STM32L5 中如何关闭 TrustZone ?

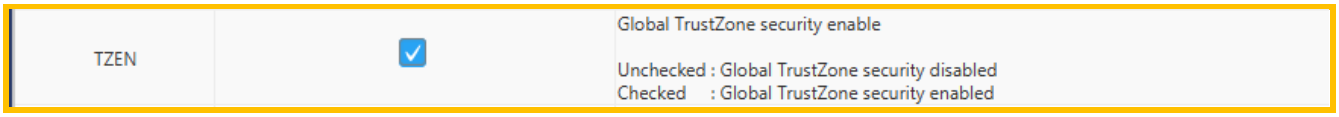
1. 前言

STM32L5 是 STM32 家族中第一个基于 Cortex-M33 内核的系列，而 TrustZone 正是此内核最重要的特性，使能 TrustZone 的方法非常简单，在 RDP=0 的情况下直接在 option byte 中将 TZEN 置 1 即可，但是一旦 TrustZone 使能后，与其相关的安全特性也将开启，由于安全方面的特性，在 TrustZone 已经打开的情况下欲将其再次关闭却不能像打开时那样那么简单操作了。本文将以用户的视角描述一下关闭 TrustZone 的过程.

2 过程

为了讲述这一过程，我们将以 NUCLEO-L552ZE-Q 这块板子为例，工具使用 STM32CubeProgrammer V2.4.0

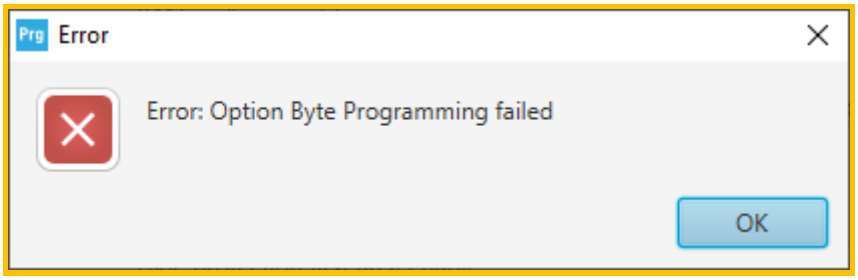
首先通过 CubeProgrammer 这个工具将 MCU 的 TrustZone 打开, 在此之前读保护 RDP=0 ,是用户面临的选项字节最初始状态 :



按客户的操作思路，接下来我们尝试关闭 TrustZone…

首先，直接在 option byte 中直将 TZEN 后那个勾去掉，然后 Apply…

此时会出现错误，如上图所示。



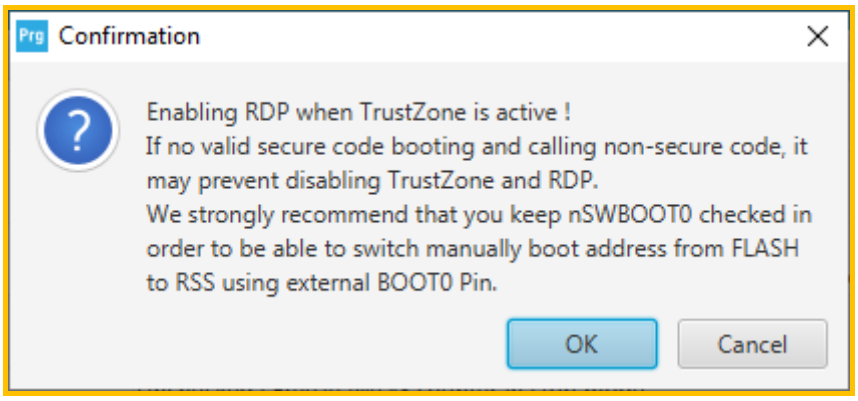
在 TrustZone 已经激活的情况下，是不能直接将其关掉的。

接下来查看参考手册，在 RM0438 4.4.2 节有讲述到如何将 TrustZone 关闭的内容 :

- TZEN option bit
  - TZEN can only be set on RDP level 0.
  - Deactivation of TZEN must be done at the same time as RDP regression from level 1 to level 0.

