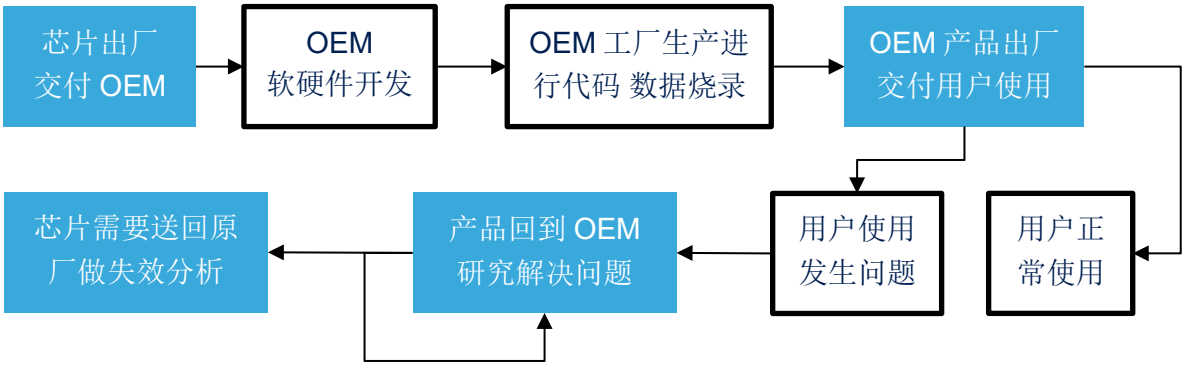
STM32U5 带 OEM Key 保护的 RDP 降级

关键字：读保护，RDP，调试保护，OEMKey

1. 引言

通常芯片在其整个生命周期中跟随产品的开发生产可能经历如下几个不同阶段：



在不同的生命周期阶段需要对芯片资源有不同的访问权限，例如芯片出厂时要开放所有资源供 OEM 进行开发，工厂生产烧录代码和数据后需要关闭某些资源的访问，确保代码与数据的安全性，设备回厂返修时需要再次允许某些资源的访问等等。

STM32MCU 的硬件中能够用来进行芯片生命周期管理的最常见的特性就是 RDP（Read Out Protection）读保护功能。通常 RDP 具有三个级别：

- Level0：完全开放，这是芯片出厂的缺省状态
- Level1：调试端口可以连接，但无法通过调试端口访问内部 Flash，部分 SRAM 以及其它一些资源，OptionByte 可以修改。Level1 可以降级回 Level0，但会伴随全片擦除。
- Level2：调试端口永久关闭，进入这种状态后调试端口完全无法访问，且这种状态无法逆转。

在 RDP Level1 调试端口依旧可以连接，虽然不能直接读取内部 Flash 的代码和数据，但是可以看到大部分 SRAM 的内容，并且 RDP Level1 允许随意回退到 Level0，并伴随全片擦除。因而从安全角度讲 Level1 这个级别的安全性不够高，因而通常对于调试端口保护我们会推荐使用 RDP Level2，但是 OEM 可能往往不会选择使用这个级别，原因有多方面，其中一部分的顾虑可能来自两方面，一个是 Level2 级别下 OptionByte 无法进行修改，另一个是设置到 Level2 级别会影响芯片失效分析。

STM32L5 在 RDP 功能上带来一些改变，首先针对 TrustZone 架构，增加了 Level0.5，

- Level0.5：调试端口可以连接，但是安全测的所有调试功能都被禁止，非安全测的调试功能依旧可以使用，因此在 RDP Level0.5 可以访问被定义为 NonSecure 的部分资源，包括片上 Flash，SRAM，部分 CPU 寄存器以及系统外设等

另外，STM32L5 的 RDP Level2 不影响 FA，但 OEM 依旧无法在这种状态下进行 RDP 降级或者 OptionByte 修改，依旧有一些局限性。

