



life.augmented

STM32 生态系统 第十九期

信息安全 . Information Security

10. SBSFU初体验

2020.03

• 初次体验：基于Nucleo-G0板

- 使用最新版本SBSFU固件包， STM32CubeExpansion_SBSFU_V2.2.0

- 在NUCLEO-G071B工程目录(2_Images), 打开三个工程文件

- 2_Image_SECoreBin ◀

- 2_Image_SBSFU ▶

- 2_Image_UserApp ◀

- 生成三个待用文件

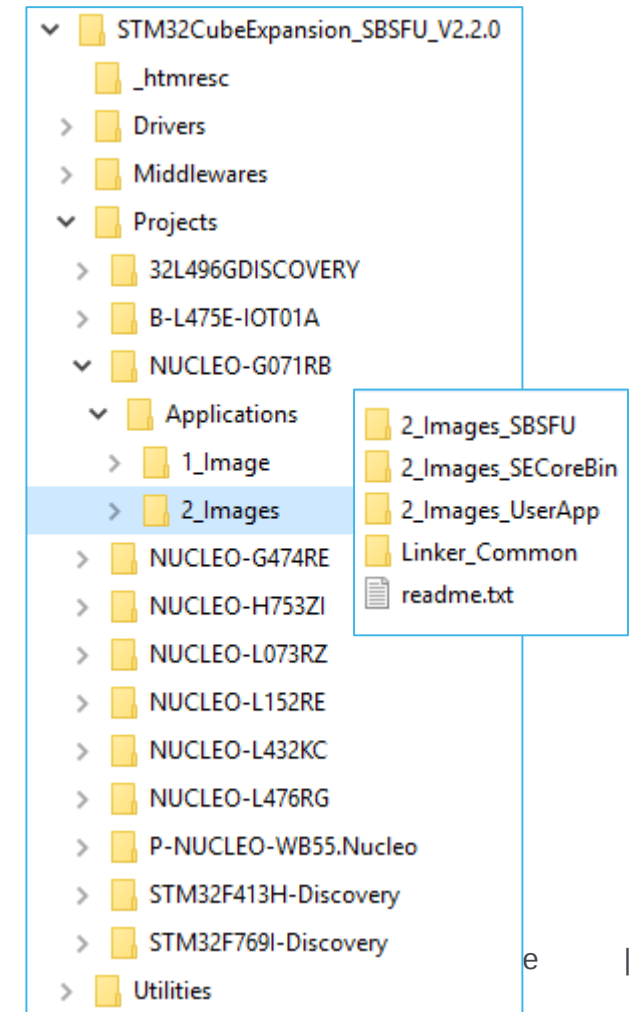
- Project.bin @ 2_Images\2_Images_SBSFU\EWARM\NUCLEO-G071RB\Exe

