



登录

找回密码

立即注册



走，一起去STM32中国峰会 暨粉丝狂欢节

生态 · 智能 · 安全 4.25—4.26

[实战经验] ST原厂FAE经验汇总

STM32应用案例分享

STM32经典图书推荐 (2017.11更新)

STM32产品介绍及设计资源

请输入搜索内容

帖子

热搜: 峰会纪念衫免费领 STM32中国峰会 RTOS Lora

论坛

【STM32/STM8专区】

STM32

【STM32F303开发】+如何找到导致程序出现HardFault的代 ...

发帖

返回列表

1

2

3

4

1 / 4 页

下一页

查看: 8419 | 回复: 37

[转载] 【STM32F303开发】+如何找到导致程序出现HardFault的代码

[复制链接]

发表于 2015-7-4 19:50:57 | 只看该作者 | 只看大图

本帖最后由 creep 于 2015-12-5 17:17 编辑

下午在社区群里和小伙伴聊天时谈到如果程序Fault时如何找到是哪句代码出现的问题，也就是说怎么找到程序运行到何处时出现Fault的。之前一直使用一种方法感觉不错，分享给有需要的同学。

大致的思想是当程序出现Falut时会跳转到相应的Fault中断里面，此时压入到堆栈的信息应该就是出现问题代码运行出错Fault的信息，我们要做的就是找到此时压入堆栈的LR的值。为了模拟Fault，我们将0写到地址0里面，此时debug下全速运行，程序就会进入到Fault函数中。

```
int main(void)
{
    uint32_t paddr = 0;
    delay_init();
    delay_ms(1000);
    *(uint32_t*)paddr = 0;
    while(1)
    {
        //将数据发送到Debug Viewer
        printf((const char*)Write_buff);
        delay_ms(1000);
    }
}
```

这句代码会导致Fault

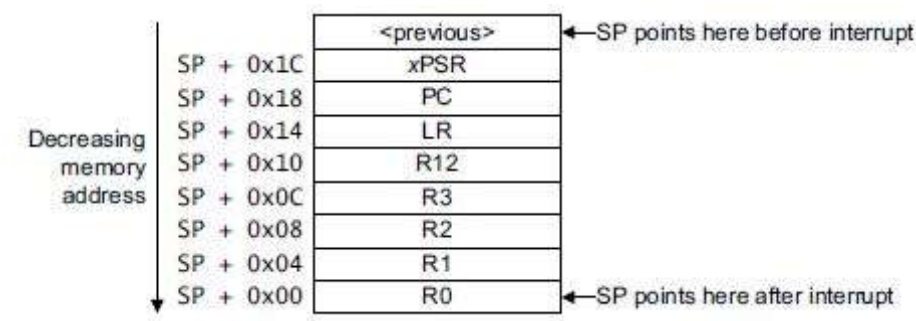
我们在Fault中断函数中添加一个软断点，这样做的好处是debug模式下全速运行，当程序跑飞（Fault时）会自动停在这里，否则我们还要手动停止运行才能发现程序进入了Fault中断函数。

```
62 void HardFault_Handler(void)
63 {
64     /* Go to infinite loop when Hard Fault exception occurs */
65     __ASM volatile("BKPT #01");
66     while (1)
67     {
68     }
69 }
```

debug时全速运行程序，有Fault出现时会自动停在这里

为了方便查看程序程序的Fault时的相关信息，我们将错误信息打印到keil的debug Viewer窗口中，关于如何打印信息到keil的debug viewer窗口，可以参考我之前的发的帖子：[【STM32F303开发】+ 使用SWO输出调试信息到Debug Viewer窗口](#)

M3/M4内核的MCU的压栈的模式如下，我们根据下面的寄存器的存放顺序来取出压入到堆栈的寄存器的值。



同时将Fault中断时的函数重载如下，用来输出更多的信息,同时判断了是使用MSP还是使用PSP,

```
#if defined(__CC_ARM)
__asm void HardFault_Handler(void)
{
    TST lr, #4
    ITE EQ
    MRSEQ r0, MSP
    MRSNE r0, PSP
    B __cpp(Hard_Fault_Handler)
}
#elif defined(__ICCARM__)
void HardFault_Handler(void)
{
    __asm("TST lr, #4");
    __asm("ITE EQ");
    __asm("MRSEQ r0, MSP");
    __asm("MRSNE r0, PSP");
    __asm("B Hard_Fault_Handler");
}
#else
#warning Not supported compiler type
```