2. STM32U5 芯片生命周期管理新特性

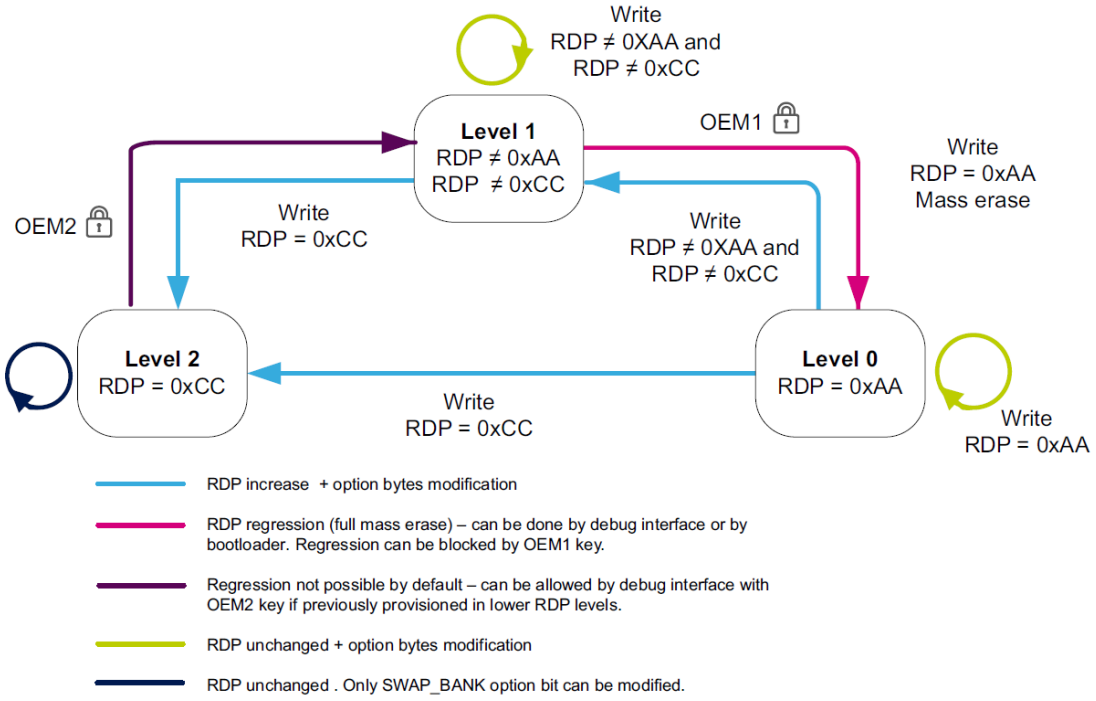
STM32U5 在芯片生命周期管理方面在 STM32L5 的基础做了进一步的改进，引入了 OEM Key 机制，使得 RDP 的级别状态转换能够通过 OEM 设置的 password 进行保护，一方面能够防止 RDP 任意降级，避免设备被远程攻击注入恶意代码后通过 RDP 降级变砖的风险，另一方面也使得 RDP2 降级成为可能，给产品后期维护带来更多的灵活性。