- UserApp.sfb @ 2_Images\2_Images_UserApp\Binary

- SBSFU_UserApp.bin @ 2_Images\2_Images_UserApp\Binary

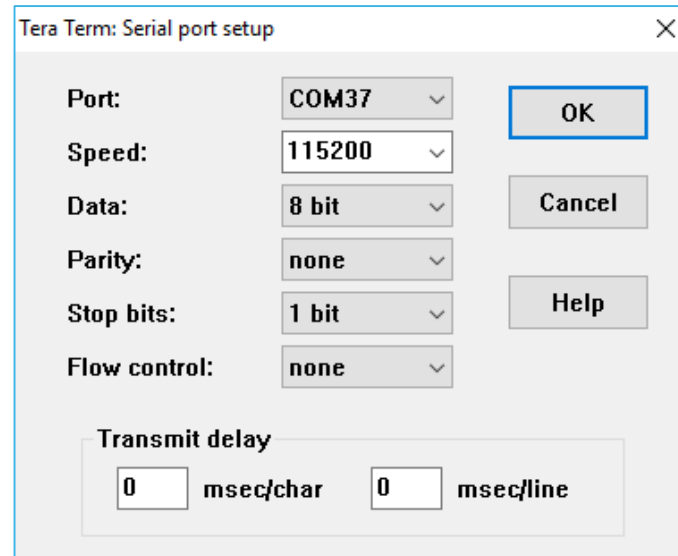


依次编译



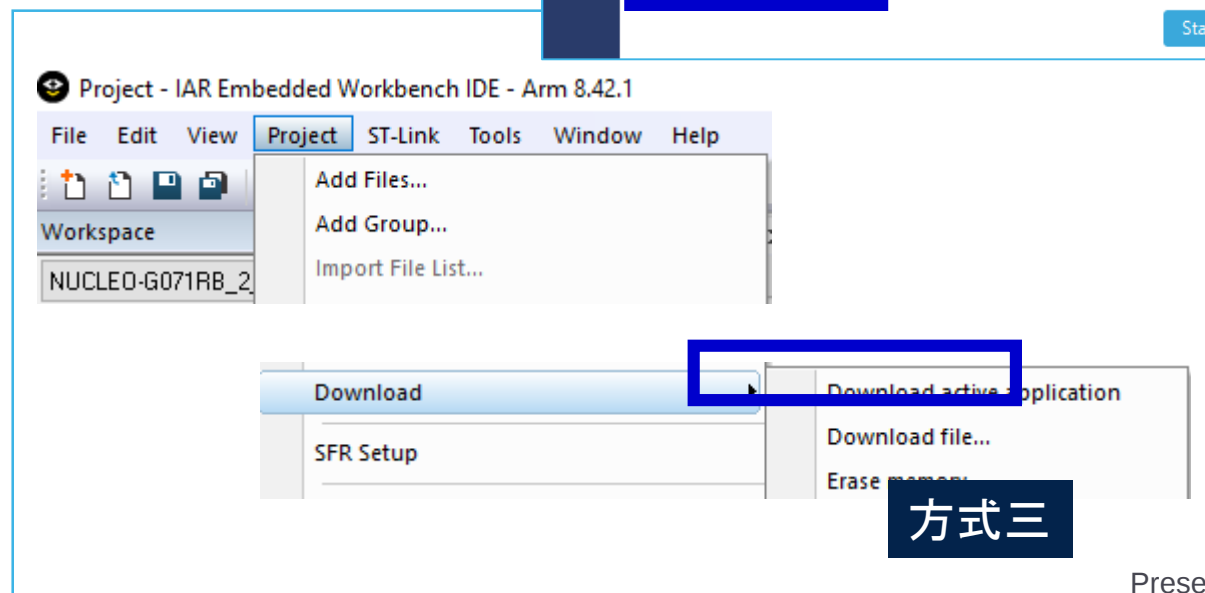
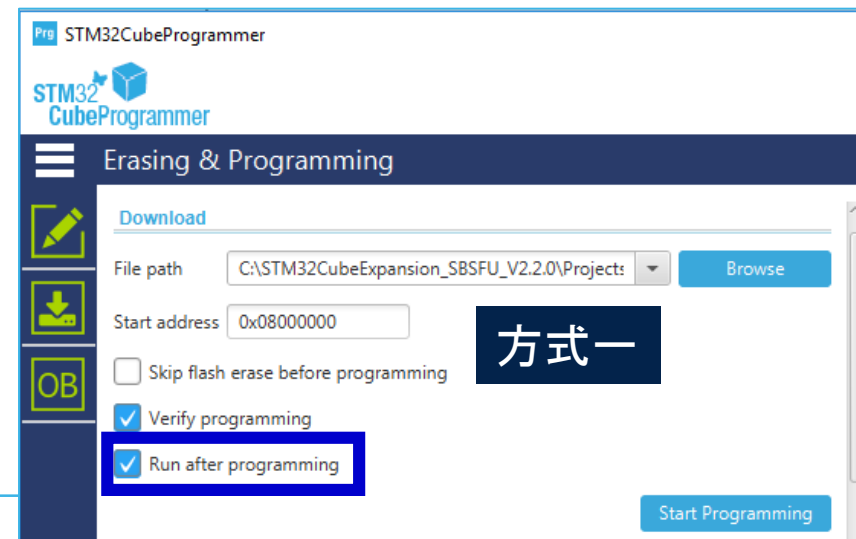
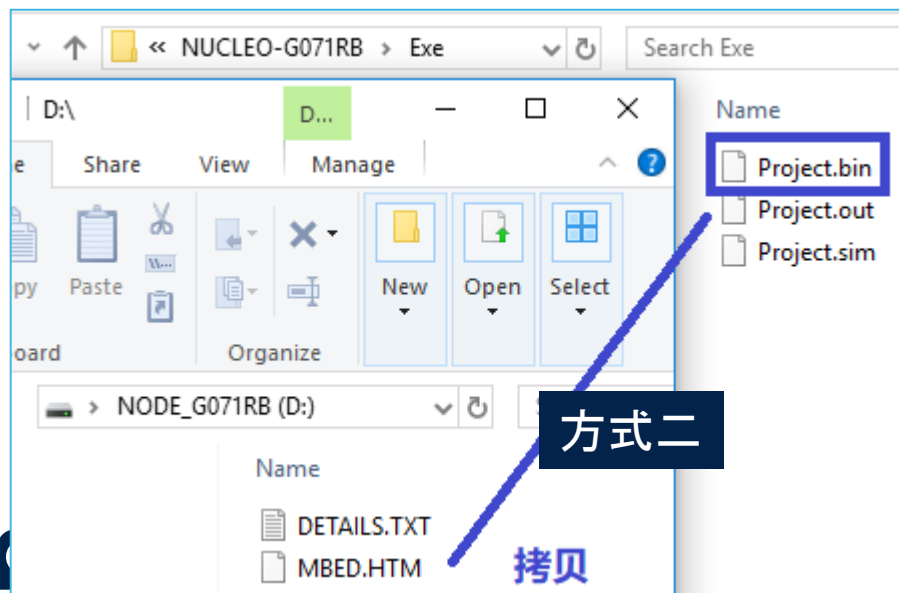
准备工作

- 板子连接电脑，设置好上位机串口工具，参数如下：
 - 该工具需要支持YMODEM协议
 - 波特率 = 115200
 - 数据位 = 8位
 - 校验位，无
 - 停止位 = 1位
 - 流控 = 无
- 通过STM32CubeProgrammer连接板子，恢复芯片的选项字节如下：
 - BOOT_LOCK disable
 - nBOOT_SEL, nBOOT0, nBOOT1 enable
 - WRP disable
 - PCROP disable + PCROP_RDP = 1
 - RDP = 0
 - 芯片处于全片擦除状态