用于使用msp和psp

faultjpg.jpg (71.47 KB, 下载次数: 111)

[下载附件](#)

2015-7-4 19:12 上传

ck[]函数根据寄存器SCB->CFSR判断并输出是那种Fault：

分享到：

creep



该用户从未签到

60

1920

7

主题

帖子

精华

版主
最后登录 2018-4-26
发消息

```
void Hard_Fault_Handler(uint32_t stack[])
{
    static char msg[80];
    printf("In Hard Fault Handler\n");
    sprintf(msg, "SCB->HFSR = 0x%08x\n", SCB->HFSR);
    printf(msg);
    if ((SCB->HFSR & (1 << 30)) != 0)
    {
        printf("Forced Hard Fault\n");
        sprintf(msg, "SCB->CFSR = 0x%08x\n", SCB->CFSR );
        printf(msg);
        if((SCB->CFSR & 0xFFFF0000) != 0) {
            printUsageErrorMsg(SCB->CFSR);
        }
        if((SCB->CFSR & 0xFF00) != 0) {
            printBusFaultErrorMsg(SCB->CFSR);
        }
        if((SCB->CFSR & 0xFF) != 0) {
            printMemoryManagementErrorMsg(SCB->CFSR);
        }
    }
    stackDump(stack);
    __ASM volatile("BKPT #01");
    while(1);
}
```

最后使用函数stackDump(stack);输出出现Fault时的堆栈的值，取值的顺序是根据上面说的M3/M4内核压栈的顺序得到的：

```
enum { r0, r1, r2, r3, r12, lr, pc, psr};

void stackDump(uint32_t stack[])
{
    static char msg[80];
    sprintf(msg, "r0 = 0x%08x\n", stack[r0]);
    printf(msg);
    sprintf(msg, "r1 = 0x%08x\n", stack[r1]);
    printf(msg);
    sprintf(msg, "r2 = 0x%08x\n", stack[r2]);
    printf(msg);
    sprintf(msg, "r3 = 0x%08x\n", stack[r3]);
    printf(msg);
    sprintf(msg, "r12 = 0x%08x\n", stack[r12]);
    printf(msg);
    sprintf(msg, "lr = 0x%08x\n", stack[lr]);
    printf(msg);
    sprintf(msg, "pc = 0x%08x\n", stack[pc]);
    printf(msg);
    sprintf(msg, "psr = 0x%08x\n", stack[psr]);
    printf(msg);
}
```

这个LR的值就是我们找到的罪魁祸首

下面我们在debug模式下全速运行如下代码，main函数如下：其中的 *(uint32_t*)paddr = 0; 会导致Fault并进入中断，

[首页](#)
[新闻](#)
[资料下载](#)
[print论坛](#)
[视频](#)
[FAQ](#)
[立刻购买](#)
[积分换礼](#)
[排行榜](#)
[快捷导航](#)