2.1. STM32U5 RDP 读保护级别状态转换

2.1.1. TrustZone 未使能 TZEN=0

芯片出厂缺省状态 TrustZone 没有使能，这时候和往常一样 RDP 依旧具有 3 个级别，如图 1 所示：

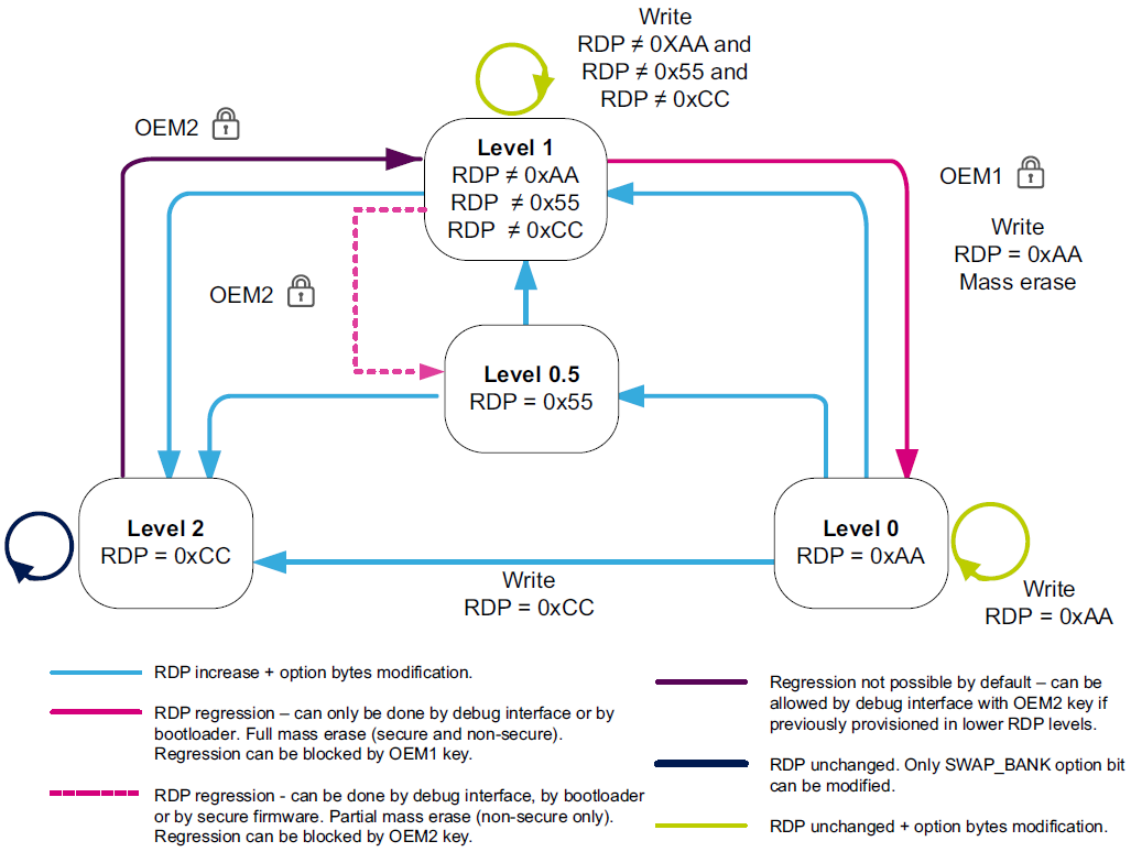
图1. STM32U5 TZEN=0 时 RDP 级别及其状态转换



2.1.2. TrustZone 未使能 TZEN=1

当选项字节中的 TZEN 被设置为 1，系统的 TrustZone 功能被使能，此时 RDP 将具有 4 个级别，如图 2 所示：

图2. STM32U5 TZEN=0 时 RDP 级别及其状态转换



3. STM32U5 OEM Key 机制

3.1. OEM1Key 与 OEM2Key

客户可以自己定义并分别烧写两组 OEM Key，每组 Key 都有 64bit，有效的 Key 值必须是非全 0 或非全 1 的值。

- OEM1Key：
  - 用于控制 RDP Level1 到 Level0 的降级
  - 一旦写入 OEM1Key，则 OEM1 处于 LOCK 状态，必须首先使用 OEM1Key 解锁后才能够进行 RDP 降级。
  - 解锁的过程需要将 OEM1Key 的 64bit 值的两个 32bit 分两次通过 JTAG 或者 SWD 端口写入 **DBGMCU_DBG_AUTH_HOST** 寄存器。如果
  - 如果 OEM1Key 未设置，则 RDP Level1 到 Level0 的降级没有限制
- OEM2Key：
  - 用于使能并保护 RDP Level2 到 RDP Level1 的降级。只有写入有效的 OEM2Key 之后，才有可能进行 RDP Level2 到 RDP Level1，且类似的，降级时必须首先使用 OEM2Key 解锁。
  - 在 TZEN=1 情况下 OEM2Key 同时保护 RDP Level1 到 RDP0.5 的降级

- 如果芯片从未写入有效的 OEM2Key，那么 RDP Level2 的效果与旧系列的 STM32 的行为一致，无法 FA，无法撤销。

如果芯片设置了 OEM2Key 和 RDP Level2 需要做 FA，则客户需要首先将芯片进行 RDP2 解锁降级之后再送交 FA。

3.2. OEM1Key 与 OEM2Key 的设置修改条件

OEM1Key 和 OEM2Key 的设置和修改是有条件的，并非在芯片的所有状态下都允许 OEMKey 的设置，表 1 总结了哪些情况下允许对 OEM1Key 和 OEM2Key 进行修改。

表1. OEM1Key 与 OEM2Key 的修改条件

Key 是否允许修改	RDP 0	RDP 0.5		RDP 1		RDP 2
		Key 尚未设置 (unlock)	Key 已经设置 (locked)	Key 尚未设置 (unlock)	Key 已经设置 (locked)	
OEM1 Key	总是允许	允许	不允许	允许	不允许	不允许
OEM2 Key	总是允许	允许	允许	允许	不允许	不允许

4. 如何使用 STM32U5 的 OEM Key 功能

4.1. 检查 OEMxKey 是否已经设置

由于 OEM Key 并非在任意情况下都允许修改，而且 OEM Key 一旦设置无法撤销，并且会影响 RDP 降级，因而**强烈建议在设置 RDP 到非 0 级别之前，首先检查 OEM Key 在所使用的开发板、芯片上是否已经设置**。