下载SBSFU固件

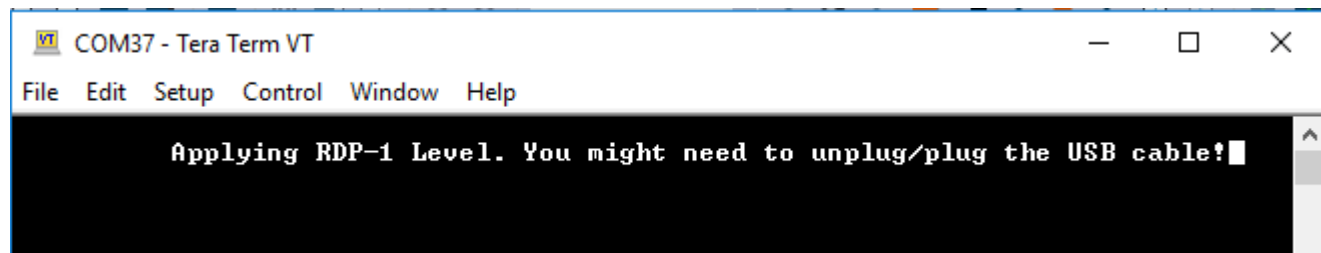
- 下载project.bin到板子（可以采用三个方式）
 - 使用STM32CubeProgrammer下载，并启动运行
 - **Project.bin**直接拖到Nucleo板在“我的电脑”下的盘符中
 - 使用IDE，仅下载程序(不调试)：以IAR为例



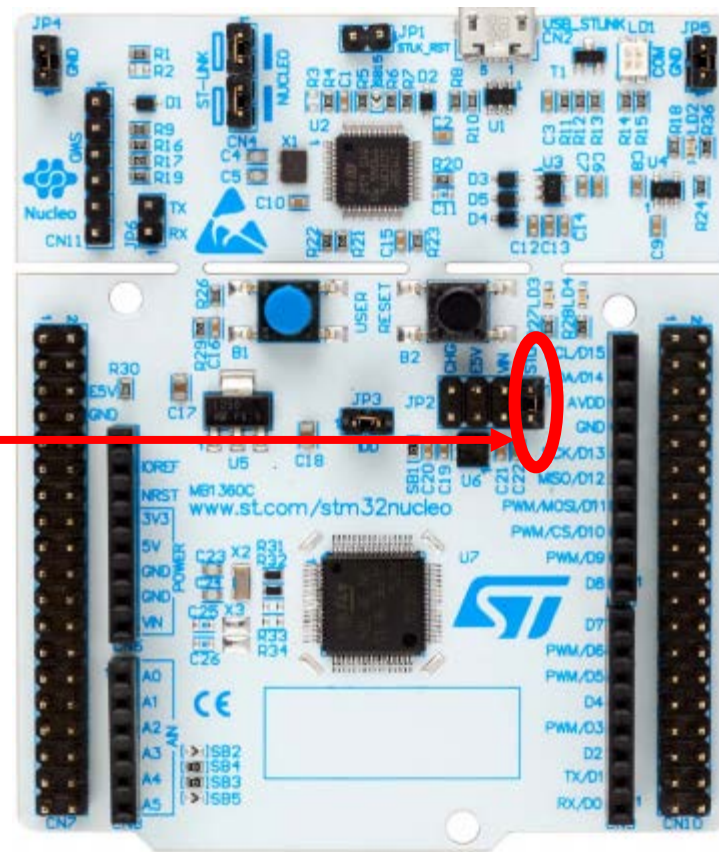


启动SBSFU固件的运行

- 由于代码默认使能了RDP1保护，STM32G0感受到JTAG/SWD连接，会复位



- 解决办法：
 - 不建议重新插拔USB线缆（串口连接已经建立）
 - 重新插拔JP2跳线组中的STLINK供电开关跳线



首次运行SBSFU

```
COM37 - Tera Term VT
File Edit Setup Control Window Help

= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 @: 800e000 / Slot #1 @: 8018000 / Swap @: 8016000

=====
=                                     =
=      <C> COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      Secure Boot and Secure Firmware Update      =
=====

= [SBOOT] STATE: WARNING: SECURE ENGINE INITIALIZATION WITH FACTORY DEFAULT VALUES!
===== End of Execution =====

= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 @: 800e000 / Slot #1 @: 8018000 / Swap @: 8016000

=====
=                                     =
=      <C> COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      Secure Boot and Secure Firmware Update      =
=====

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by Software reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
No valid FW found in the active slot nor new encrypted FW found in the
UserApp download area
Waiting for the local download to start...
= [SBOOT] STATE: DOWNLOAD NEW USER FIRMWARE
File> Transfer> YMODEM> Send .....
```

