

Esecuzione di interrupt handler (ARM)

All'indirizzo 0 si trova l'interrupt vector, che contiene una parola per ogni tipo di interrupt. Quella parola deve essere un'istruzione per l'esecuzione dell'handler appropriato (branch o load su PC).

Alcuni registri esistono in più copie (*banked registers*). In particolare, ciascun modo PL1 ha un proprio SP, LR e SPSR, e in fast interrupt anche R8-R12 sono copiati.

User	System	Fast Interrupt	Interrupt	Supervisor	Abort	Undefined
R0	R0	R0	R0	R0	R0	R0
R1	R1	R1	R1	R1	R1	R1
R2	R2	R2	R2	R2	R2	R2
R3	R3	R3	R3	R3	R3	R3
R4	R4	R4	R4	R4	R4	R4
R5	R5	R5	R5	R5	R5	R5
R6	R6	R6	R6	R6	R6	R6
R7	R7	R7	R7	R7	R7	R7
R8	R8	R8_fiq	R8	R8	R8	R8
R9	R9	R9_fiq	R9	R9	R9	R9
R10	R10	R10_fiq	R10	R10	R10	R10
R11	R11	R11_fiq	R11	R11	R11	R11
R12	R12	R12_fiq	R12	R12	R12	R12
R13 (SP)	R13 (SP)	R13_fiq	R13_irq	R13_svc	R13_abt	R13_und
R14 (LR)	R14 (LR)	R14_fiq	R14_irq	R14_svc	R14_abt	R14_und
R15 (PC)	R15 (PC)	R15 (PC)	R15 (PC)	R15 (PC)	R15 (PC)	R15 (PC)

Program Status Registers

CPSR	CPSR	CPSR	CPSR	CPSR	CPSR	CPSR
		SPSR_fiq	SPSR_irq	SPSR_svc	SPSR_abt	SPSR_und

Quando viene segnalato un interrupt:

- $LR_{mode} \leftarrow PC+4$;
- $SPSR_{mode} \leftarrow CPSR$;
- scrittura dei bit di modo nel CPSR;
- attivazione dei registri banked;
- disabilitazione degli interrupt (IRQ sempre, FIQ solo durante i fast interrupt);
- $PC \leftarrow$ indice mode.

Per esempio, per un SVC:

```
R14_svc = PC + 4
SPSR_svc = CPSR
CPSR[4:0] = 0x10011 // supervisor mode
CPSR[5] = 0          // ARM (non-thumb)
                      // FIQ non modificato
CPSR[7] = 1          // disabilita IRQ
PC = 0x00000008
```

L'handler deve salvare sullo stack tutti i registri non banked che modifica, e al termine per restituire il controllo:

- ripristina i registri salvati;
- $CPSR \leftarrow SPSR_{mode}$;
- $PC \leftarrow LR_{mode}-4$.

Questa operazione deve essere atomica, così come il trasferimento del controllo iniziale all'handler, per non avere uno stato non valido dei registri di controllo (PC, SP, CPSR) nel caso di ricezione di un'interrupt.

È necessario decrementare il LR banked di 4 perché è stato salvato PC+4, e gli interrupt vengono gestiti al termine dell'esecuzione delle istruzioni, quindi PC puntava già all'istruzione seguente.

Per ripristinare la SPSR si usa `movs pc, lr, subs pc, lr, xx` (tipicamente #4), o `ldmfd sp!, {PC, ...}`.