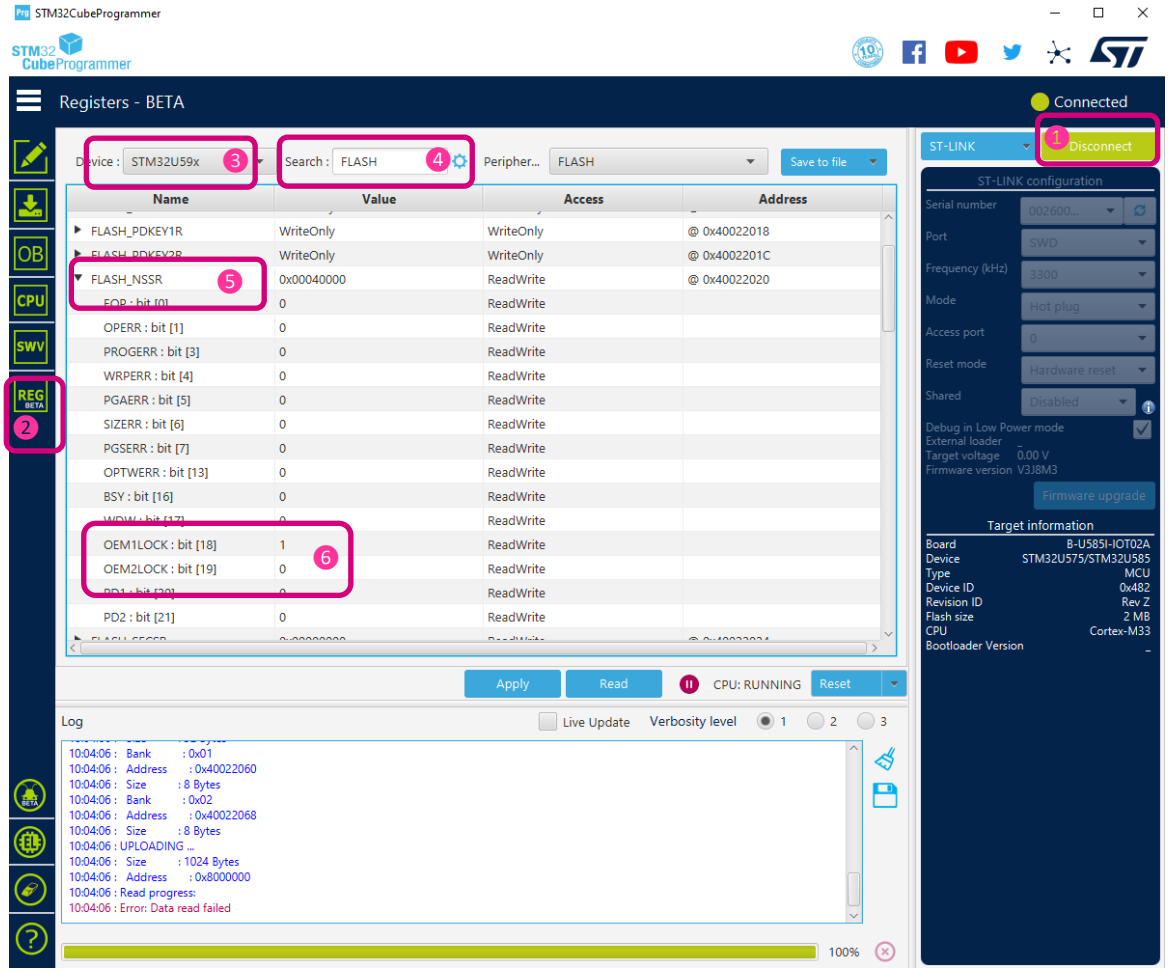
如果 OEM Key 曾经被设置过，如果不能确认之前设置的 KEY 的值，那么我们建议在 RDP 为 Level0 的时候，对 OEM Key 进行重新配置，这样可以保证新设置的 KEY 是自己确认知道的值。

如果该芯片尚未设置过 OEM Key，那么可以根据需要选择是否要进行 KEY 的设置。

检查 OEM Key 是否已经设置过，可以通过查看 FLASH 的 NSSR 寄存器来实现，即可以通过软件代码读取，也可以通过 STM32CubeProgrammer 读取。使用 STM32CubeProgrammer 来读取 NSSR 的方法更加简单直接。步骤如图 3 所示

- 打开 STM32CubeProgrammer（建议版本 v2.8.0 及以上）
- 点击 Connect 连接芯片
- 根据使用的具体芯片在 REG 页面中选择 Device
- 在 Search 框中填入 FLASH 并回车，这时候将看到 FLASH 寄存器的内容
- 点击 FLASH_NSSR 左边小三角，展开 NSSR 寄存器内容
- 查看 OEM1LOCK，OEM2LOCK bit 的值
  - 1：表示该 KEY 已经设置，在图 3 的例子中 OEM1Key 已经设置
  - 0：表示该 KEY 从未被设置过，在图 3 的例子中 OEM2Key 未设置

图3. 通过 STM32CubProgrammer 查看 OEM1/OEM2 Key 设置情况示例



4.2. 设置 OEM1Key 和 OEM2Key

OEMxKey 的设置是通过操作 Flash 选项字节对应的 OEM Key 寄存器实现的

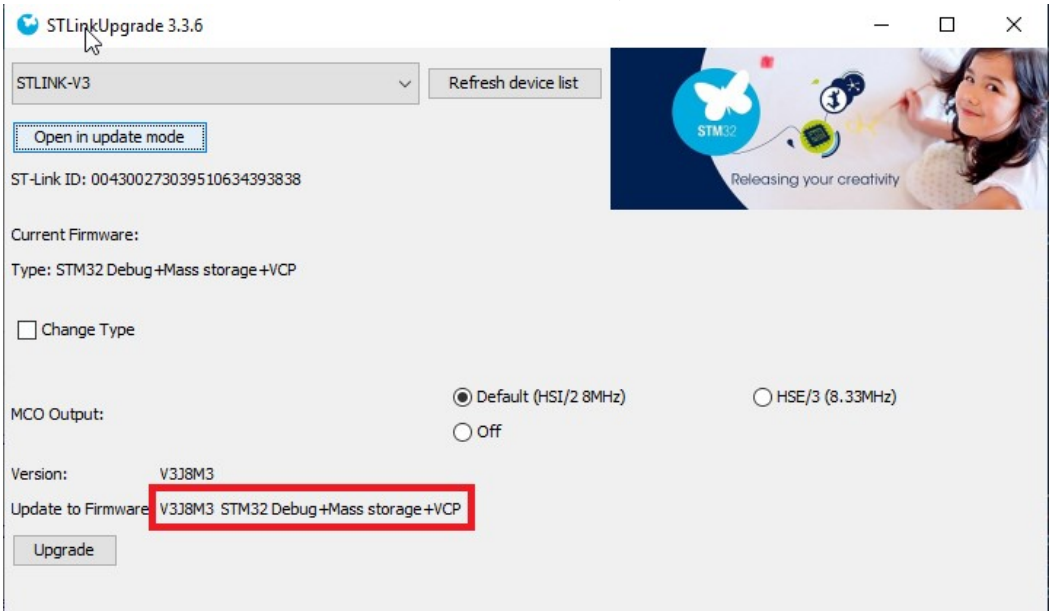
- OEM1Key：**FLASH OEM1 key register 1 & FLASH OEM1 key register 2**
- OEM2Key：**FLASH OEM2 key register 1 & FLASH OEM2 key register 2**

