Università di Roma Tor Vergata
Corso di Laurea triennale in Informatica

Sistemi operativi e reti

A.A. 2016-17

Pietro Frasca

Lezione 15

Giovedì 1-12-2016

Gestione degli errori e delle eccezioni

- Durante un'operazione di ingresso/uscita si possono verificare molte eccezioni.
- Alcune di queste possono essere dovute a guasti hardware che si possono verificare nei dispositivi come, ad esempio, la rottura di una testina di lettura/scrittura di un disco.
- In altri casi, meno gravi, l'eccezione, può essere causata da uno stato particolare in cui si può trovare un dispositivo. Ad esempio, in fase di stampa la mancanza della carta nel vassoio della stampante o, in fase di lettura di un file da un DVD, lo sportello non completamente chiuso.

- Altre eccezioni possono essere originate da errori di programmazione come, ad esempio, il tentativo di comunicare con un dispositivo non connesso al computer, o semplicemente spento, oppure il tentativo di aprire un file inesistente.
- E' necessario che tutte le suddette eccezioni siano adeguatamente gestite affinché i processi possano completare la loro esecuzione in modo corretto. Se non è possibile risolvere l'eccezione è necessario far eseguire ai processi funzioni di programma alternativi.
- Per via dell'organizzazione stratificata del sottosistema di I/O la gestione delle eccezioni è **svolto all'interno dei diversi livelli**.
- In genere è **conveniente gestire le eccezioni localmente**, a partire dal livello hardware, propagandola al livello superiore soltanto nel caso in cui non sia stato possibile gestirla completamente.

- Per esempio, molti problemi di funzionamento che sono rilevati dal controllore di un dispositivo sono dovuti a inconvenienti temporanei come nel caso di un errore in lettura da DVD causato da dalla superficie del disco polverosa e rilevato dal controllo di parità o di *checksum.*
- In questi casi è il driver del dispositivo che tenta di recuperare il corretto funzionamento, ad esempio ripetendo più volte l'operazione. Se il driver non riesce a risolvere il problema, propaga l'eccezione al livello superiore.
- Anche nel livello indipendente dai dispositivi sono implementate routine di gestione delle eccezioni, in particolare di tutte quelle che si verificano a questo livello oltre a quelli propagati dal livello inferiore.
- In casi sfortunati l'eccezione arriva a livello di applicazione, dove è necessario gestirla per non mandare in crash il processo.
- Per rendere più robusto il software applicativo i linguaggi di programmazione, come ad esempio Java, obbligano il programmatore ad occuparsi delle possibili eccezioni.

Allocazione dei dispositivi e tecniche di spooling

I dispositivi, secondo le loro caratteristiche, possono essere allocati ad un processo alla volta o essere condivisi tra più processi contemporaneamente.

