

One Time Programmable(OTP) ON AT32 MCU

前言

对于AT32 MCU，除了出厂固化的bootloader，用户也可以在应用程序中编写自己的bootloader程序随着嵌入式应用越来越广泛，产品的安全也越来越重要，一方面是为了保护硬件设计，另一方面也是为了产品本身的安全，防止被hacked。嵌入式系统中，所有的代码和数据都是存储在Flash内部。Flash的特点是可以多次擦写，并且掉电数据不会丢失。为了保护Flash中的数据，很多Flash厂商在内部提供了一种特殊的寄存器：OTP(One Time Programmable)寄存器，该寄存器只可以编程一次，并且编程后再也无法修改。用户可以在OTP寄存器中保存一些特殊信息，例如产品的软件版本号、硬件版本号、密钥等等。

这篇应用笔记描述了如何使用带安全库功能的AT32 MCU，来实现类似OTP寄存器的功能。

参考资料：

各型号参考手册的闪存控制器章节

支持型号列表：

支持型号	具备 sLib 的型号
------	-------------

目录

1	概述.....	5
2	操作说明	6
	2.1 通过代码操作.....	6
	2.2 通过 ICP/ISP 等工具操作	6
3	版本历史	9

表目录

表 1. 文档版本历史	9
-------------------	---

图目录

图 1. ICP 添加文件	7
图 2. ICP 下载配置	7
图 3. 验证结果	8

1 概述

对于 AT32 MCU 不同的系列，因为功能改进等原因，安全库区的配置使用可能有所差异。用户使用 OTP 功能主要目的是需要将一些特殊数据保存其中，在需要时可以读取，并且不允许修改和擦除。

目前 AT32 MCU 的安全库区根据内部结构可以分为以下几种区域

- 仅允许 I-Code 总线读取指令的区域(I-BUS area)
- 仅允许 D-Code 总线读取数据的区域(D-BUS area)
- 允许 I-Code 和 D-Code 总线读取的唯读区域(READ-ONLY area)

只要包含允许 D-Code 总线访问的区域，其特点就是允许读取数据，不允许擦除或者修改（除非原应用设计者输入自定义密钥 KEY 解除 slib 进行全部擦除），达到 OTP 功能的效果。所以只要设计者将需使用 OTP 功能的数据保存在允许 D-Code 总线访问的安全库区域，就能达到只允许读取，不允许擦除和修改的目的。

2 操作说明

根据 AT32 MCU 的安全库区结构划分，必须将要保存的 OTP 数据放置在允许 D-Code 总线访问的区域(D-BUS area 或者 READ-ONLY area)。

2.1 通过代码操作

Demo 中 403A 的 AT-START 开发板上，演示如何开启 slib，并将数据放在 slib 的 D-Code 区域。

执行流程及说明：

- 1) 按 USER 键触发；
- 2) 如果程序首次执行(MCU 处于 slib disable 状态)，顺序往下执行步骤 3，如果程序非首次运行(MCU 处于 slib enable 状态)，跳转到流程步骤 7 进行；
- 3) 配置 slib，包括 password 和 range；
- 4) 写入 OTP 数据到 slib 的 D-code 区域；
- 5) LED2/3/4 会同时亮起；
- 6) 按 RESET 键复位，重新执行流程步骤 1；
- 7) 此时 OTP 功能生效，因为 slib 已开启，无法再次配置 slib，也不能擦除或者修改对应区域数据，LED2 亮起；
- 8) 按 USER 键触发；
- 9) 关闭 slib（当程序在 flash 运行时，执行该步骤会触发 flash mass erase，程序无法再继续运行），执行系统复位，结束演示。

注意事项：

- demo 中定义 256 字节数据作为 OTP 数据，选择的 slib D-Code 区域是对应系列 MCU 可设置 slib 范围的最后一个 sector。关于不同系列 MCU 的 slib 可设置范围，可以参看对应的 AT32 各系列安全库区(SLIB)应用指南。
- 演示完成后，关闭 slib 是为了方便后续 MCU 调试使用。真实应用时 slib OTP 功能开启会不再 disable。