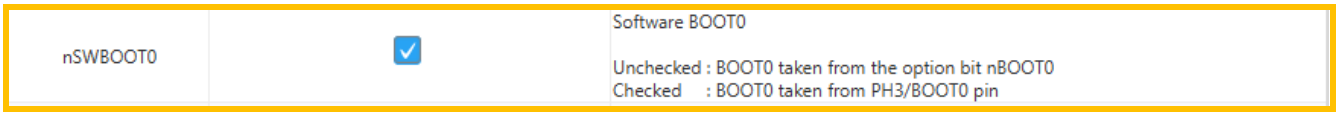
显然，原来 TrustZone 关闭必须是在读保护从 RDP1 回退到 RDP0 的同时进行才可以。

首先，我们要将 RDP 设置为 level1,然后再回退…



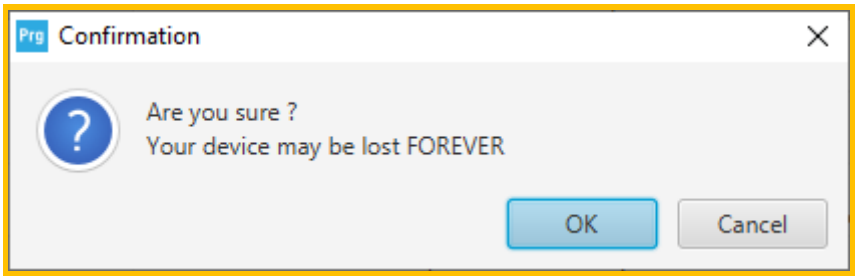
如上图所示，在设置 RDP1 的时候, 此时会出现警告，意思是说在 TrustZone 开启的情况下尝试使能 RDP，如果当前 FLASH 内的代码不能使得芯片上电后执行的程序最终跳转到 NS 空间，将会导致关闭 trustzone 和回退 RDP 失败，强烈建议将 nSWBOOT0 设置为 1。这样可以确保我们可以通过调整 PH3/Boot0 引脚电平来从系统 bootloader 启动，这是一定可以跑到 NS 程序空间的。【NS :Non-Secure】

我们先选择“取消”，然后检查 nSWBOOT0 的设置 :

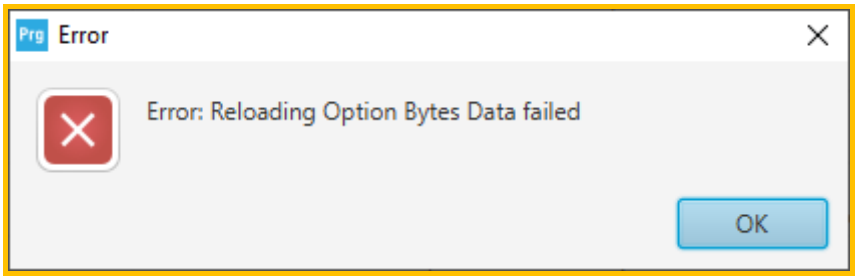


如上图所示，nSWBOOT0 的值已经为 1，是 OK 的，其值表示 BOOT0 的值将从 PH3 引脚的状态来决定 。

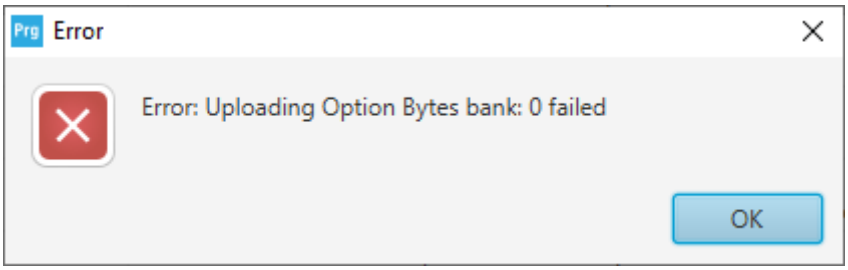
既然关闭 TrustZone 必须是 RDP 从 LEVEL 1 回退到 LEVEL 0 的过程中操作才行，那么我们必须要先将 RDP 设置为 LEVEL 1 才行。使能 RDP LEVEL 1：