首次启动，检查系统安全配置，通过

上电后首次进入SBSFU

安全引擎使用默认值初始化BootInfo区域，然后系统重启

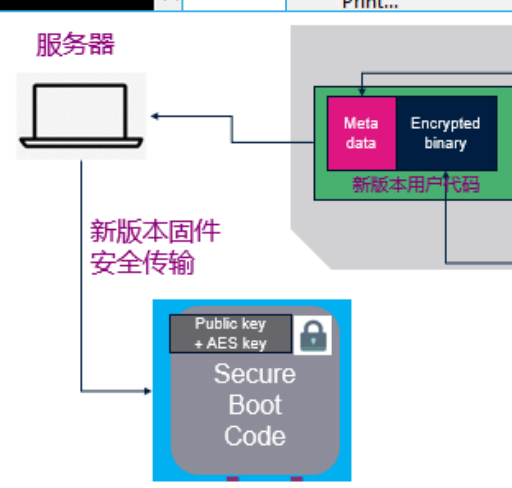
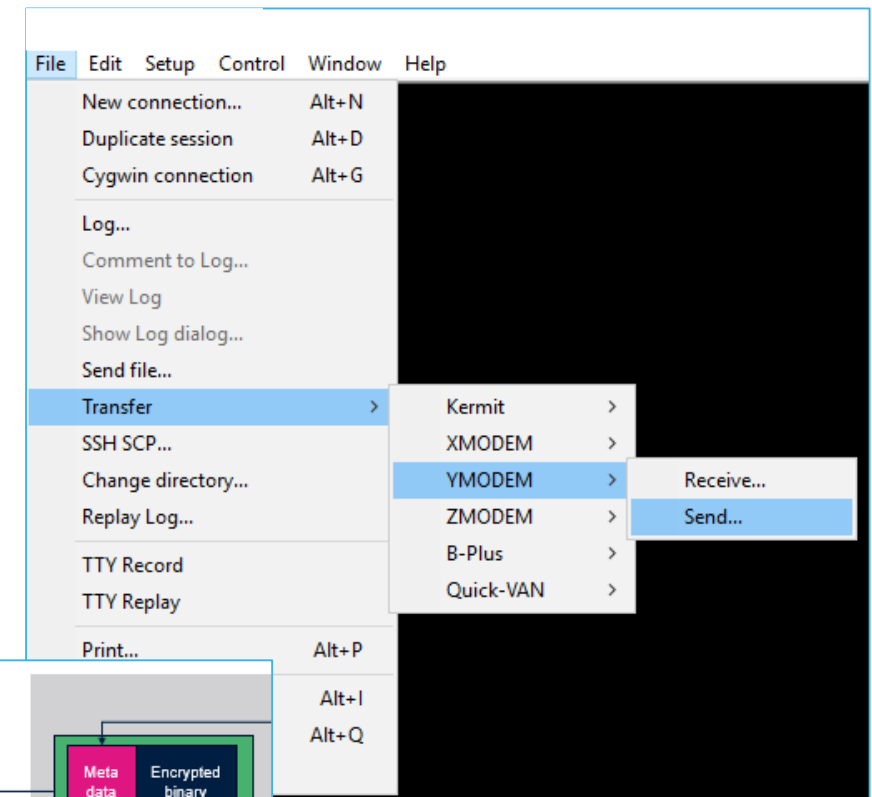
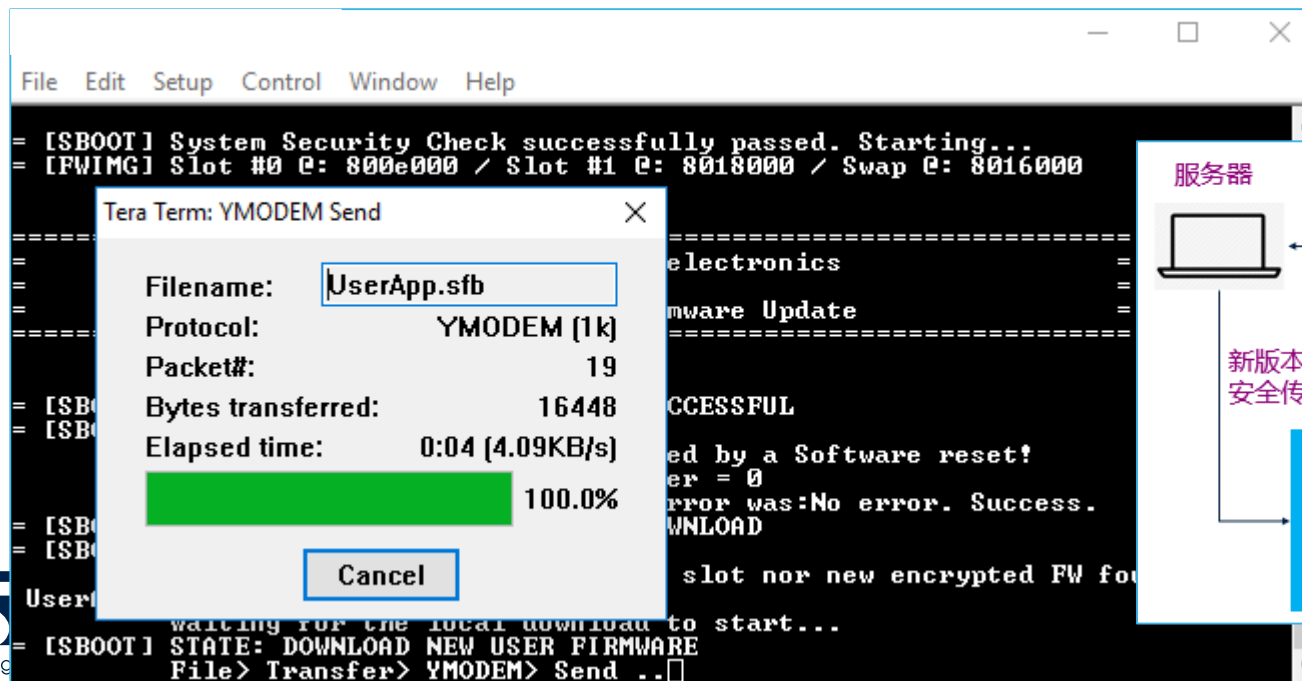
安全引擎，BootInfo区域已经初始化认为SFU启动成功