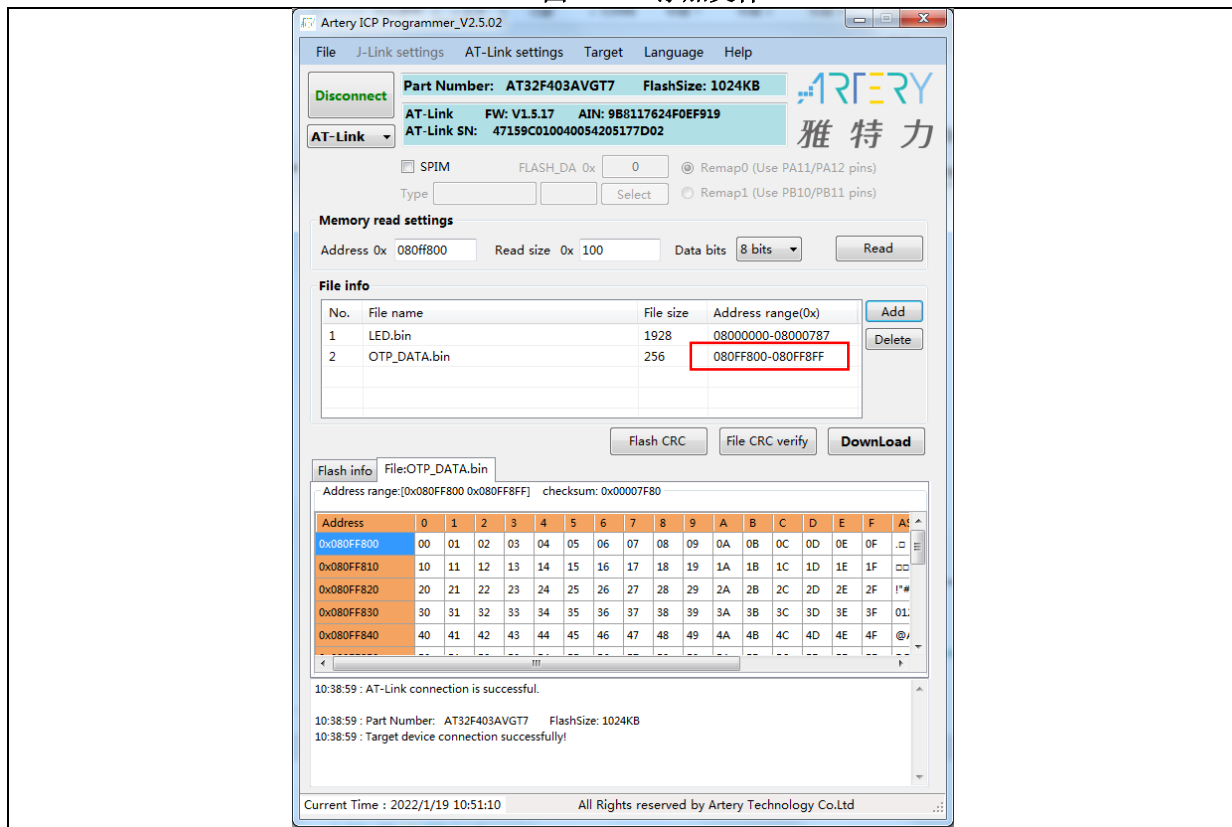
2.2 通过 ICP/ISP 等工具操作

通过 Artery 的 ICP/ISP 等上位机软件可以更方便的实现该功能，在烧录项目文件时，将需保存的 OTP 数据一起烧录，完成 slib OTP 功能。

以 ICP 工具在线烧录为例，步骤如下：

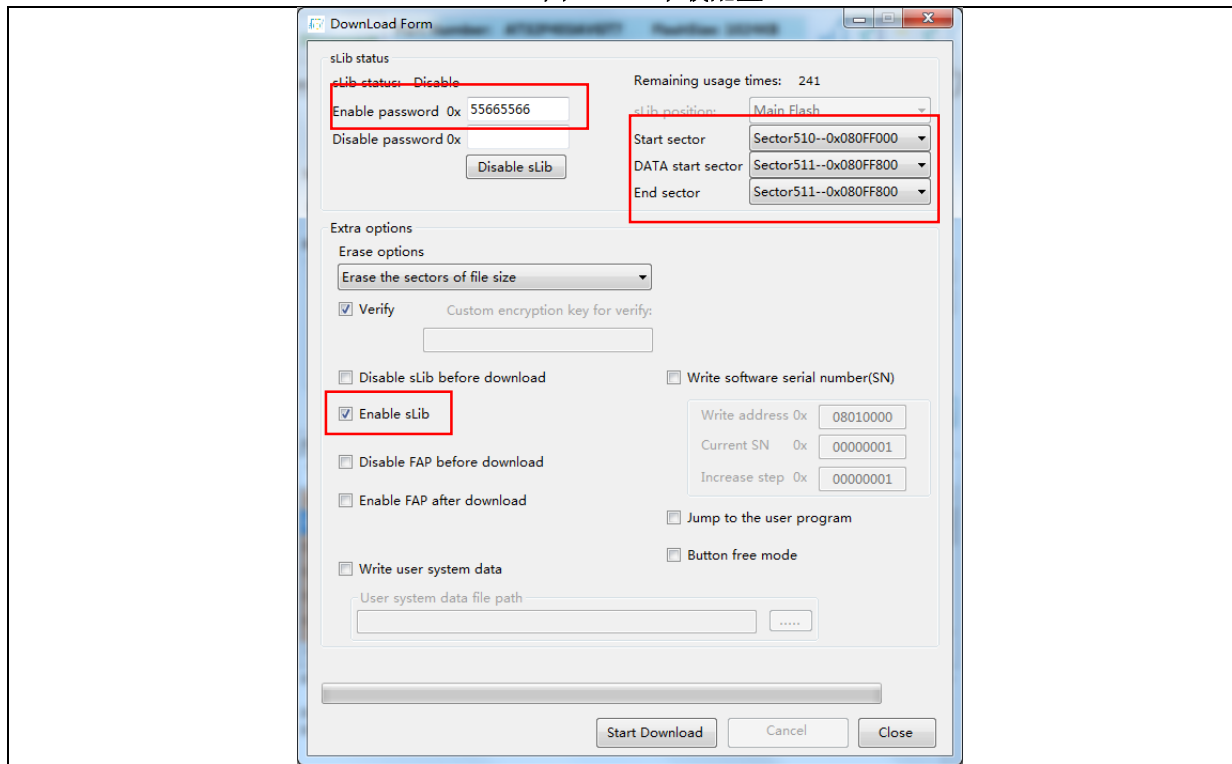
- 1) 添加对应烧录文件：LED.bin 为项目文件，OTP_DATA.bin 为需要保存的 OTP 数据；

图 1. ICP 添加文件



2) 配置对应 slib 参数，开始下载；

图 2. ICP 下载配置



3) 验证 OTP 功能：执行主存储擦除，擦除后读取 OTP 数据存储位置，数据无法擦除，仍然有效。

图 3. 验证结果

Address range:[0x080FF800 0x080FF8FF] checksum: 0x00007F80

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	A5
0x080FF800	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	.
0x080FF810	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	□
0x080FF820	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	!"#
0x080FF830	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	012