这个操作可以通过两种方式实现，一种方法是使用 STM32CubeProgrammer CLI 命令完成，另一种方法是通过软件代码实现。

注意：

1. OEMxKey 不能设置为全 0 或者全 1 的值
2. OEMx2Key 一旦成功写入，无法通过读取相应的 OptionByte 获取，且在不可修改的 RDP Level 将无法重新设置，所以写入的 OEM Key 要确认 Key 保存好并记牢
3. 如果没有成功设置 OEM2Key，则 RDP Level2 无法回退，无法进行 FA
4. 如果客户设置了 RDP Level2 并需要对芯片做 FA，则需要客户首先使用 OEM2Key 将芯片解锁并进行 RDP Level2 降级到 RDP level1，否则无法进行失效分析
5. STM32CubeProgrammer 的版本建议 v2.8.0 或以上
6. STLink FW 需要更新到 V3J8M3 或以上版本，如图 4 所示

图4.　STLINK FW 版本



4.2.1. 使用 STM32CubeProgrammer CLI 命令设置 OEMxKey

通过 STM32CubeProgrammerCLI 命令设置 OEM1/2Key 的示例

```
STM32_Programmer_CLI -c port=swd mode=hotplug -lockRDP1 0x12345678 0xDEADBEEF

STM32_Programmer_CLI -c port=swd mode=hotplug -lockRDP2 0xFACEB00C 0xDEADBABE
```

4.2.2. 通过软件代码设置 OEMxKey

以下是通过软件代码设置 OEM1/2Key 的示例，这个例子中我们在 RDP 为 Level0 的条件下设置 OEMxKey。实际使用中代码可以根据实际需求结合 **Error! Reference source not found.**的内容决定在哪种 RDP 级别下允许修改 OEMxKey。

```
#define OEM1KEY_WORD_1 ((uint32_t)0x12345678)
#define OEM1KEY_WORD_2 ((uint32_t)0xDEADBEEF)
#define OEM2KEY_WORD_1 ((uint32_t)0xFACEB00C)
#define OEM2KEY_WORD_2 ((uint32_t)0xDEADBABE)

FLASH_OBProgramInitTypeDef OptionsBytesInit;

/**
  * @brief Function to set and lock OEM1 key
  * @param key1: OEM1 key part 1
  * @param key2: OEM1 key part 2
  */
static void OB_Test_SetOEM1Key(uint32_t key1, uint32_t key2)
{
	OptionsBytesInit.OptionType = OPTIONBYTE_RDP;
	HAL_FLASHEx_OBGetConfig(&OptionsBytesInit);

	if (OptionsBytesInit.RDPLevel == 0xAA)
	{
		HAL_FLASH_Unlock();
		HAL_FLASH_OB_Unlock();
```

```
                OptionsBytesInit.OptionType = OPTIONBYTE_RDPKEY;
                OptionsBytesInit.RDPKeyType = OB_RDP_KEY_OEM1;
                OptionsBytesInit.RDPKey1 = key1;
                OptionsBytesInit.RDPKey2 = key2;

                HAL_FLASHEx_OBProgram(&OptionsBytesInit);
                HAL_FLASH_OB_Launch();
        }
}
/**
* @brief Function to set and lock OEM2 key
* @param key1: OEM2 key part 1
* @param key2: OEM2 key part 2
*/
static void OB_Test_SetOEM2Key(uint32_t key1, uint32_t key2)
{
        OptionsBytesInit.OptionType = OPTIONBYTE_RDP;
        HAL_FLASHEx_OBGetConfig(&OptionsBytesInit);

        if (OptionsBytesInit.RDPLevel == 0xAA)
        {
                HAL_FLASH_Unlock();
                HAL_FLASH_OB_Unlock();
                OptionsBytesInit.OptionType = OPTIONBYTE_RDPKEY;
                OptionsBytesInit.RDPKeyType = OB_RDP_KEY_OEM2;
                OptionsBytesInit.RDPKey1 = key1;
                OptionsBytesInit.RDPKey2 = key2;
                printf("Program OB\r\n");
                HAL_FLASHEx_OBProgram(&OptionsBytesInit);
                printf("Launch OB\r\n");
                HAL_FLASH_OB_Launch();
        }
}
```

