

## 使用 **LPC17XX** 的代码读保护

### 概述

代码读保护是一种机制，使用户能够在不同层次的系统安全性保护他们的软件代码和硬件。LPC1700 器件有三种不同的安全级别：CRP1，CRP2 和 CRP3。每个模式增加了安全级别，并限制任何设备访问 CRP3。在这个应用笔记我们研究所有这些安全级别，以及如何使用它们。我们也提供一个例子来检验这些模式的。

会用到 Keil 的 MCB1700 评估板的 Keil uVision3 和 Flash Magic

注意：虽然本应用笔记的例子经过详细的测试，但是仍然强烈建议初步配置器件的安全级别低于 CRP3。一旦代码被成功地保护于 CRP3，将不能更改。

### Flash 存取方法

一般来说，LPC1700 闪存有两种不同的方式访问：

- 使用 JTAG 编程接口：这种方法可以用 Debug 工具下载代码到器件并可以停止运行器件。
- 使用在系统编程 (ISP)：这种方法是通过引导加载器实现，使用 UART0 串行端口。

### 理解 CRP 安全级别

顾名思义，代码读保护 (CRP) 的为用户提供一个方法保护自己的代码被从 Flash 被读取。这样，设计人员阻止未经授权的用户获得目标代码下载到另一个硬件平台。这种情况可以使用 CRP1(代码阅读保护 - 等级 1)，如果使用 CRP2 和 CRP3, JTAG 访问将被阻止，所以 JTAG 没有办法读/擦除/写入闪存，ISP 也无法读取 Flash 内容，只有 Flash 的更新可以执行。

为进一步提高安全等级，防止未经授权的用户更改代码，例如使用 ISP，或者部分更新 Flash 或者破解。可以使用 CRP2，这种情况允许通过 ISP 更新部分 Flash，但是这种方式不允许通过未经授权的用户修改现有代码，因为没有办法修改 Flash，除非首先删除所有 Flash 的内容，这样现有代码也将被丢失。

更高的安全级别是，在你的硬件上下载他自己的代码，这就是硬件保护，能阻止其他人重复使用硬件，在这种情况下，可以防止用户拉低 P2.1 脚进入 ISP 模式，这样未经授权的用户不用通过 ISP 访问 Flash，这种方式提供了最高层的保护。需要注意的是一旦使用了 CRP3 就没有办法更新 Flash 了，但是内部的用户代码可以调用 ISP 命令 (即 IAP)，调用引导加载程序进入 ISP 模式。当我们在调用 ISP 命令，这时候会打开 CRP3 的保护，这意味着会降级我们的保护到 CRP2，在这个保护级别我们依然无法读取 Flash 的内容，但是可以下载新的代码。所以当你使用 CRP3 的保护时，建议用户代码应该留一些这样的“后门”，为了打破 CRP3 的保护。

图 1 显示了不同的 CRP 水平在不同的使用情况下的保护级别

		ISP ACCESS			JTAG ACCESS
		Read Code	Modify sectors	Full Erase & Download new code	
Security levels	NO CRP	Allowed	Allowed	Allowed	Allowed
	CRP1	Not Allowed	Allowed	Allowed	Not Allowed
	CRP2	Not Allowed	Not Allowed	Allowed	Not Allowed
	CRP3	Not Allowed	Not Allowed	Not Allowed	Not Allowed

References:

Allowed
Not Allowed

**Fig 1. Flash device access according the CRP level.**

值得一提的是在应用中编程 (IAP)，不受任何 CRP 的限制。在本应用指南中我们提供了一个打破 CPR3 保护的例子，在需要的时候可以使用。可以解压到本地 PC 的硬盘中，使用 Keil 3.70 编译。(评估版可用)，连接 Keil MCB1700 评估板的串口 0 (标记为 COM0) 和 PC 的串行 COM 。在连接 USB 供电的电缆从 PC。请参考 Keil 评估板的使用手册，以正确的设置跳线进入 ISP。