零死角玩转STM32

设置FLASH的读写保护及解除

淘宝：firestm32.taobao.com

论坛： www.firebbs.cn

扫描进入淘宝店铺

主讲内容

01 选项字节与读写保护

02 修改选项字节的过程

03 操作选项字节的库函数

04 实验：设置读写保护及解除

参考资料:《零死角玩转STM32》

“设置FLASH的读写保护及解除”章节

设置FLASH的读写保护及解除

选项字节与读写保护

在实际发布的产品中，在STM32芯片的内部FLASH存储了控制程序，如果不作任何保护措施的话，可以使用下载器直接把内部FLASH的内容读取回来，得到bin或hex文件格式的代码拷贝，别有用心的厂商即可利用该代码文件山寨产品。为此，STM32芯片提供了多种方式保护内部FLASH的程序不被非法读取，但在默认情况下该保护功能是不开启的，若要开启该功能，需要改写内部FLASH选项字节(Option Bytes)中的配置。

设置FLASH的读写保护及解除

选项字节的内容

选项字节是一段特殊的FLASH空间，STM32芯片会根据它的内容进行读写保护等配置，选项字节的构成如下：

地址	[31:24]	[23:16]	[15:8]	[7:0]
0x1FFF F800	nUSER	USER	nRDP	RDP
0x1FFF F804	nData1	Data1	nData0	Data0
0x1FFF F808	nWRP1	WRP1	nWRP0	WRP0
0x1FFF F80C	nWRP3	WRP3	nWRP2	WRP2

设置FLASH的读写保护及解除

STM32F103系列芯片的选项字节有8个配置项，即上表中的USER、RDP、DATA0/1及WRP0/1/2/3，而表中带n的同类项是该项的反码，即nUSER的值等于(~USER)、nRDP的值等于(~RDP)，STM32利用反码来确保选项字节内容的正确性。

选项字节具体的数据位配置（第一部分）：

选项字节	
地址 0x1FFF F800	
位[7:0] RDP： 读保护选项字节。 读保护用于保护 Flash 中存储的软件代码。 -把 RDP 配置为值 0xA5 时，内部 FLASH 处于无读保护状态 -把 RDP 配置为其它非 0xA5 的值时，内部的 FLASH 处于读保护状态	
位[23:16] USER:用户选项字节 这个字节用于配置下列功能： – 选择看门狗事件：硬件或软件 – 进入停机(STOP)模式时的复位事件 – 进入待机模式时的复位事件	
位 19:23	0xF8：不用
位 18	nRST_STDBY 待机模式复位事件 0：当进入待机模式时产生复位 1：进入待机模式时不产生复位
位 17	nRST_STOP 停机复位事件 0：当进入停机(STOP)模式时产生复位 1：进入停机(STOP)模式时不产生复位
位 16	WDG_SW 门狗事件 1：硬件看门狗 0：软件看门狗

设置FLASH的读写保护及解除

选项字节的内容

选项字节具体的数据位配置（第二部分）：

地址 0x1FFF F804
Datax： 2 个字节的用户数据 这个地址可以使用选项字节的编程方式编程。
地址 0x1FFF F808-0x1FFE F80C
WRPx(0-3)：FLASH 写保护选项字节 对于小容量产品，选项字节 WRPx 中的每一个比特位用于保护主存储器中 4 个存储页(1K 字节/页)： - 0：实施写保护 -1：不实施写保护 每个用户选项字节用于保护 32K 字节的主存储器。 WRP0：第 0~31 页的写保护 对于中容量产品，选项字节 WRPx 中的每一个比特位用于保护主存储器中 4 个存储页(1K 字节/页)： -0：实施写保护 - 1：不实施写保护 四个用户选择字节用于保护总共 128K 字节的主存储器。 WRP0：第 0~31 页的写保护 WRP1：第 32~63 页的写保护 WRP2：第 64~95 页的写保护 WRP3：第 96~127 页的写保护 对于大容量产品，选择字节 WRPx 中的每一个比特位用于保护主存储器中 2 个存储页(2K 字节/页)，但是 WRP3 的位 7 用于保护第 62~255 页： - 0：实施写保护 - 1：不实施写保护 四个用户选择字节用于保护总共 512K 字节的主存储器。 WRP0：第 0~15 页的写保护 WRP1：第 16~31 页的写保护 WRP2：第 32~47 页的写保护 WRP3：位 0~6 提供第 48~61 页的写保护；位 7 提供第 62~255 页的写保护