4.3. 使用 OEM Key 解锁并进行 RDP 降级

当 OEM1/2 Key 成功设置之后，对应的 RDP 降级需要配合 OEM1/2 Key 的解锁之后才能够完成。

注意：

1. 通过 OEMxKey 解锁+RDP 降级只能通过 JTAG/SWD 端口完成，无法通过软件进行 OEMxKey 解锁

   如果系统使能了 TrustZone，当 RDP 为非 Level0 状态时，缺省上电 Debug 端口就处于禁止状态，需要首先确保片上代码能够正常运行到 NonSecure 代码才能允许 Debug 连接，否则即使有 OEMxKey，也无法解锁降级。

4.3.1. TrustZone 未使能（TZEN=0）RDP1 解锁降级到 RDP0

通过 STM32CubeProgrammerCLI 命令使用 OEM1Key 解锁后做 RDP 降级的示例

- 方法一：分两步，先 OEM1Key 解锁，后 RDP 降级

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0x12345678 0xDEADBEEF

STM32_Programmer_CLI -c port=swd mode=hotplug -ob RDP=0xAA
```

解锁降级回退过程将会在 cmd 窗口看到类似如下打印信息

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0x12345678 0xDEADBEEF
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.30V
SWD freq    : 24000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.30V
SWD freq    : 1000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0xd0
Debug in Low Power mode enabled


Unlock RDP1 password successfully done

STM32_Programmer_CLI -c port=swd mode=hotplug -ob RDP=0xAA
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.30V
SWD freq    : 24000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.30V
SWD freq    : 1000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
```

```
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x20
Debug in Low Power mode enabled


UPLOADING OPTION BYTES DATA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[████████████████████████████████████████████████] 100%

  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes

[████████████████████████████████████████████████] 100%


PROGRAMMING OPTION BYTES AREA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[                                                ]

Reconnecting...
Reconnected !


UPLOADING OPTION BYTES DATA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[████████████████████████████████████████████████] 100%

  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes

[████████████████████████████████████████████████] 100%

OPTION BYTE PROGRAMMING VERIFICATION:

Option Bytes successfully programmed
```

- 方法二：一条命令同时解锁和降级

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0x12345678 0xDEADBEEF -ob
RDP=0xAA
```

4.3.2. TrustZone 未使能（TZEN=0）RDP2 解锁降级到 RDP1

通过 STM32CubeProgrammerCLI 命令使用 OEM2Key 解锁后做 RDP 降级的示例

- OEM2Key 解锁后，硬件将自动把 RDP 降级为 Level1，RDP 的值为 0xFF，不需要额外的命令进行降级

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP2 0xFACEB00C 0xDEADBABE
```

解锁降级回退过程将会在 cmd 窗口看到类似如下打印信息

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP2 0xFACEB00C 0xDEADBABE
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.30V
Unlock RDP2 password succefully done!
SWD freq    : 3300 KHz
Connect mode: Power Down
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
SWD freq    : 1000 KHz
Connect mode: Power Down
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0xe0
Debug in Low Power mode enabled
```

此时 RDP 已经恢复到 Level1(0xFF)

4.3.3. TrustZone 使能（TZEN=1）RDP1 解锁降级到 RDP0

通过 STM32CubeProgrammerCLI 命令使用 OEM1/2Key 解锁后做 RDP 降级的示例（首先需要确认系统能够正常运行到 NonSecure 状态）

- 如果仅仅做 RDP Level1 到 Level0 降级，TZEN 保持为 1，这种情况与 TZEN=0 时类似，可以直接使用如下命令完成解锁和降级

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0x12345678 0xDEADBEEF -ob
RDP=0xAA
```

- 如果 RDP Level1 降级到 RDP Level0 并同时回退 TZEN，可以使用一条命令同时进行 OEM1Key 解锁和 RDP 降级+TZEN 回退

```
STM32_Programmer_CLI -c port=swd  mode=hotplug -unlockRDP1  0x12345678  0xDEADBEEF -ob
RDP=0xAA TZEN=0
```

