

FLASH 被异常改写

问题描述:

某客户反馈，当 MCU 频繁的正常通断电的时候。FLASH 被异常改写，出现各种各样的异常（整片擦除、中断向量表被改写为 0、写保护被清掉、被加上读保护）

问题调研:

首先跟客户沟通:

- 他们是延续之前的项目，进行的一些软硬件简单修改。之前的项目没有出现过类似的问题。
- 确认通断电的时间是足够，就是说他们断电后所有的 VDD 都回到 0. 上电的时序也是正常。
- 原理图确认这是 follow 了我们的参考设计。
- 测量工作时的电压，只是发觉他们上电时会有一些抖动，其它一切正常。尝试让他们改善上电电路，去掉这一抖动，再次实验，仍然出现类似的问题。

到这里似乎跟硬件没有任何的问题了，接着让客户代码进行删减又做了如下实验:

1. 去掉 APP 部分代码，仅仅留下 IAP 代码。做相同的实验，问题再现。
2. 进一步删减程序，客户去掉程序中所有跟 flash 以及 OPTION BYTE 相关的部分，做相同的实验，问题再现。
3. 没招，再删，最后仅仅留下下面程序:

```
int main(void)
{
    ....delay_init(168);
    ....drv_led_init();
    ....chip_add_flash_wr_protect();

    ....SYS_GREEN_LED_ON();
    ....SYS_RED_LED_OFF();

    ....while (1)
    ....{

    ....}
}
```

```
void chip_add_flash_wr_protect(void)
{
    /* Get FLASH_WRP_SECTORS write protection status */
    SectorsWRPStatus = FLASH_OB_GetWRP() & FLASH_WRP_SECTORS;
    if (SectorsWRPStatus != 0x00)
    {
        /* If FLASH_WRP_SECTORS are not write protected, enable the write protection */
        /* Enable the Flash option control register access */
        FLASH_OB_Unlock();
        /* Enable FLASH_WRP_SECTORS write protection */
        FLASH_OB_WRPConfig(FLASH_WRP_SECTORS, ENABLE);

        /* Start the Option Bytes programming process */
        if (FLASH_OB_Launch() != FLASH_COMPLETE)
        {
            /* User can add here some code to deal with this error */
            while (1)
            {
                SYS_RED_LED_ON(); // 绿灯常亮表示加保护失败
            }
            /* Disable the Flash option control register access (recommended to protect
            the option bytes against possible unwanted operations) */
            FLASH_OB_Lock();
            /* Get FLASH_WRP_SECTORS write protection status */
            SectorsWRPStatus = FLASH_OB_GetWRP() & FLASH_WRP_SECTORS;

            /* Check if FLASH_WRP_SECTORS are write protected */
            if (SectorsWRPStatus == 0x00)
            {
                green_led_blink = 1;
                /* OK, turn ON LED4 */
                SYS_GREEN_LED_ON();
            }
            else
            {
                green_led_blink = 2;
                /* KO, turn ON LED3 */
                SYS_GREEN_LED_ON();
                SYS_RED_LED_ON();
            }
        }
    }
}
```

```
void delay_init(u8 SYSCLK)
{
    NVIC_PriorityGroupConfig(NVIC_PriorityGroup_2);
    SysTick_CLKSourceConfig(SysTick_CLKSource_HCLK_Div8);
    fac_us=SYSCLK/8;

    fac_ms=(u16) fac_us*1000;
}
```

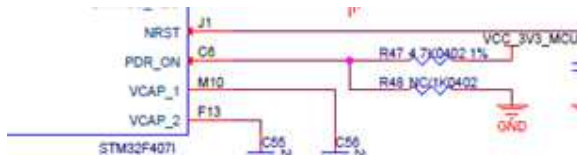
客户反应只要掉用了 `delay_init` 函数就会出问题，不调用就不会出问题（仅仅做了一天的实验）。到这里似乎跟我们的软件有关系了，我们进一步分析发现他们改写了我们的 `systick` 的 `config` 函数，那么我就做下一个实验。

4. 改为标准库中的 `systick` 例程，去掉写保护，加一个 `GPIO` 定时翻转程序。同时在烧录之后，加上写保护，做相同的实验，问题再现。
5. 到这里我们都怀疑是芯片真的有损伤了，我们再做了一个实验用 `cubemx` 生成了一个 `GPIO` 翻转和 `systick` 的延时，做相同的实验，问题再现。

原因：

到这里我们似乎是江郎才尽，只能坐等 `FA` 的报告，看看芯片是否真的坏了与否。我们抱着怀疑一切的态度，请他们的硬件工程师再次确认他们的硬件和原理图的一致性，我们怀疑他们的硬件是否有装错的元器件。主要集中在 `MCU` 周边。最后他们的工程反馈，他们的 `PDR_ON` 脚，板子上装的元器件跟原理图不一致。他们把 `R47` 和 `R48` 都装了，那么相当于在 `PDR_ON` 上是一个 `0.6v` 的电压，也就是关断了 `MCU` 内部复位。

真是山穷水尽疑无路，柳暗花明又一村，问题应该跟内部复位有关。



2.2.15 Power supply supervisor

Internal reset ON

On packages embedding the PDR_ON pin, the power supply supervisor is enabled by holding PDR_ON high. On all other packages, the power supply supervisor is always enabled.

The device has an integrated power-on reset (POR) / power-down reset (PDR) circuitry coupled with a Brownout reset (BOR) circuitry. At power-on, POR/PDR is always active and ensures proper operation starting from 1.8 V. After the 1.8 V POR threshold level is reached, the option byte loading process starts, either to confirm or modify default BOR threshold levels, or to disable BOR permanently. Three BOR thresholds are available through option bytes. The device remains in reset mode when V_{DD} is below a specified threshold, $V_{POR/PDR}$ or V_{BOR} , without the need for an external reset circuit.

Internal reset OFF

This feature is available only on packages featuring the PDR_ON pin. The internal power-on reset (POR) / power-down reset (PDR) circuitry is disabled with the PDR_ON pin.

An external power supply supervisor should monitor V_{DD} and should maintain the device in reset mode as long as V_{DD} is below a specified threshold. PDR_ON should be connected to this external power supply supervisor. Refer to [Figure 7: Power supply supervisor interconnection with internal reset OFF](#).

从上面规格书来看，如果我们关闭 mcu 内部的复位电路，需要在外部接一个复位信号保证 VDD 达到正常工作电压之前一直使 MCU 处于复位状态。

解决办法：

问题找到后解决办法就很简单，去掉 R48 这个 1k 欧姆的电阻，重做实验，再没有发现问题。

结论：

其实在之前我们的另外一个西安的客户发生过频繁上电不工作的情况。他们也是使用了就得数据手册，没有把 PDR_ON 脚拉到 VDD 所致。

对于 ST MCU 来说，这个 PDR_ON 引脚有的封装是被引出来了，有的封装没有引出，如果没有引出的是默认使能内部复位功能，如果引出的话，大家也要当心有的型号是拉低使能内部复位；有得是拉高使能内部复位。所以在检查电路时一定要当心。

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。