第八章 安全性

8.1 引言

器件的安全性是基于闪存模式的选择。随后的章节介绍闪存安全性的概述和详细信息以及和无安全性设置的区别。

8.2 闪存安全性

Flash 模块通过 FSEC[SEC]位的状态向 MCU 提供 Flash 的安全信息。MCU 确定安全信息以及控制对 Flash 源代码的访问。在复位过程中，flash 模块根据读取的 flash 安全配置位来初始化 FSEC 寄存器。

注意

安全特性只是限制外部的访问：调试和 EzPort。

CPU 的访问是不受 FSEC 的影响的。

在未加密状态，所有的 flash 指令都可以通过外部编程接口(JTAG 和 EzPort)执行。Flash 控制器执行用户代码。当 flash 处于加密状态(FSEC[SEC] = 00，01，或者 11)时，编程接口只支持批量擦除，不会允许存储器的读写。

更多关于 flash 安全选项和使用/禁用 flash 安全选项的信息请查阅 flash 模块章节。

8.3 安全性对其他模块的影响

SOC 使用安全选项来确定那些资源是可用的。下面的章节描述了各个模块和安全性使用和禁止的情况下之间的影响。

8.3.1 安全性和 FlexBus 之间的影响

当安全选项启用时，SIM_SOPT2[FBSL]控制着 FlexBus 的访问权限。FBSL 位同样控制着操作码和操作对象访问允许还是仅操作对象访问允许。

8.3.2 安全性和 EzPort 之间的影响

当安全选项启用时 EzPort 启动模式仍然可用。EzPort 保持 flash 逻辑处于特殊 NVM 模式，这些都限制着 flash 的操作。当 EzPort 和安全模式都启用时，flash 块擦除（BE）仍旧可以执行。写 FCCOB 寄存器(WRFCCOB)命令被限制只能是批量擦除(Erase All Blocks)和验证首块(Read 1s All Blocks)命令。当使能安全选项时通过 EzPort 访问内部存储的命令是被禁止的。

批量擦除(Erase All Blocks)指令可以解除芯片的安全选项。但是所有的信息都会丢失。通过 EzPort 批量擦除也是可用的尽管某些存储部分设置的保护选项。

当批量擦除禁止时，通过 EzPort 批量擦除是被禁用的，不会成功。

8.3.2 安全性和 Debug 之间的影响

当安全选项启用时，JTAG 访问存储资源是被禁止的。边界扫描电路使工作的，但是调试功能是禁止的，所以调试接口是无法读取 flash 内容的。

尽管大部分调试功能是禁止的。调试器仍能够写 MDM-AP 控制器的寄存器来执行批量擦除功能。即使是某些存储器设置了保护选项。

当批量擦除禁止时，通过调试器执行批量擦除的功能也是无效的。

作者 ：默_li
源文件名称 ：K60P144M100SF2RM.pdf
源文件版本 ：K60 Sub-Family Reference Manual, Rev. 6, Nov 2011
目标文件版本 ：0.1
最后编辑日期 ：2012.05.12.13.58
修改说明 ：初稿，本人水平有限，红色部分是在是没能直接翻译出来
有问题可以 Email：soonli@qq.com