解锁降级回退过程将会在 cmd 窗口看到类似如下打印信息

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0x12345678 0xDEADBEEF -ob
RDP=0xAA TZEN=0
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------
ST-LINK SN : 004300273039510634393838
ST-LINK FW : V3J7M2
Board : STM32U599J-DK
Voltage : 1.80V
SWD freq : 24000 KHz
Connect mode: Hot Plug
Reset mode : Software reset
Device ID : 0x481
Revision ID : Rev B
Reconnecting with the recommended frequency (3300 kHz)!
ST-LINK SN : 004300273039510634393838
ST-LINK FW : V3J7M2
Board : STM32U599J-DK
Voltage : 1.80V
SWD freq : 3300 KHz
Connect mode: Hot Plug
Reset mode : Software reset
Device ID : 0x481
Revision ID : Rev B
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U5xx
Flash size : 4 MBytes (default)
Device type : MCU
Device CPU : Cortex-M33
BL Version : 0x91
Debug in Low Power mode enabled
Unlock RDP1 password successfully done
UPLOADING OPTION BYTES DATA ...
Bank : 0x00
Address : 0x40022040
Size : 40 Bytes
[==================================================] 100%
Bank : 0x01
Address : 0x40022060
Size : 16 Bytes
[==================================================] 100%
PROGRAMMING OPTION BYTES AREA ...
Bank : 0x00
Address : 0x40022040
Size : 40 Bytes
[==================================================]
Reconnecting...
Reconnected !
UPLOADING OPTION BYTES DATA ...
Bank : 0x00
Address : 0x40022040
Size : 32 Bytes
[==================================================] 100%
Bank : 0x01
Address : 0x40022068
Size : 8 Bytes
[==================================================] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
```

```
Option Bytes successfully programmed
```

4.3.4. TrustZone 使能（TZEN=1）RDP1 解锁降级到 RDP0.5

通过 STM32CubeProgrammerCLI 命令使用 OEM1/2Key 解锁后做 RDP 降级的示例

注意：

1. TZEN=1 且 RDP 级别非 0 时，首先要保证代码能够正常运行到 NS 状态
2. RDP1 到 RDP0.5 的降级将导致所有 NS Flash 区的内容都被擦除，这意味着 S code 可能无法正常跳转到 NS Flash Code，从而导致 debug 端口无法连上的情况
   a. 如果 OptionByte 的设置允许从 RSS/SystemBootloader 启动，还可以通过拉高 BOOT PIN 的方式回复调试连接
   b. 如果 OptionByte 的设置不允许从 RSS/SystemBootloader 启动（例如设置了 BOOT_LOCK），那么建议 S code 中增加 NS RAM code 的部分，并在无法跳转到有效 NS Flash code 的情况下跳转 NS RAM code，从而保持调试连接可能性

- 这里降级命令使用-unlockRDP1，但是 Key 需要用前面设置过的 OEM2Key 的值

```
STM32_Programmer_CLI -c port=swd  mode=hotplug -unlockRDP1  0xFACEB00C 0xDEADBABE -ob
RDP=0x55
```

解锁降级回退过程将会在 cmd 窗口看到类似如下打印信息

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP1 0xFACEB00C 0xDEADBABE -ob
RDP=0x55
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
SWD freq    : 24000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
SWD freq    : 1000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x80
Debug in Low Power mode enabled
```

```
Unlock RDP1 password successfully done

UPLOADING OPTION BYTES DATA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[████████████████████████████████████████████████] 100%

  Bank           : 0x01
  Address        : 0x40022060
  Size           : 8 Bytes

[████████████████████████████████████████████████] 100%

  Bank           : 0x02
  Address        : 0x40022068
  Size           : 8 Bytes

[████████████████████████████████████████████████] 100%


PROGRAMMING OPTION BYTES AREA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒]

Reconnecting...
Reconnected !


UPLOADING OPTION BYTES DATA ...

  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes

[████████████████████████████████████████████████] 100%

  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes

[████████████████████████████████████████████████] 100%

OPTION BYTE PROGRAMMING VERIFICATION:

Option Bytes successfully programmed
```

4.3.5. TrustZone 使能（TZEN=1）RDP2 解锁降级到 RDP1

RDP Level2 解锁降级到 RDP Level1，与 TZEN=0 情况下相同

```
STM32_Programmer_CLI -c port=swd  mode=hotplug -unlockRDP2  0xFACEB00C 0xDEADBABE
```

解锁降级回退过程将会在 cmd 窗口看到类似如下打印信息

```
STM32_Programmer_CLI -c port=swd mode=hotplug -unlockRDP2 0xFACEB00C 0xDEADBABE
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------
ST-LINK SN : 004300273039510634393838
ST-LINK FW : V3J8M3
Board : STM32U599J-DK
Voltage : 1.79V
Unlock RDP2 password succefully done!
```

5. 使用特殊 CHIPID

通常从安全角度考虑，我们会倾向使用一机一密，也就是说比较好的方式是每颗芯片烧写不同的 OEMxKey，但是这样做一方面对 OEMxKey 的管理是一个挑战，另一方面，在 RDP Level2 的时候，由于调试连接已经无法读取任何片上资源，也很难通过通常的芯片 96bit UID 来确定当前的芯片应该对应哪一组 OEM Key。

针对这个问题，STM32U5 在原有 96bit UID 的基础上，增加了一个 32bit 的特殊 CHIPID，这个 CHIPID 存在于硬件的 DBG 单元中，而且即使在 RDP Level2，这个 CHIPID 也可以由调试器通过 JTAG/SWD 端口获取。因而 OEM 可以利用这个特殊 CHIPID 来简化一机一密的 OEMxKey 烧录过程，同时也可以在需要使用 OEMxKey 解锁的时候轻松读出 CHIPID，然后找到对应的 OEMxKey 进行解锁。