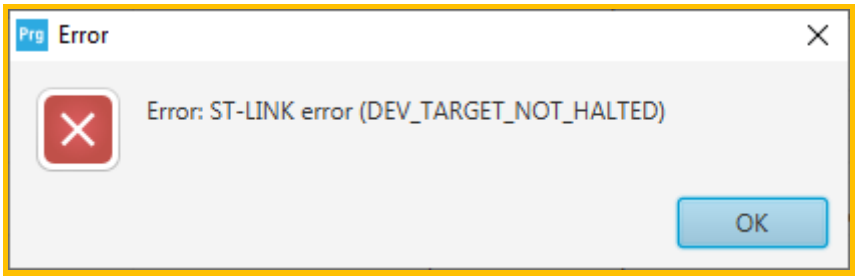
如上图所示,警告意思是 :你确定 ?你的 MCU 将可能永远丧失 ! 点击 OK。如下图所示 :



表示 FLASH 内的数据已经不能读取了，RDP LEVEL 1 使能后，FLASH 的内容自然不能再读出，点击 OK…



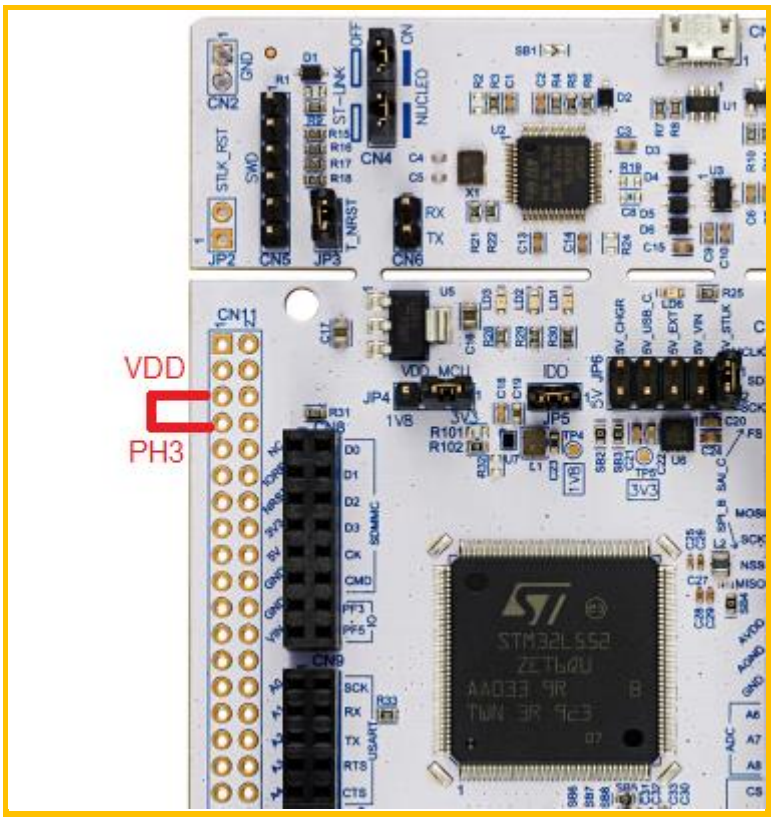
此时再次尝试连接，则出现如下界面所示：



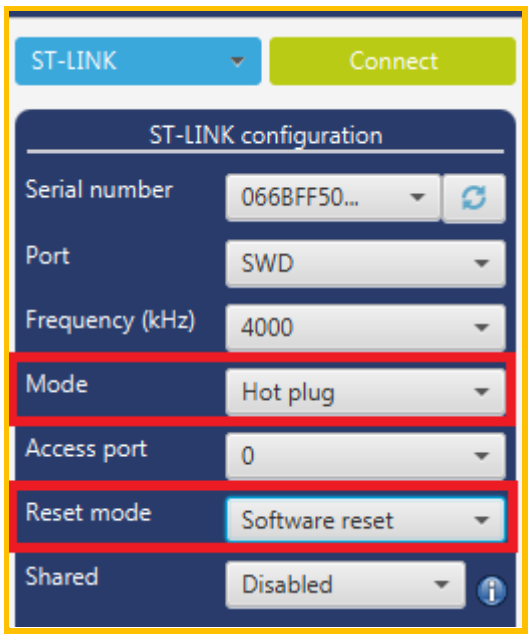
此时，ST-Link 果然不能再连接。

那么接下来我们该如何做呢？ ->拉高 PH3, 让 MCU 从 RSS 启动.