0x080FF840	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	@
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

3 版本历史

表 1. 文档版本历史

日期	版本	变更
2022.01.18	2.0.0	最初版本

重要通知 - 请仔细阅读

买方自行负责对本文所述雅特力产品和服务的选择和使用，雅特力概不承担与选择或使用本文所述雅特力产品和服务相关的任何责任。

无论之前是否有过任何形式的表示，本文档不以任何方式对任何知识产权进行任何明示或默示的授权或许可。如果本文档任何部分涉及任何第三方产品或服务，不应被视为雅特力授权使用此类第三方产品或服务，或许可其中的任何知识产权，或者被视为涉及以任何方式使用任何此类第三方产品或服务或其中任何知识产权的保证。

除非在雅特力的销售条款中另有说明，否则，雅特力对雅特力产品的使用和/或销售不做任何明示或默示的保证，包括但不限于有关适销性、适合特定用途（及其依据任何司法管辖区的法律的对应情况），或侵犯任何专利、版权或其他知识产权的默示保证。

雅特力产品并非设计或专门用于下列用途的产品：（A）对安全性有特别要求的应用，例如：生命支持、主动植入设备或对产品功能安全有要求的系统；（B）航空应用；（C）航天应用或航天环境；（D）武器，且/或（E）其他可能导致人身伤害、死亡及财产损害的应用。如果采购商擅自将其用于前述应用，即使采购商向雅特力发出了书面通知，风险及法律责任仍将由采购商单独承担，且采购商应独立负责在前述应用中满足所有法律和法规要求。

经销的雅特力产品如有不同于本文档中提出的声明和/或技术特点的规定，将立即导致雅特力针对本文所述雅特力产品或服务授予的任何保证失效，并且不应以任何形式造成或扩大雅特力的任何责任。

© 2022 雅特力科技 保留所有权利