进入SBSFU状态机，STATE依次轮换

- ▶ 没有检测到用户按键（表示有新固件下载）
- ▶ 没有当前可运行的用户代码，也没有在下载区的代码
- ▶ 等待用户代码的下载

首次下载用户固件

- 使用串口工具的YMODEM协议下载用户固件
- 第三个工程的编译输出文件（用户应用）
 - UserApp.sfb
 - @ 2_Images\2_Images_UserApp\Binary



用户应用运行

进入SBSFU状态机，STATE依次轮换

用户代码下载完毕，重启

进入SBSFU状态机，STATE依次轮换

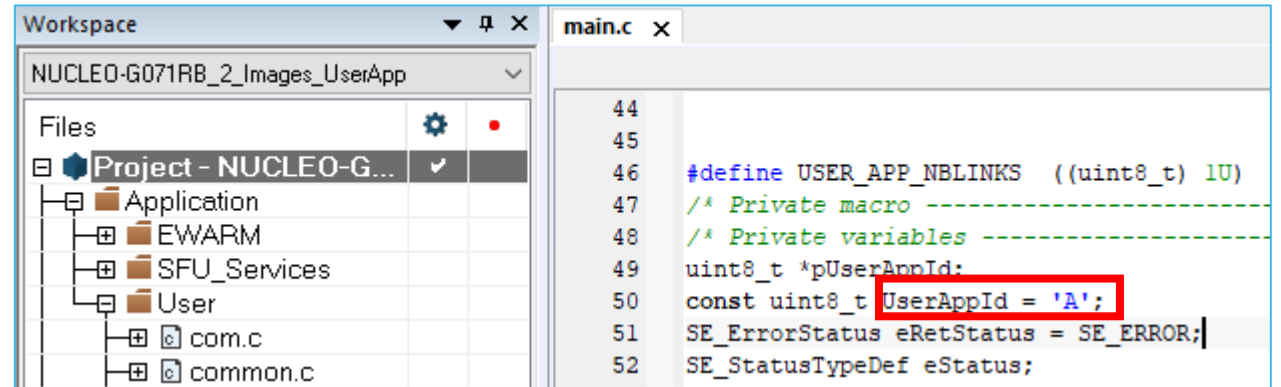
- ▶ 没有检测到用户按键（表示没有新固件下载）
- ▶ 检测到下载区有用户代码密文
- ▶ 安装该用户代码（slot0为空）
- ▶ 对该用户代码进行认证（核实签名）
- ▶ 认证通过，启动该用户代码

进入用户代码执行（版本#A）

- ▶ 展示菜单栏如下...

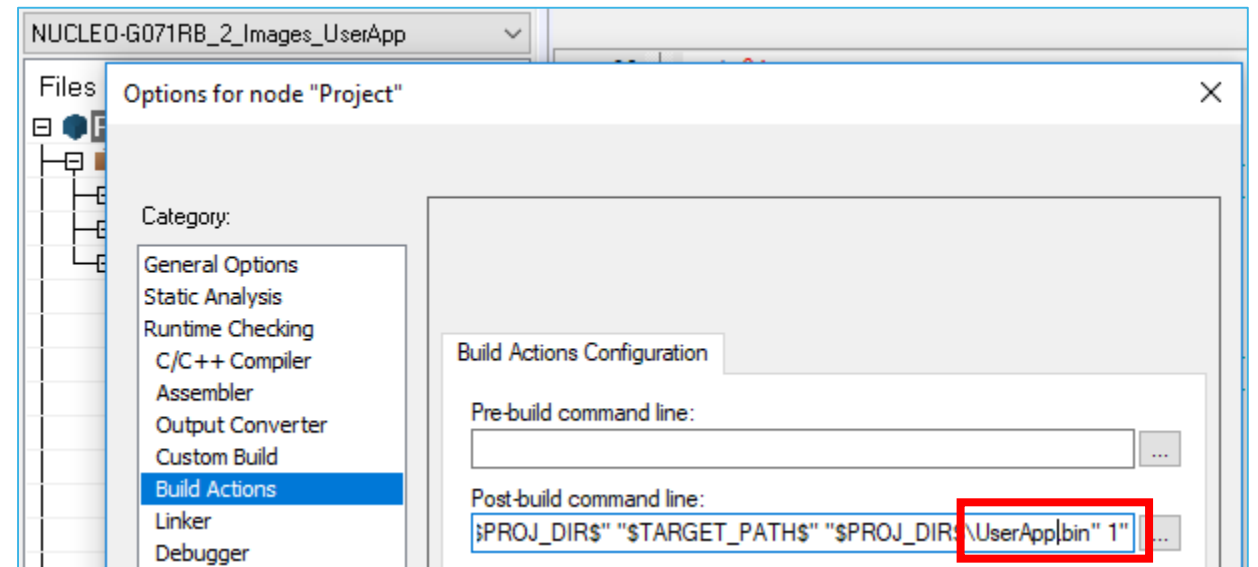
生成新版本用户应用代码

- 修改UserApp项目，main.c如下代码
 - UserAppId = 'B'
- 修改UserApp项目
 - Build action → Post-build
 - UserApp.bin" 2"
- 重新编译
 - 生成UserApp.sfb
 - @ 2_Images\2_Images_UserApp\Binary



