C8051F MCU 应 用 笔 记

AN020 — FLASH 安全用户指南

相关器件

本应用笔记适用于下列器件：

C8051F000、C8051F001、C8051F002、C8051F005、C8051F006、C8051F010、C8051F011、C8051F012、C8051F015、C8051F016、C8051F017、C8051F206、C8051F220、C8051F221、C8051F226、C8051F230、C8051F231、C8051F236。

引言

Cygnal集成器件公司的在系统可编程FLASH存储器有使用方便、便于程序升级的特点。可以通过JTAG接口或应用程序对FLASH编程，灵活性最高。程序或常数形式的专有信息常常保存在FLASH存储器中。Cygnal提供了可由用户任意支配的安全选项，以防止对保存在FLASH存储器中的信息进行未经授权的访问。

Cygnal集成器件公司提供FLASH安全安全选项以达到下述目的：

1. 防止对以程序或常数形式保存在FLASH存储器中的知识产权信息进行未经授权的访问。
2. 防止最终用户无意中修改程序代码。
3. 防止因异常系统条件导致代码改变（例如低压电源条件）。

Cygnal的这些MCU器件提供的安全选项可以防止通过JTAG口和最终用户下载的应用软件对FLASH进行未经授权的访问。*FLASH程序存储器安全字节*用于防止通过JTAG接口的访问，而*软件读限制*（大多数Cygnal器件都具有该功能）用于防止通过应用软件进行未经授权的访问。本应用笔记讨论FLASH安全选项的操作和使用。

关键点

- 通过将FLASH安全字节中的位设置为0来保护FLASH存储器不能通过JTAG接口被访问。
- 可以用软件设置一个软件读访问限制来保护FLASH存储器不能被读取。（用于允许最终用户访问FLASH存储器器的某些部分。）
- 已被软件访问保护的FLASH存储器也应该用FLASH安全字节保护，使其不能被通过JTAG接口访问。
- 在保护FLASH时，包含FLASH安全字节的FLASH页也应被保护起来。（FLASH不能用软件解保护。）
- 如果最终用户不需要访问FLASH，可以通过简单地锁定整个FLASH存储器保护其不能通过JTAG访问（在这种情况下不需要软件读限制，因为最终用户不能下载软件去访问产权信息）。

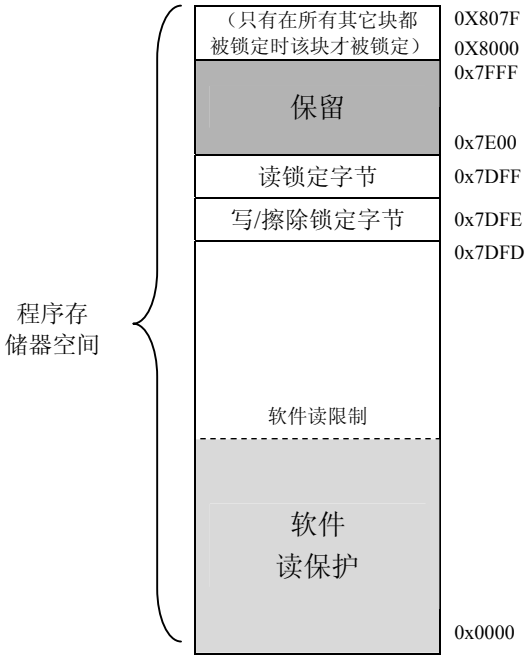
Silicon Laboratories Inc.
4635 Boston Lane
Austin, TX 78735
Email: mcuinfo@silabs.com
Internet: www.silabs.com

新华龙电子有限公司
深圳市福田区华强北路现代之窗大厦 A 座 13F C 室(518013)
电话：0755-83645240 83645242 83645244 83645251
电邮：shenzhen@xhl.com.cn
网址：www.xhl.com.cn

防止通过 JTAG 接口对 FLASH 访问

两种读、写和擦除FLASH存储器的方法之一就是通过JTAG接口（见AN005 – 通过JTAG接口对FLASH编程）。位于FLASH存储器中的*FLASH程序存储器安全字节*用于防止**通过JTAG接口**对一个存储器块中的任一字节或所有512字节进行读和/或写/擦除操作。