creep



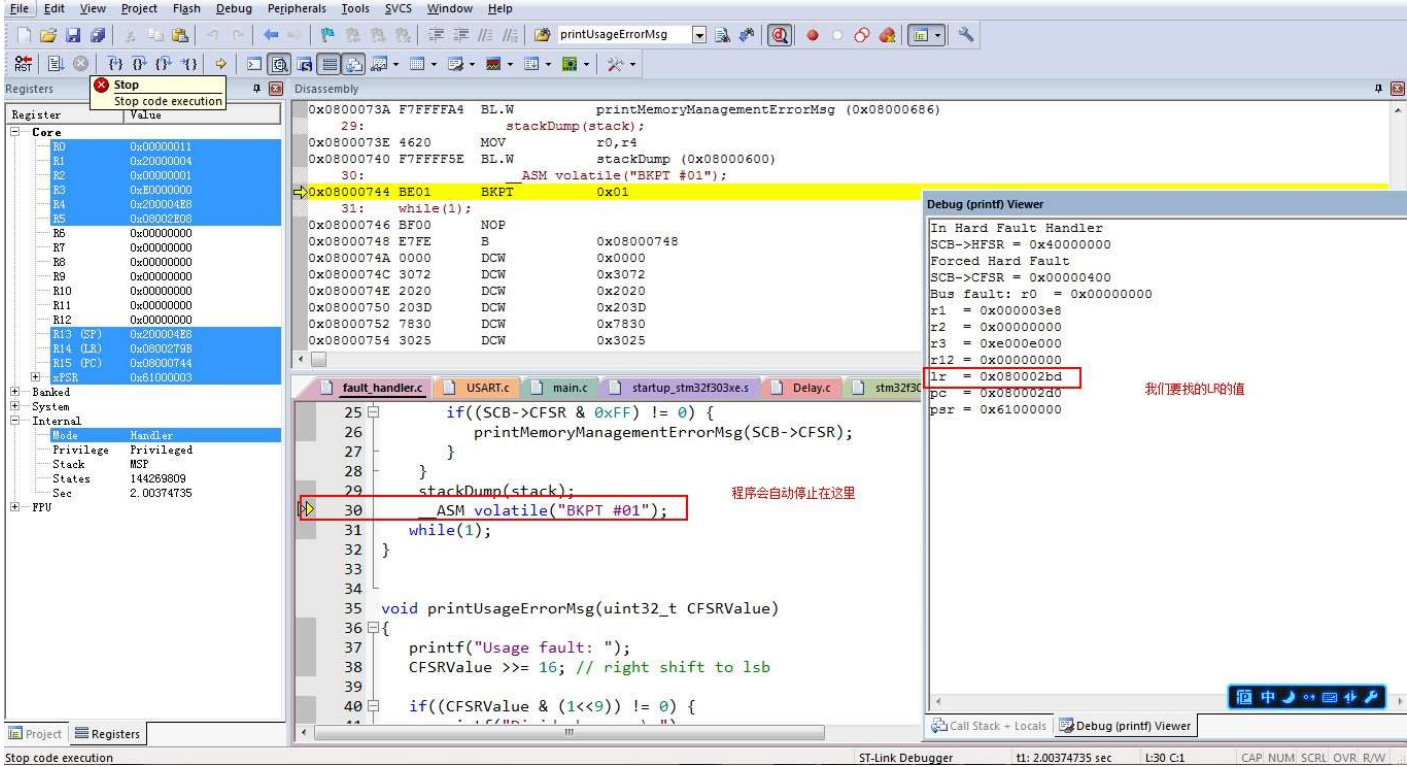
该用户从未签到

60	1920	7
主题	帖子	精华

版主
最后登录 2018-4-26
发消息

```
u8 Write_buff[20] = "Hi,i am creep !\n\r";
int main(void)
{
    uint32_t paddr = 0;
    delay_init();
    delay_ms(1000);
    *(uint32_t*)paddr = 0;
    while(1)
    {
        //将数据发送到Debug Viewer
        printf((const char*)Write_buff);
        delay_ms(1000);
    }
}
```

在debug模式下全速运行，不要设置任何断点，最后程序程序会在debug viewer中输出出错Fault的相应的寄存器的值并停止在__ASM volatile("BKPT #01");，此处得到的LR的值就是我们要找的LR的。