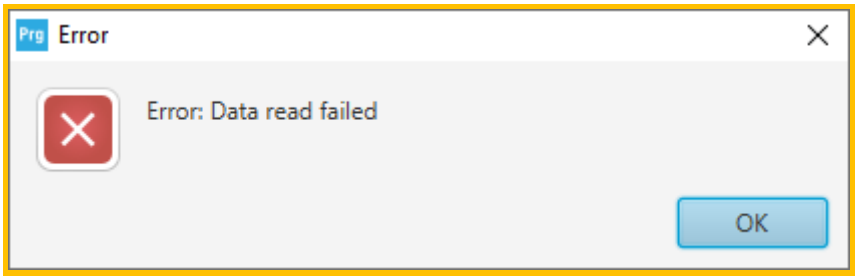
以 NUCLEO-L552-Q 板为例，将 PH3 拉到 VDD 后，再次上电重启，此时板上的蓝色的 LD2 和红色 LD3 亮起。按照这块板子的用户手册 UM2581，章节 6.11.2 说明：直接把 CN11 上的引脚 5(VDD)和引脚 7(PH3_BOOT0)短接即可。



使用 Cubeprogrammer，以 hotplug 模式进行连接(Mode :Hot plug)：

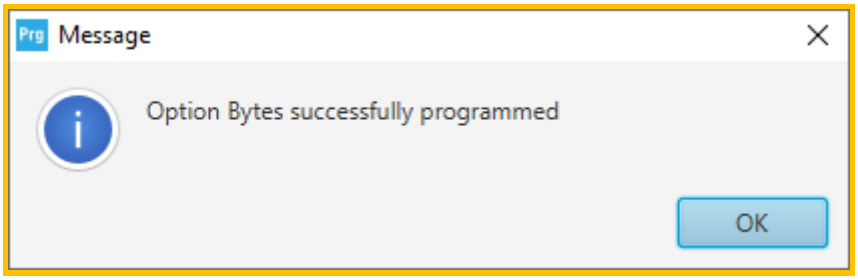


尝试连接：

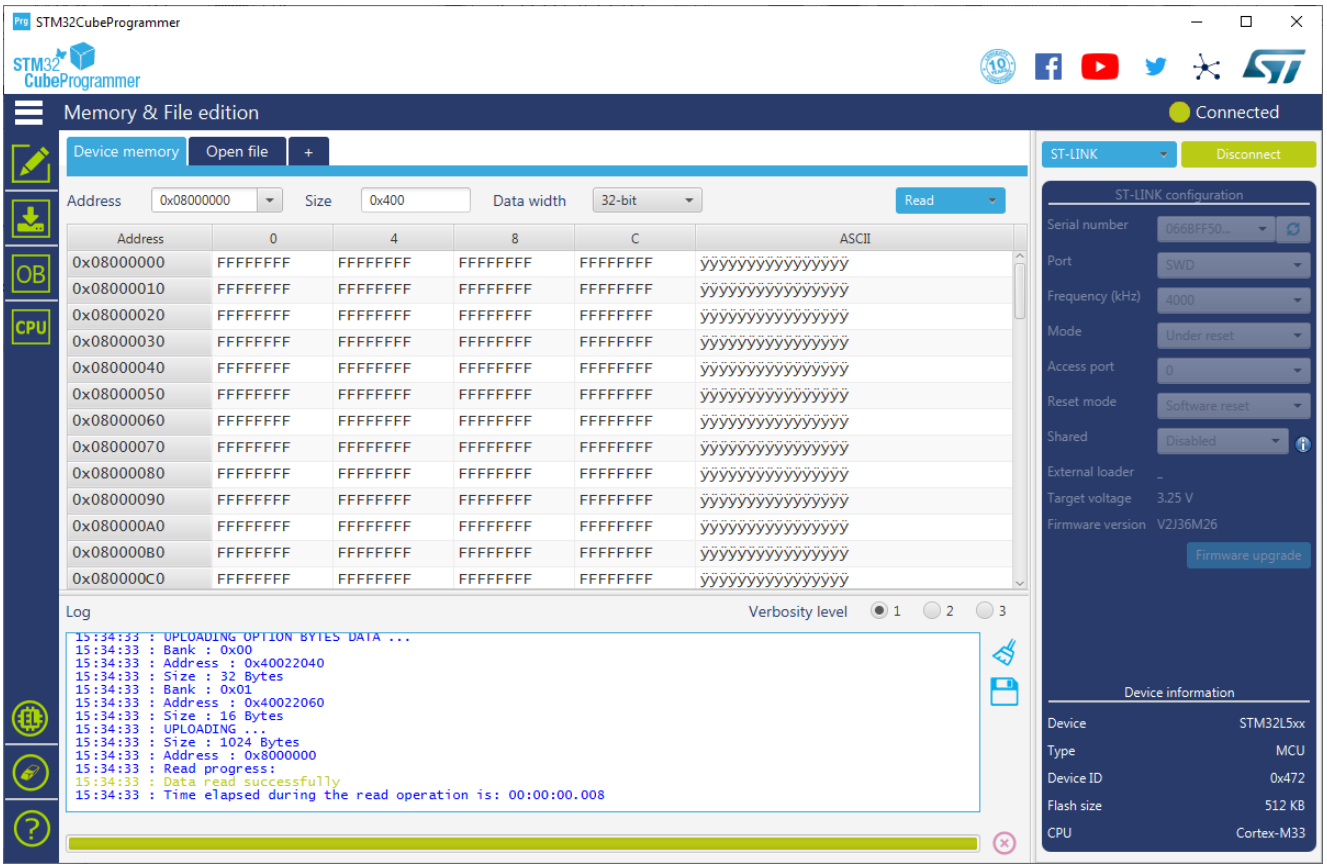


如上图所示，ST-Link 已经连接上，只不过由于 RDP LEVEL 1 使能了而不能读取 FLASH 内容，但此时 option bytes 是可以修改的。

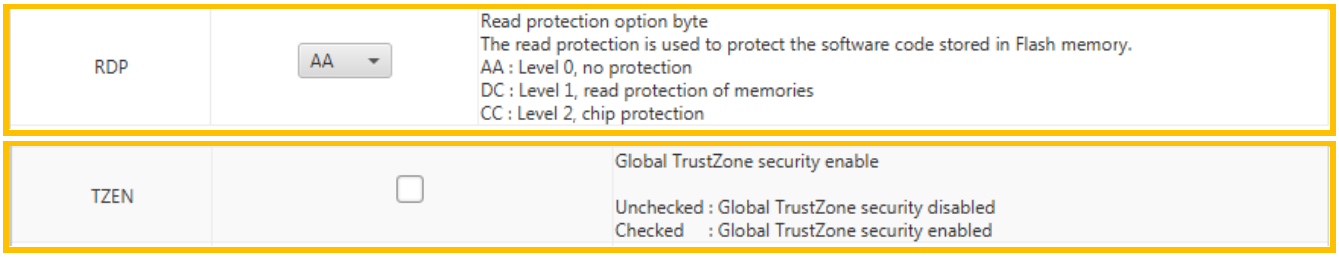
打开 Option byte 界面，在 User configuration 下将 TZEN 对应的复选框内的勾去掉，然后再将 Read Out Protection 下的 RDP 改回 LEVEL 0，然后点击 Apply…



上图表示已经修改成功，断开连接，断开电源，然后将 PH3 引脚的高电平恢复到低电平。上电后再次连接…



如上图所示，再次连上时，FLASH 的内容由于 RDP LEVEL 1 回退到 LEVEL 0 时被全部清空。此时再次查看 RDP 和 TZEN 的值：



RDP 恢复到 LEVEL 0，TrustZone 成功关闭。

后注：

1> 关闭 trustzone 需要通过 RDP 级别回退完成。

2> nSWBOOT0=1 && BOOT0/ PH3 引脚为高，使得上电后系统从 RSS 启动。

3> 在 STM32CubeProgrammer 中使用 hot plug 连接方式是为了让 MCU 从 RSS 启动后，在运行到 NS 空间的时候方便跟调试端口连接，以便进行后续的 Option Bytes 修改操作。

参考文档：AN5347

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、更正、增强、修改和改进的权利，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。所有其他产品或服务名称均为其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。