32bit CHIPID 可以通过调试端口工具读取，也可以通过代码读取，CHIPID 的地址为 0xE0044104。

注意：

- 当 RDP 处于 Level0 时，读取 32bit CHIPID 读到值为全 0
- 只有当 RDP 处于**非 Level0** 时才能读出正确的 CHIPID

CHIPID 通常的使用流程如下

- OEMxKey 烧录过程
  - 设置 RDP 为 Level1（或 Level 0.5）
  - 读取 CHIPID
  - 上位机根据一个密钥种子和 CHIPID 使用某种算法派生出该 CHIPID 对应的 Key
  - 将派生的 Key 作为 OEMxKey 写入芯片
  - 设置 RDP 到最终需要的级别（如 Level2）
- OEMxKey 解锁过程
  - 调试器通过 JTAG/SWD 连接芯片读取 CHIPID
  - 上位机根据一个密钥种子和 CHIPID 使用某种算法派生出该 CHIPID 对应的 Key 将派生的 Key 作为 OEMxKey 解锁芯片并进行 RDP 降级。

5.1. 特殊 CHIPID 的读取

特殊 CHIPID 可以通过软件代码直接读地址 0xE0044104 获得，也可以通过 STM32CubeProgrammerCLI 命令来读取，命令如下：

```
STM32_Programmer_CLI -c port=swd  mode=hotplug getAuthID
```

注意：

1. STLink 需要更新到 V3J9M3 或以上版本
2. STM32CubeProgrammer 需要更新到 V2.9.0 或以上版本

运行该命令在 RDP Level1 时将看到类似如下信息，蓝色高亮的部分即为获取的 CHIPID

```
STM32_Programmer_CLI.exe -c port=swd mode=hotplug getAuthID
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.9.0
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
SWD freq    : 24000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
DBGMCU_DBG_AUTH_DEVICE : 0x292D8E4A
SWD freq    : 1000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x__
Debug in Low Power mode enabled
```

运行该命令在 RDP Level2 时将看到类似如下信息，此时调试连接会出错，这是正常现象，因为 RDP Level2 时禁止调试连接，但是 CHIPID 依旧可以读取，蓝色高亮的部分即为获取的 CHIPID

```
STM32_Programmer_CLI.exe -c port=swd mode=hotplug getAuthID
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.9.0-A02
      -------------------------------------------------------------------

ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
Error: Cannot connect to access port 0
If you are trying to connet to a device with TrustZone enabled please try to connect with
HotPlug mode
```

```
2nd connect tentative with a lower frequency (8MHz)
ST-LINK SN  : 003E00473438510D34313939
ST-LINK FW  : V3J9M3
Board       : NUCLEO-U575ZI-Q
Voltage     : 3.29V
DBGMCU_DBG_AUTH_DEVICE : 0x292D8E4A
Error: Cannot connect to access port 0
If you are trying to connet to a device with TrustZone enabled please try to connect with
HotPlug mode
```

6. 小结

STM32U5 提供了更灵活的芯片生命周期管理机制，在 STM32L5 的基础上增加了 OEM Key 特性，一方面能够保护 RDP 级别的状态转换，防止任意的回退；另一方面也减少了 RDP Level2 使用中的局限性和顾虑点，同时还增加了 32bit 特殊 CHIPID，能够方便地实现在不同芯片上配置不同 OEMxKey 的需求。

参考文献

【如有， 请注明；否则，请注明：无】

文件编号	文件标题	版本号	发布日期
RM0456	Reference manual STM32U575/585 Arm®-based 32-bit MCUs	Rev0.4	
UM2237	STM32CubeProgrammer software description	Rev16.0	

文档中所用到的工具及版本

STM32CubeProgrammer v2.8.0

版本历史

日期	版本	撰写/变更
2021 年 11 月 20 日	1.0	首版发布

重要通知 – 请仔细阅读

意法半导体公司及其子公司 （“ST”）保留随时对 ST 产品和 / 或本文档进行变更的权利，恕不另行通知。买方在订货之前应获取关于 ST 产品的最新信息。 ST 产品的销售依照订单确认时的相关 ST 销售条款。

买方自行负责对 ST 产品的选择和使用， ST 概不承担与应用协助或买方产品设计相关的任何责任。

ST 不对任何知识产权进行任何明示或默示的授权或许可。

转售的 ST 产品如有不同于此处提供的信息的规定，将导致 ST 针对该产品授予的任何保证失效。

ST 和 ST 徽标是 ST 的商标。若需 ST 商标的更多信息，请参考 *www.st.com/trademarks*。所有其他产品或服务名称均为其 各自所有者的财产。

本文档是 ST 中国本地团队的技术性文章，旨在交流与分享，并期望借此给予客户产品应用上足够的帮助或提醒。若文中内容存有局限或与 ST 官网资料不一致，请以实际应用验证结果和 ST 官网最新发布的内容为准。您拥有完全自主权是否采纳本文档（包括代码，电路图等）信息，我们也不承担因使用或采纳本文档内容而导致的任何风险。

本文档中的信息取代本文档所有早期版本中提供的信息。