ARM异常处理(4)：SVC和PendSV的作用详解

原创 tilblackout 于 2022-12-05 18:32:45 发布 4309 收藏 34 版权
分类专栏： ARM 文章标签： arm

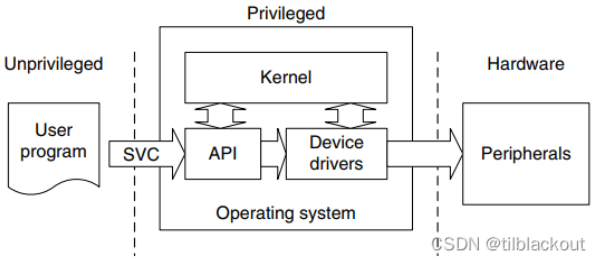
可以翻译为：管理调用 异常

SVC （Supervisor Call）和PendSV（Pendable Service Call）是针对软件和操作系统的两个异常。

1 SVC

SVC用于生成系统函数调用，例如，用户程序不允许直接访问硬件，操作系统可以通过SVC提供对硬件的访问。因此，当用户程序想要使用某些硬件时，可以使用SVC指令，然后执行操作系统中的软件异常处理程序，并提供用户应用程序请求的服务。通过这种方式，对硬件的访问由操作系统控制，操作系统可以阻止用户应用程序直接访问硬件，从而提供更可靠的系统。

SVC还可以使软件更具可移植性，因为用户程序不需要知道硬件的编程细节。用户程序只需要知道应用程序编程接口(API)函数ID和参数，而实际的硬件级编程是由设备驱动程序处理的。



SVC异常由SVC指令产生，该指令需要一个立即数 作为参数，根据这个参数执行不同的SVC处理函数。例：

```
SVC #0x3 ; 调用SVC函数3
SVC 0x3 ;  传统的语法(没有#)也可行
```

在C语言中，可以使用编译器关键字函数 __svc 或者使用内联汇编代码来执行SVC指令。

对于操作系统来说，当SVC处理程序被执行时，我们可以通过读取堆栈中的 PC 值来确定SVC指令中的立即数据值，然后从该地址读取指令并屏蔽不需要的位。如果使用的 PSP 堆栈，则还需要通过LR寄存器判断当前使用的是哪个堆栈。

SVC和软件中断指令(ARM7)

在ARM7中有一个软件中断指令SWI（Software interrupt instruction）。实际上，SVC指令的二进制编码与ARM7中的SWI是相同的。由于异常模型发生了变化，这条指令被重命名，以确保程序员能够正确地将软件代码从ARM7移植到Cortex-M3。

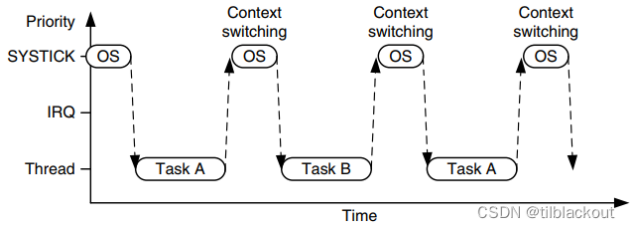
由于Cortex-M3中的中断优先级模型，我们不能在SVC处理程序中使用SVC指令(因为优先级与当前优先级相同)，这样做将导致 Usage fault 。出于同样的原因，在NMI处理程序或 Hard fault 处理程序中使用SVC也是不允许的。

2 PendSV

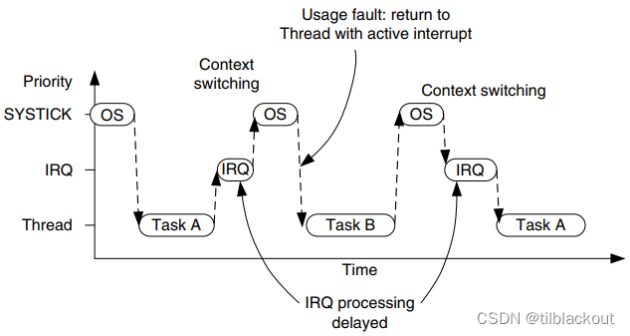
PendSV与操作系统中的SVC协同工作。SVC不能挂起，它将立即被执行；而PendSV可以暂时挂起异常，对于操作系统来说这很有用，它可以等待一个重要的任务执行完毕后再处理该异常。

PendSV异常通过向 NVIC Interrupt Control State Register 中的 PENDSVSET 置1来产生。

PendSV的一个典型应用就是上下文切换。例如，一个系统可能有两个任务，上下文切换可以通过调用 SVC 函数或被 Systick 触发。



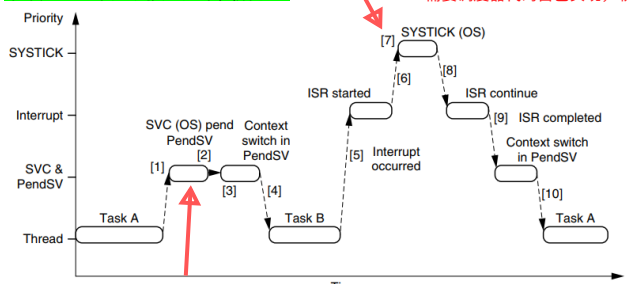
如果中断请求发生在 Systick 异常之前， Systick 异常将抢占IRQ处理程序。在这种情况下，操作系统不应该进行上下文切换，否则IRQ处理程序进程将被延迟执行。对于Cortex-M3，如果操作系统在中断active时试图切换到线程模式，可能会产生 Usage fault，如下图所示：



为了避免延迟处理IRQ处理的问题，一些操作系统在没有任何IRQ处理程序正在执行时才执行上下文切换。但这可能导致任务切换有很大的延迟，特别是当中断源的频率接近 Systick 异常的频率时。

PendSV异常通过延迟上下文切换请求直到IRQ处理程序完成来解决这个问题。为此，PendSV异常的优先级设置为最低，如果操作系统检测到一个IRQ当前处于活动状态(IRQ处理程序正在运行并且被 Systick 抢占)，它通过挂起PendSV异常来延迟上下文切换。如下图所示：

需要调度器代码自己实现，软件实现



SVC通过立即数执行某个函数，如此处 调用 “ 调度器 ” 函数。

调度器函数：
1. 判断当前环境是否为某个中断在激活状态；

2. 若是某个中断运行中，挂起当前异常；
若是没有中断运行，执行后续context switch；

(1)任务A调用SVC进行任务切换(如等待其它任务释放一个信号量)
(2)操作系统接收请求，准备上下文切换，并挂起PendSV异常。
(3)当CPU退出SVC时，它立即进入PendSV并进行上下文切换。
(4)当PendSV完成并返回到线程级别时，它执行任务B。
(5)IRQ产生并进入中断处理程序
(6)当运行中断处理程序时，发生 Systick 异常
(7)操作系统执行基本操作，然后挂起PendSV异常，为上下文切换做好准备
(8)当SYSTICK异常退出时，它返回到中断服务例程。
(9)当中断服务例程完成时，PendSV启动并执行实际的上下文切换操作。
(10)当PendSV完成时，程序返回到线程级别，继续执行任务A