此时打开汇编窗口，在汇编窗口里面右键show Disassembly at Address选项输入LR的值然后回车

首页 新闻 资料下载 论坛 视频 FAQ 立刻购买 积分换礼 排行榜 快捷导航

creep



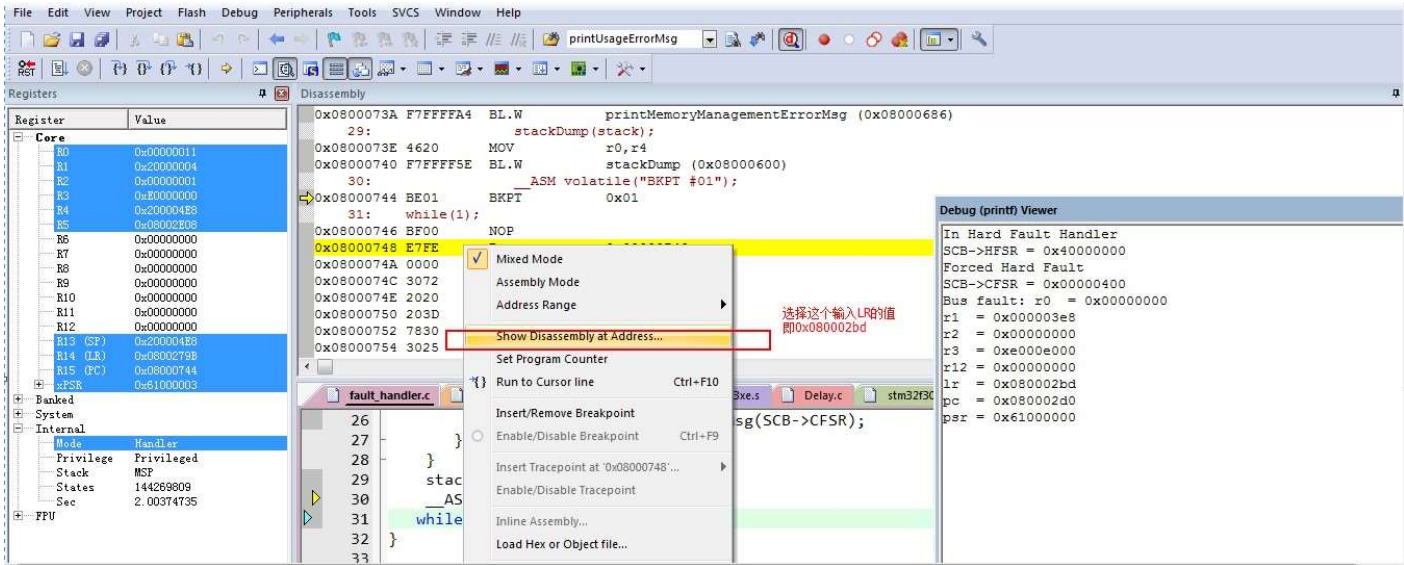
该用户从未签到

60 1920 7
主题 帖子 精华

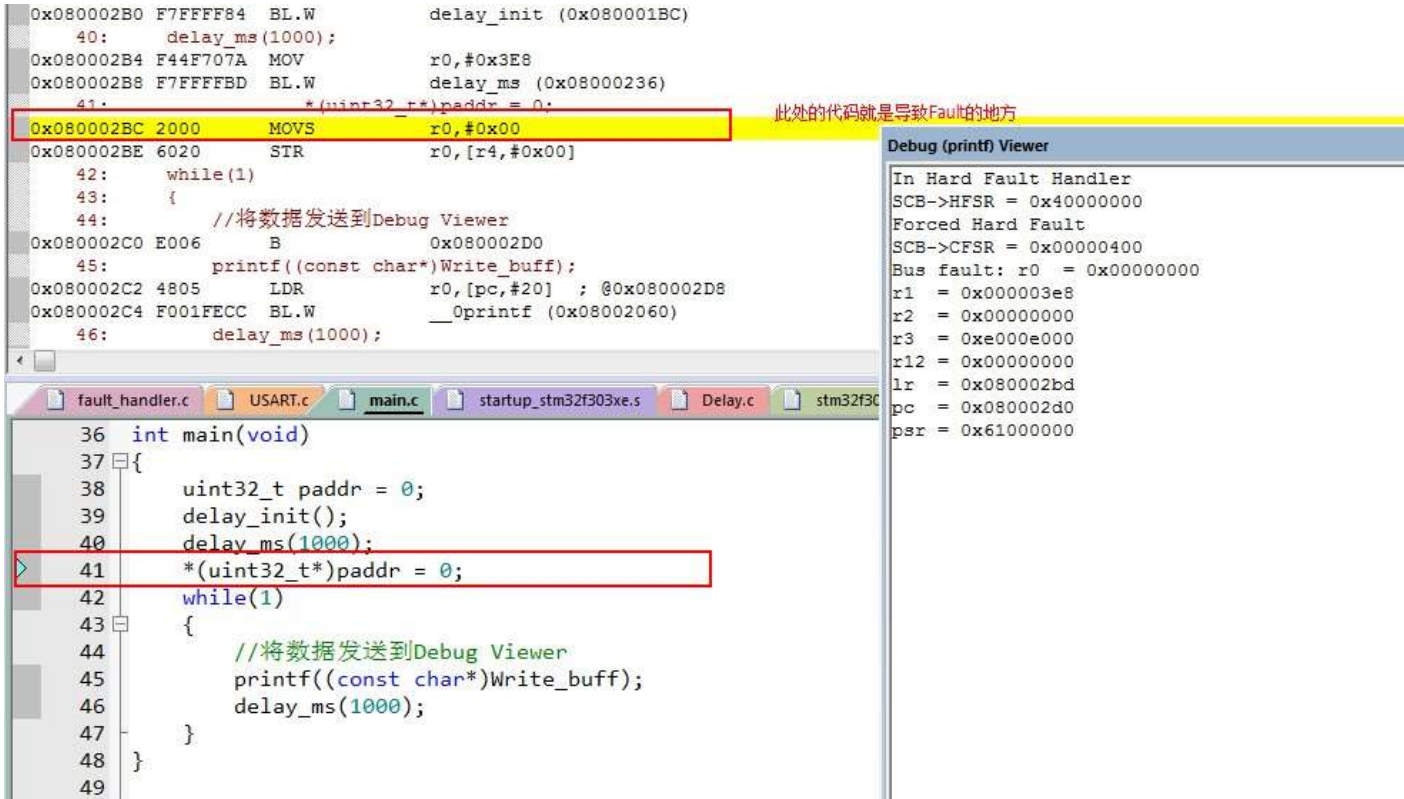
版主

最后登录 2018-4-26

发消息



调转到的汇编的地方就是导致程序出现Fault的地方，注意M3/M4内核使用Thumb指令，要求最低bit为1，



上面的过程大致就是找到程序出现Fault跑飞时的方法，基本上能定位到出错的代码，使用OS时要注意判断是哪个SP在起作

首页

新闻

资料下载

论坛

视频

FAQ

立刻购买

积分换礼

排行榜

快捷导航

这个方法很早就看到过，但是今天查资料发现是国外的一个工程师在ARM举行的Technical Conference上做的一个分享，

具体参考网页：[Developing a Generic Hard Fault handler for ARM Cortex-M3/Cortex-M4](#)

如果有问题可在社区QQ群(427779516)讨论

上面用到的测试代码：

 [F303RE_Fault_Handler.rar](#) (396.61 KB, 下载次数: 240)

内核寄存器说明：

 [M4_programming_manual.pdf](#) (2.6 MB, 下载次数: 185)

参考代码：

 [CM3_Fault_Handler-master.zip](#) (4.02 KB, 下载次数: 130)

延伸阅读：[【STM32F303开发】+使用fromelf反汇编keil生成的AXF文件](#)

creep



该用户从未签到

60

主题

1920

帖子

7

精华

版主
最后登录 2018-4-26
[发消息](#)

【STM32F303开发】+ 关于连接寄存器LR的值

Updated (2015-12-05) : 建议首先使用**PC**的值去找Fault的地址，有的Fault问题使用LR的值可能不准确。
更权威详细的方法请参考：[Developing a Generic Hard Fault handler for ARM Cortex-M3/Cortex-M4](#)

评分

参与人数 2 ST金币 +38 理由 [收起](#)

 wofei1314	+ 18
 zero99	+ 20

[查看全部评分](#)

 收藏 31  淘帖

[STM32中国峰会纪念衫，免费申请>>](#) [看峰会直播送STM32H7，戳我报名>>](#)