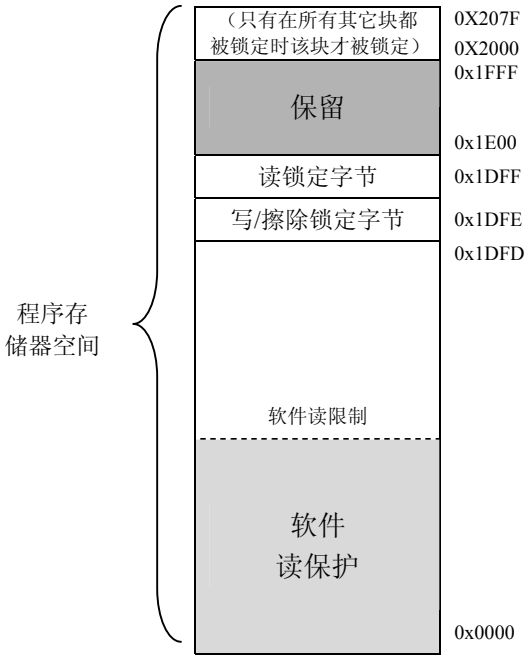
FLASH安全字节在FLASH存储器中的位置如图1和图2所示。为了保护一个FLASH块，防止通过JTAG接口对其进行未经授权的读或写/擦除操作，参见存储器块示意图（在每个器件的数据表中都有）。



读和写/擦除安全位。
（位7为MSB。）

位	存储器块
7	0x7000 – 0x7DFD
6	0x6000 – 0x6FFF
5	0x5000 – 0x5FFF
4	0x4000 – 0x4FFF
3	0x3000 – 0x3FFF
2	0x2000 – 0x2FFF
1	0x1000 – 0x1FFF
0	0x0000 – 0x0FFF

图1. 80C51F0xx系列器件的FLASH安全字节



读和写/擦除安全位。
（位7为MSB。）

位	存储器块
7	0x1C00 – 0x1DFD
6	0x1800 – 0x1BFF
5	0x1400 – 0x17FF
4	0x1000 – 0x13FF
3	0x0C00 – 0x0FFF
2	0x0800 – 0x0BFF
1	0x0400 – 0x07FF
0	0x0000 – 0x03FF

图2. 80C51F2xx系列器件的FLASH安全字节

试图在一个被读锁定的扇区内读一个字节会导致返回一个‘0’值，并将FLASHDAT寄存器中的FAIL位置‘1’，表示本次FLASH操作失败。（若需更多关于如何通过JTAG接口读FLASH数据的信息，请见应用笔记：“AN005 – 通过JTAG接口对FLASH编程”）。将读锁定字节中的一位清0可防止通过JTAG接口读相应的FLASH扇区。

试图在一个被写/擦除锁定的扇区内进行写或擦除一个字节的操作将被忽略，FLASHDAT寄存器中的FAIL位被置‘1’，表示本次FLASH操作失败。将写/擦除锁定字节中的一位清0可防止通过JTAG接口对相应的FLASH扇区进行写/擦除操作。将整个安全字节清除为0x00可保护整个FLASH代码空间不能由JTAG接口操作。

注意：FLASH安全字节只能防止JTAG接口对FLASH操作 — 软件仍然可以访问JTAG锁定的存储块！为防止未经授权的访问，应用程序应锁定整个FLASH存储器。锁定全部存储器字节可以防止最终用户下载程序对存储器空间解锁并进而用软件访问锁定空间的信息。如果一个应用必须留出一部分未锁定的存储器空间，但设计者还想防止他人访问某些FLASH存储器，则可将*FLASH访问限制*功能与安全字节配合使用。在一个某些FLASH存储块被锁定而另一些留给最终用户的存储块不被锁定的应用中，应对包含安全字节的存储块进行写/擦除锁定，以防止通过擦除含有安全字节的FLASH页对被保护的FLASH存储块解锁。

器件擦除

使用读锁定字节或擦除/写锁定字节的地址执行一次擦除操作将自动启动对整个FLASH程序空间的擦除操作（保留区例外）。**这只能通过JTAG接口实现，不能用软件实现。**如果软件试图擦除

包含锁定字节的FLASH页，则该擦除操作将被忽略。如果执行一次FLASH擦除时所使用的地址是FLASH安全字节所在扇区内的一个非安全字节，则只有这一个512字节的页被擦除（包括安全字节）。