本章主要讲解选项字节配置中的RDP位和WRP位，它们分别用于配置读保护和写保护。

设置FLASH的读写保护及解除

RDP读保护级别

修改选项字节的RDP位的值可设置内部FLASH为以下保护级别：

- **0xA5：级别0，无保护**

这是STM32的默认保护级别，它没有任何读保护，读取内部FLASH的内容都没有任何限制。也就是说，第三方可以使用调试器等工具，获取该芯片FLASH中存储的程序，然后可以把获得的程序以bin和hex的格式下载到另一块STM32芯片中，加上PCB抄板技术，轻易复制出同样的产品。

- **其它值：级别1，使能读保护**

把RDP配置成除0xA5外的任意数值， 都会使能读保护。在这种情况下，若使用调试功能(使用下载器、仿真器)或者从内部SRAM自举时都不能对内部FLASH作任何访问(读写、擦除都被禁止)；而如果STM32是从内部FLASH自举时，它允许对内部FLASH的任意访问。也就是说，任何尝试从外部访问内部FLASH内容的操作都被禁止。

设置FLASH的读写保护及解除

RDP读保护级别

例如，无法通过下载器读取它的内容，或编写一个从内部SRAM启动的程序，若该SRAM启动的程序读取内部FLASH，会被禁止。而如果是芯片原本的内部FLASH程序自己访问内部FLASH（即从FLASH自举的程序），是完全没有问题的，例如芯片本身的程序，若包含有指针对内部FLASH某个地址进行的读取操作，它能获取正常的数据。

设置FLASH的读写保护及解除

RDP读保护级别

另外，被设置成读保护后，FLASH前4K字节的空间会强制加上写保护，也就是说，即使是从FLASH启动的程序，也无法擦写这4K字节空间的内容；而对于前4K字节以外的空间，读保护并不影响它对其它空间的擦除/写入操作。利用这个特性，可以编写IAP代码(In Application Program)更新FLASH中的程序，它的原理是通过某个通讯接口获取将要更新的程序内容，然后利用内部FLASH擦写操作把这些内容烧录到自己的内部FLASH中，实现应用程序的更新，该原理类似串口ISP程序下载功能，只不过ISP这个接收数据并更新的代码由ST提供，且存放在系统存储区域，而IAP是由用户自行编写的，存放在用户自定义的FLASH区域，且通讯方式可根据用户自身的需求定制，如IIC、SPI等，只要能接收到数据均可。

设置FLASH的读写保护及解除

RDP读保护级别

- 解除保护

当需要解除芯片的读保护时，要把选项字节的RDP位重新设置为0xA5。在解除保护前，芯片会自动触发擦除主FLASH存储器的全部内容，即解除保护后原内部FLASH的代码会丢失，从而防止降级后原内容被读取到。

芯片被配置成读保护后根据不同的使用情况，访问权限不同，总结如下表：

存储区	保护设置	从RAM自举（SRAM调试模式）			从内部FLASH自举		
		读	写	擦除	读	写	擦除
主FLASH前4K字节	读保护	否			是	否	否
主FLASH前4K字节外的空间	读保护	否			是		
选项字节	读保护	是			是		

设置FLASH的读写保护及解除

WRP写保护

使用选项字节的WRP0/1/2/3可以设置主FLASH的写保护，防止它存储的程序内容被修改。

- 设置写保护

写保护的配置一般以4K字节为单位，除WRP3的最后一位比较特殊外，每个WRP选项字节的一位用于控制4K字节的写访问权限， 把对应WRP的位置0即可把它匹配的空间加入写保护。被设置成写保护后，主FLASH中的内容使用任何方式都不能被擦除和写入，写保护不会影响读访问权限，读访问权限完全由前面介绍的读保护设置限制。

- 解除写保护

解除写保护是逆过程，把对应WRP的位置1即可把它匹配的空间解除写保护。解除写保护后，主FLASH中的内容不会像解读保护那样丢失，它会被原样保留。

THANKS

论坛： www.firebbs.cn

淘宝：firestm32.taobao.com

扫描进入淘宝店铺