The screenshot shows the IDE workspace with the project 'NUCLEO-G071RB_2_Images_UserApp' selected. The 'Files' pane on the left shows the project structure: Application, EWARM, SFU_Services, User, com.c, and common.c. The 'main.c' file is open in the editor, showing the following code:

```
44  
45  
46 #define USER_APP_NBLINKS ((uint8_t) 1U)  
47 /* Private macro -----  
48 /* Private variables -----  
49 uint8_t *pUserAppId;  
50 const uint8_t UserAppId = 'A';  
51 SE_ErrorStatus eRetStatus = SE_ERROR;  
52 SE_StatusTypeDef eStatus;
```



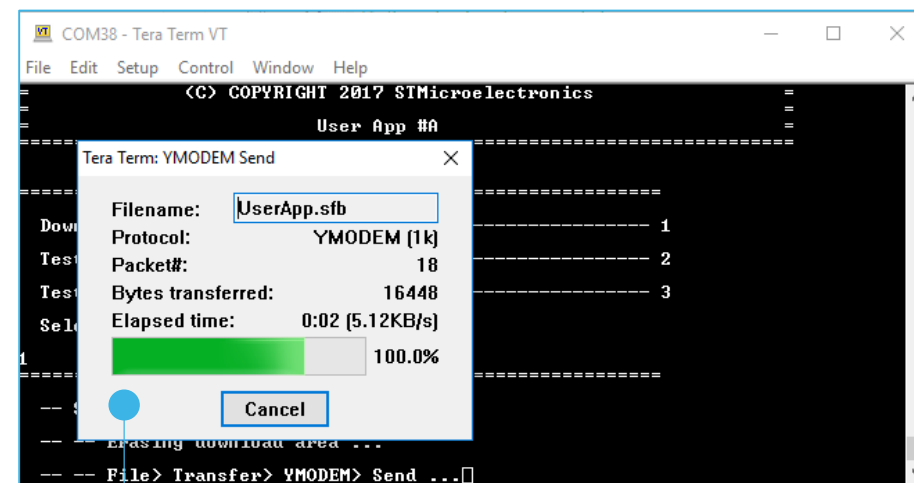
从用户程序(版本A)下载新用户程序(版本B)

```
=====
(C) COPYRIGHT 2017 STMicroelectronics
=====
User App #A
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Selection :

1
===== New Fw Download =====

-- Send Firmware
-- -- Erasing download area ...
-- -- File> Transfer> YMODEM> Send ...
-- -- Programming Completed Successfully!
-- -- Bytes: 16448
-- Image correctly downloaded - reboot
```



进入用户代码执行 (版本#A)
▶ 选择1, 下载新版本 (版本#B) 用户程序...

使用串口终端的YMODEM协议传输用户固件 (到Slot#1)

下载完毕, 重启

重启后运行新版本用户程序(版本B)

```
[SBOOT] System Security Check successfully passed. Starting...
[FWIMG] Slot #0 @: 800e0000 / Slot #1 @: 80180000 / Swap @: 80160000

=====
<C> COPYRIGHT 2017 STMicroelectronics
Secure Boot and Secure Firmware Update
=====

[SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
[SBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Software reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was: No error. Success.
[SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
[SBOOT] STATE: CHECK USER FW STATUS
New Fw Encrypted, to be decrypted
[SBOOT] STATE: INSTALL NEW USER FIRMWARE ←
Image preparation done.
Swapping the firmware images...
[SBOOT] STATE: VERIFY USER FW SIGNATURE
[SBOOT] STATE: EXECUTE USER FIRMWARE

=====
<C> COPYRIGHT 2017 STMicroelectronics
User App #B
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Selection :
```

进入SBSFU状态机，STATE依次轮换

- ▶ 没有检测到用户按键（表示没有新固件下载）
- ▶ 检测到下载区有用户代码密文
- ▶ 安装该用户代码（slot0有旧代码，需要swap）
- ▶ 对该用户代码进行认证（核实签名）
- ▶ 认证通过，启动该用户代码

进入用户代码执行（版本#B）

- ▶ 展示菜单栏如下...