防止通过软件访问 FLASH

注：C8051F000/01/02和C8051F010/11/12不具备下面将要讨论的**软件访问读限制**这一安全功能。对于这些器件，应使用FLASH安全字节对整个FLASH用户空间实行读和写/擦除锁定以保护知识产权。

可以通过应用软件访问Cygnal器件的FLASH存储器（见应用笔记：“AN009 – 从应用程序写FLASH”）。这为应用程序设计（包括实现引导装入程序）提供了最大的灵活性，但也给最终用户提供了一条访问JTAG锁定的FLASH存储器的途径（除非所有的FLASH存储器都被锁定）。为此，Cygnal器件提供了软件读限制这一FLASH访问功能，可以限制下载的应用程序对FLASH存储器进行访问。软件读限制与安全字节配合使用可以防止JTAG访问，软件读限制允许应用程序保护某些FLASH存储器不被软件访问，而留出一些FLASH存储器供最终用户自由使用。

FLASH软件访问限制的工作原理如下。设计者定义一个访问限制地址。从地址0x0000到该地址（包含该地址）的存储区被定义为*软件读限制*区而受到保护，不能用软件访问。如果位于该软件访问限制地址之上的程序试图执行一条MOVC指令以访问被设置为软件读保护的地址空间，返回值将是0x00。位于软件保护空间之内（在FLACL边界以下）的程序在执行时不受任何限制。在软件访问限制地址边界以上的FLASH存储器可作为正常工作区（即软件可以正常进行读和写/擦除操作），但不能写或擦除FLACL边界地址以下的代码。这样，应用程序就可以保护代码使其免于非授权访问，而又给最终用户留出可用的FLASH存储器空间。

注：应使用安全字节对被设置为软件读保护的FLASH锁定，防止通过JTAG接口对被保护存储块的访问。（当只锁定某些存储块时，应保证锁定包含安全字节的存储块，以防止JTAG访问和最终用户对FLASH存储器解锁。）

设置软件读限制

使用FLASH访问限制（FLACL）这一特殊功能寄存器来设置软件读限制。所希望的软件访问限制地址（设计者希望的软件访问保护的最高地址）的高字节被装入FLACL寄存器。该限制地址的低字节为0x00。参见图3。如果FLACL寄存器被赋值为0x40，则软件访问限制地址为0x4000。所有位于地址0x0000到0x4000（包括0x4000）的存储区内的代码将不能被在该地址以上执行的软件访问。在FLACL边界之上执行的程序可以用跳转或调用指令进入到FLACL边界以下的保护存储区。软件读限制只对MOVX和MOVC操作起作用。为了防止对FLASH的访问，应使用FLASH安全字节保护0x4000以下的存储区或进行整体保护（见前一节：“防止通过JTAG接口对FLASH访问”）。

R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W	复位值
								00000000
位7	位6	位5	位4	位3	位2	位1	位0	SFR地址: 0xB7

位 7-0: FLACL: FLASH 存储器读限制
该寄存器保存 16 位程序存储器读限制地址的高字节。完整的 16 位访问限制地址值按 0xNN00 计算，其中 NN 用 FLACL 的内容替换。对该寄存器的写操作设置 FLASH 访问限制地址。在下一次复位之前，任何后续的写操作都被忽略。

图 3. FLACL: FLASH 访问限制特殊功能寄存器

如果在一个应用中不需要最终用户对FLASH存储器重新编程，则最好的做法是用安全字节锁定整个FLASH存储器，而不必设置软件访问限制（最终用户将不能下载代码到FLASH中访问被保护的信息）。

FLASH 写和擦除允许位

FLASH安全的功能之一是防止对代码的无意修改。如果不设置程序存储写允许（PSWE）和程序存储擦除允许（PSEE）位，则不允许对Cygnal FLASH存储器进行写和擦除操作。如果要写FLASH存储器，PSWE位必须被置‘1’。当PSWE位被置‘1’时，MOVX指令写入到FLASH而不写到XRAM（默认目标）。如果要擦除FLASH存储器的一个页面，PSEE位和PSWE位必须被置‘1’。当PSEE位被置‘1’时，FLASH控制逻辑将一个FLASH写操作解释为一个FLASH擦除操作。PSEE和PSWE位有助于防止对代码的意外写和擦除修改。当然，这并不能实现保护知识产权不被最终用户访问的功能，因为PSWE和PSEE位总是可访问的。要使用软件读访问限制和/或FLASH安全字节对知识产权进行保护。