。
6. 第 6 步：验证闪存寻址配置
 - 确认闪存器件在复位后保留的寻址模式。

2.6 缓解和设计建议

2.6.1 首选解决方案：闪存复位同步

首选解决方案是确保闪存器件在每次处理器复位时都复位。

这可确保闪存存在引导 ROM 开始执行之前返回到 3 字节寻址模式，并提供更高级别的启动稳健性。

2.6.2 替代解决方案：驱动程序层级缓解

在所研究的平台上，通过使用 0x6C 命令配合 4 字节地址阶段来标准化闪存读取操作，从而实施了软件缓解措施。

与引导 ROM 命令 0x6B 不同，无论闪存器件当前处于 3 字节还是 4 字节寻址模式，只要目标地址仍处于较低地址的闪存地址空间内，命令 0x6C 即可正常工作。

这种方法消除了正常软件操作期间对当前闪存寻址状态的依赖。在重复进行 MCU_PORz 复位测试期间实施该修改后，未观察到启动故障。

2.6.3 0x6C 缓解措施的适用性

当应用不需要在 16MB 地址边界之外执行擦除或编程操作时，基于 0x6C 的缓解措施有效。

典型示例包括：

- 引导镜像存储
- 固件存储
- 只读配置存储

在此类系统中，闪存访问可统一使用带有 4 字节地址阶段的 0x6C 命令，从而消除对寻址模式的依赖。

2.6.4 大容量闪存应用的设计限制

对于需要跨越 16MB 边界执行擦除或编程操作的应用，仍必须进入 4 字节寻址模式才能访问更高的内存区域。

在此类操作之后，一次意外的复位可能导致闪存器件停留在 4 字节寻址模式，而引导 tROM 则继续假定为 3 字节寻址模式。

对于没有独立 RESET# 引脚的闪存器件，这种情况可能再次导致本应用手册中所述的启动兼容性问题。因此：

- 硬件复位同步仍然是首选解决方案。
- 选择器件时必须考虑闪存复位行为。
- 鉴定测试必须包括热复位验证。
- 必须在软件中显式管理寻址模式转换。

3 总结

本文档所研究的启动问题可追溯至 AM62Ax 引导 ROM 与闪存器件之间的寻址模式不匹配。

尽管外部迹象表现为证书认证失败，但引导 ROM 日志分析、CCS 内存检查、镜像对比以及 QSPI 总线验证均表明，实际根本原因是引导 ROM 访问一个仍处于 4 字节寻址模式的闪存器件时引入了 1 个字节的位移。

对于完全在低 16MB 地址空间内运行的系统，已验证了一种基于命令 0x6C 的驱动程序层面缓解措施。然而，需要跨越 16MB 边界执行擦除或编程操作的应用，必须谨慎管理进入和退出 4 字节寻址模式的切换过程。

对于没有独立 RESET# 引脚的闪存器件，将闪存复位与处理器复位同步仍然是首选解决方案，因为这样可以在执行引导 ROM 之前确保闪存处于已知的寻址状态，并提供最高级别的启动可靠性。

4 参考资料

1. 德州仪器 (TI), 《AM62Ax Sitara™ 处理器》, 数据表。
2. 德州仪器 (TI), 《AM62A Sitara™ 处理器技术参考手册》, 技术参考手册。
3. 德州仪器 (TI), 《适用于 AM62AX 的 Processor SDK Linux 软件开发指南》。
4. 德州仪器 (TI), 《适用于 AM62AX 的 AM62Ax MCU+ SDK 11.01.00.16》。
5. Infineon, 《256 Mb/512 Mb/1 Gb SEMPER™ Flash》, 数据表。
6. Dosilicon, DS25M4CB QSPI 闪存数据表。
7. 德州仪器 (TI), AM62A3: 《AM62A3 POR 复位后异常启动》, E2E™ 技术支持论坛。

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。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月