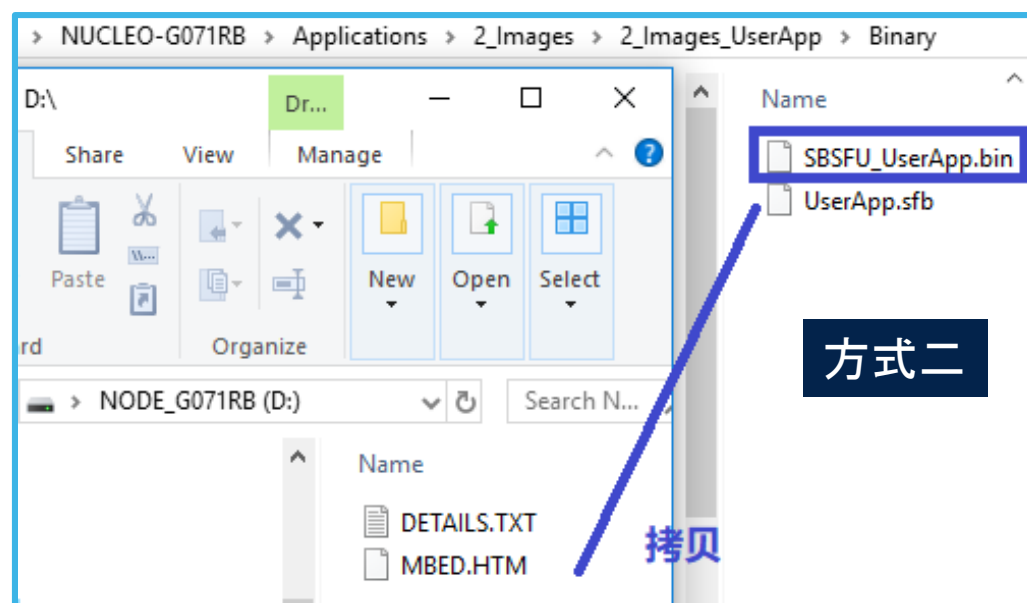
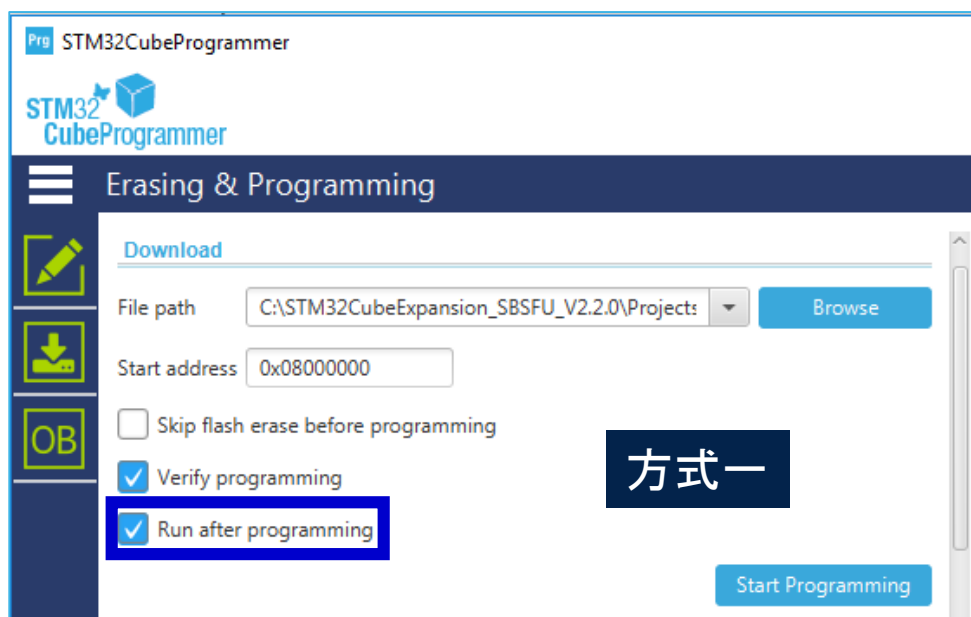
同时下载sbsfu和初始用户代码

准备工作

- 通过STM32CubeProgrammer连接板子，恢复芯片的选项字节如下：
 - RDP = 0
 - PCROP disable
 - WRP disable
 - BOOT_LOCK disable
 - nBOOT_SEL enable
 - 芯片处于全片擦除状态
- 修改UserApp项目，main.c如下代码
 - UserAppId = "C";
- 修改UserApp项目
 - Build action → Post-build
 - UserApp.bin" 3"
- 重新编译得到
 - UserApp.sfb 和 SBSFU_UserApp.bin
 - @ 2_Images\2_Images_UserApp\Binary

下载SBSFU_UserApp.bin

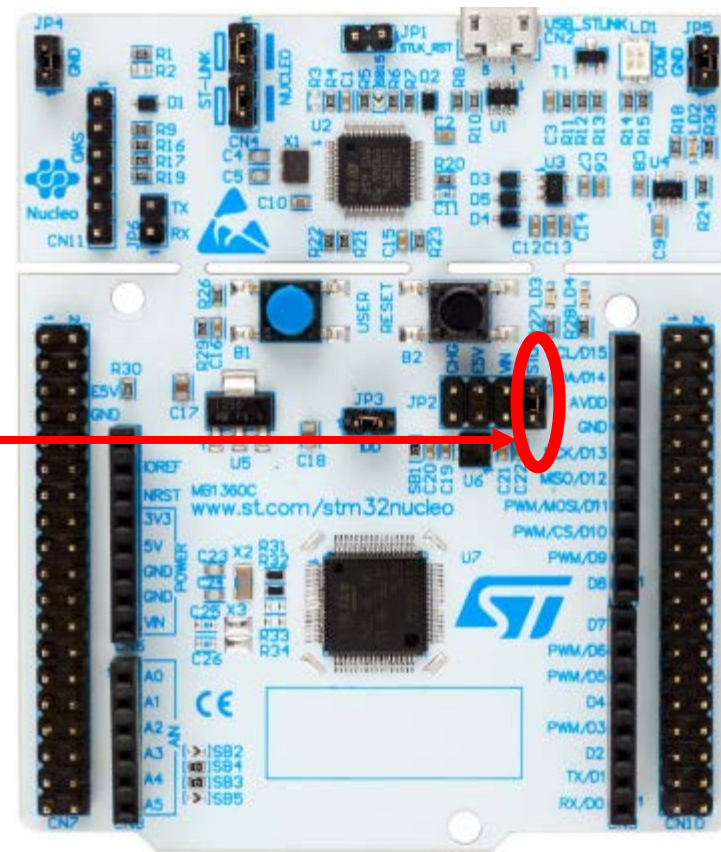
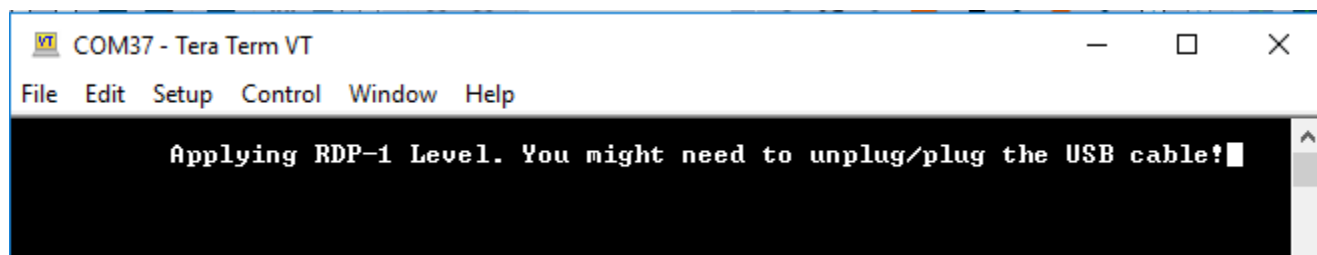
- 下载SBSFU_UserApp.bin到板子（可以采用两个个方式）
 - 使用STM32CubeProgrammer下载，并启动运行
 - SBSFU_UserApp.bin直接拖到Nucleo板代表的盘符中