回复 举报

 楼主 | 发表于 2015-7-4 21:03:14 | 只看该作者 推荐



creep

z00 发表于 2015-7-4 20:05
记得在《cortex m3 权威指南》也有过这方面的介绍

《cortex m3 权威指南》是本好书，值得多读几遍！

[首页](#) [新闻](#) [资料下载](#) [论坛](#) [视频](#) [FAQ](#) [立即购买](#) [积分换礼](#) [排行榜](#) [快捷导航](#)

该用户从未签到

creep

60 | 1920 | 7



该用户从未签到

z00

60 | 1920 | 7

主题 | 帖子 | 精华

回复 支持 1 反对 0 举报

 发表于 2015-7-4 20:05:37 | 只看该作者 沙发

记得在《cortex m3 权威指南》也有过这方面的介绍

版主

最后登录 2018-4-25

发消息



该用户从未签到

47	427	0
主题	帖子	精华

论坛元老

最后登录 2018-4-25

发消息

风子



该用户从未签到

33	1276	3
主题	帖子	精华

论坛元老

最后登录 2018-4-20

发消息

Paderboy



该用户从未签到

最后登录 2018-4-26

1920	1920	1920
主题	帖子	精华

发消息


STM32中国峰会纪念衫, 免费申请>>> 看峰会直播送STM32H7, 戳我报名>>>

回复 支持 反对 举报

 发表于 2015-7-4 20:21:28 | 只看该作者 板凳

谢谢分享, 很有用的东西

回复 支持 反对 举报

 发表于 2015-7-4 20:34:40 | 只看该作者 地板

版主
最后登录 2018-4-26

发消息



该用户从未签到
47 1243 2
主题 帖子 精华

论坛元老
最后登录 2018-4-26
发消息

yvonn



该用户从未签到
2 73 0
主题 帖子 精华

中级会员
最后登录 1970-1-1

发消息

creep



该用户从未签到
60 1920 7
主题 帖子 精华

回复 支持 反对

举报

发表于 2015-7-4 21:14:13 | 只看该作者

6#

谢谢分享

回复

举报

发表于 2015-7-4 21:24:52 | 只看该作者

7#

ST的专门正对这个错误，出过指导，可能因为是英文的原因，没有被广泛传阅，让很多后来者，还在这里苦苦探索，好大的坑，如果没记错的话二姨家应该就有，实在不行去官网下也行。方法好像有好几种，不过还是支持楼主的分享精神。

首页

新闻

资料下载

论坛

视频

FAQ

立刻购买

积分换礼

排行榜

快捷导航

回复 支持 反对

举报

楼主 | 发表于 2015-7-4 21:45:49 | 只看该作者

8#

yvonn 发表于 2015-7-4 21:24

ST的专门正对这个错误，出过指导，可能因为是英文的原因，没有被广泛传阅，让很多后来者，还在这里苦苦探索 ...

谢谢指导，不知道你说的ST的出的指导哪里可以找到，能不能给些提示或者连接！
这里导致导致Bus Fault 的那句代码是我故意写的用于触发Fault的。

69

1920

7

主题

帖子

精华

最后登录

2018-4-26

发消息

最后登录

2018-4-26

发消息

lk0305



该用户从未签到

40

1632

1

主题

帖子

精华

金牌会员

最后登录

2017-11-29

发消息

你好我好大家好！



该用户从未签到

首页

新闻

55

1214

0

主题

帖子

精华

creep



对地址0写0肯定是不允许的，这是为了模拟怎么找到错误代码的方法。
因为在一个功能复杂代码很多的程序里去直接定位跑飞（Fault）的代码不是很容易，所以可以使用这个方法去定位问题！

回复支持反对

举报

发表于 2015-7-4 22:11:17 | 只看该作者

9#

多谢分享！

STM32中国峰会纪念衫，免费申请>>

看峰会直播送STM32H7，戳我报名>>

回复

举报

发表于 2015-7-5 08:08:01 | 只看该作者

10#

楼主很强啊

资料下载论坛视频FAQ立刻购买积分换礼排行榜

快捷导航

回复支持反对

举报

该用户从未签到

下一 页 »

60

1920

7

主题

帖子

精华

返回列表

1

2

3

4

1 / 4 页

下一页