启动SBSFU_UserApp.bin的运行

- 由于代码默认使能了RDP1保护，STM32G0感受到JTAG/SWD连接，会复位
- 解决办法：
 - 不建议重新插拔USB线缆（串口连接已经建立）
 - 重新插拔JP2跳线组中的STLINK供电开关跳线



下载SBSFU_UserApp.bin后，启动

```
= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 0: 800e000 / Slot #1 0: 8018000 / Swap 0: 8016000

=====
=                                     =
=      (C) COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      Secure Boot and Secure Firmware Update      =
=====

= [SBOOT] STATE: WARNING: SECURE ENGINE INITIALIZATION WITH FACTORY DEFAULT VALU
ES!
===== End of Execution =====

= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 0: 800e000 / Slot #1 0: 8018000 / Swap 0: 8016000

=====
=                                     =
=      (C) COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      Secure Boot and Secure Firmware Update      =
=====

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Software reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was:No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
A valid FW is installed in the active slot - version: 3
= [SBOOT] STATE: VERIFY USER FW SIGNATURE
= [SBOOT] STATE: EXECUTE USER FIRMWARE

=====
=                                     =
=      (C) COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      User App #C      =
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Selection :
```

复位后首次进入SBSFU

安全引擎，初始化BootInfo区域
认为SFU启动失败，系统重启

安全引擎，BootInfo区域已经初始化
认为SFU启动成功

进入SBSFU状态机，STATE依次轮换

- ▶ 没有检测到用户按键（表示没有新固件下载）
- ▶ 检测到slot0已安装有用户代码（版本3）
- ▶ 对该用户代码进行认证（核实签名）
- ▶ 认证通过，启动该用户代码

进入用户代码执行（版本#C）

- ▶ 展示菜单栏如下...

从SBSFU下载新用户程序(版本D)

- 按着用户按键，同时复位Nucleo板

```
= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 C: 800e000 / Slot #1 C: 8018000 / Swap C: 8016000

=====
<C> COPYRIGHT 2017 STMicroelectronics
=====
Secure Boot and Secure Firmware Update
=====

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Hardware reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: DOWNLOAD NEW USER FIRMWARE
File> Transfer> YMODEM> Send ...
= [SBOOT] STATE: REBOOT STATE MACHINE
===== End of Execution =====
```

进入SBSFU状态机，STATE依次轮换

- ▶ 检测到用户按键（表示有新固件下载）
- ▶ 下载新固件，从YMODEM
- ▶ 下载完毕，系统重启

```
= [SBOOT] System Security Check successfully passed. Starting...
= [FWIMG] Slot #0 C: 800e000 / Slot #1 C: 8018000 / Swap C: 8016000

=====
<C> COPYRIGHT 2017 STMicroelectronics
=====
Secure Boot and Secure Firmware Update
=====

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Software reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
New Fw Encrypted, to be decrypted
= [SBOOT] STATE: INSTALL NEW USER FIRMWARE
Image preparation done.
Swapping the firmware images...
= [SBOOT] STATE: VERIFY USER FW SIGNATURE
= [SBOOT] STATE: EXECUTE USER FIRMWARE

=====
<C> COPYRIGHT 2017 STMicroelectronics
=====
User App #D
=====
```

进入SBSFU状态机，STATE依次轮换

- ▶ 没有检测到用户按键（表示没有新固件下载）
- ▶ slot1有加密固件下载好了
- ▶ 安装新固件（slot0已经有固件，需要swap）
- ▶ 对该用户代码进行认证（核实签名）
- ▶ 认证通过，启动该用户代码（版本#D）

谢 谢

© STMicroelectronics - All rights reserved.

The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.