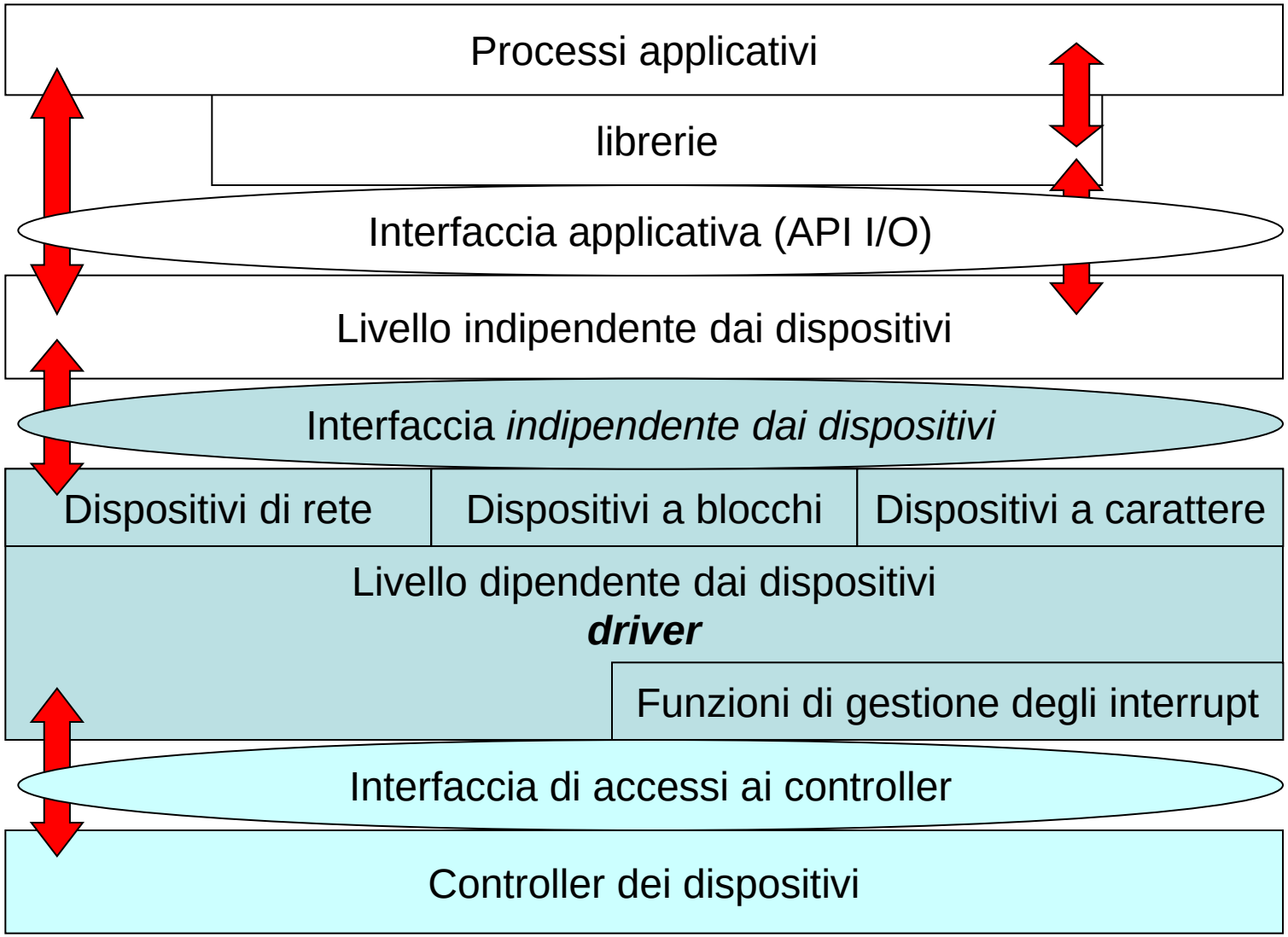
- Per esempio, un disco è una risorsa condivisa poiché più processi, leggono e/o scrivono file memorizzati sullo stesso disco.
- In altri casi, ad esempio nel caso di una stampante, il dispositivo deve essere assegnato a un processo per volta per evitare che pagine appartenenti a un processo siano alternate a pagine di altri processi.
- Per i dispositivi lenti, una tecnica spesso utilizzata al posto dell'allocazione dinamica di un dispositivo è la tecnica di ***spooling (spool -* Simultaneous Peripheral Operations On-line**) che consente di ridurre i tempi di attesa a un processo applicativo che, nel richiedere l'uso esclusivo del dispositivo, e trovandolo già occupato, deve attendere il suo rilascio per un tempo spesso lungo e non facilmente prevedibile.
- Tale tecnica è spesso usata per risorse come la stampante. In questo caso il processo applicativo non invia dati direttamente alla stampante ma genera file di stampa in una directory del disco, detta **directory di spool**.

- I file contenuti in questa directory saranno successivamente elaborati da un processo di sistema che si occupa della gestione della stampante.
- Dinamicamente si viene quindi a creare una **lista di *file di spool*** in attesa di essere letti e inviati in stampa dal processo di sistema uno alla volta.
- La coda dei file che si crea è visibile all'utente che in ogni momento può gestire tale coda (in base a determinati diritti di accesso) rimuovendo, ad esempio, alcuni dei file in attesa.
- Ad esempio, in unix un *demone* (processo di sistema che svolge un servizio) di stampa molto usato è **lpd (line printer daemon)**, e il client di stampa è **lpr (line printer)**. L'utente per gestire la coda di stampa può usare l'utility **lpq** (**line printer queue**) che consente di visualizzare i job in coda ed eventualmente rimuoverli con **lprm.** Inoltre può usare **lpc (line printer control)** per visualizzare lo stato delle code e intervenire su alcune problematiche del funzionamento delle stampanti (per il completo controllo dei comandi lcp è necessario avere i diritti di root).

- Come già detto, un disco è condiviso tra più processi. Le operazioni di lettura e/o scrittura dei vari processi non avvengono contemporaneamente, ma in sequenza. Pertanto si gestiscono le richieste mediante una lista. Quindi, dinamicamente si forma una coda di richieste di accesso ai settori del disco da parte di processi diversi, che devono essere soddisfatte una alla volta, in un ordine stabilito da qualche strategia.
- Nasce quindi il problema di come ordinare le esecuzioni di tutti i trasferimenti pendenti.
- Le politiche di schedulazione più semplici sono la **FIFO** che evita sicuramente lo ***starvation***, oppure quelle **basate sulle priorità** dei processi che hanno richiesto il trasferimento.
- Spesso, però, tenendo conto delle caratteristiche hardware dei dischi si preferisce realizzare una **diversa politica di schedulazione**.

- Infatti il tempo medio di accesso al disco dipende soprattutto da due parametri: il primo, e più rilevante è detto **tempo di *seek*** che è l'intervallo di tempo necessario per spostare la testina dalla posizione corrente alla posizione desiderata. Questo tempo di spostamento meccanico della testina è di alcuni ordini di grandezza superiore al tempo effettivo per il trasferimento dei dati. C'è, inoltre, anche da considerare il **tempo di rotazione** necessario affinché il settore su cui operare passi sotto la testina. In base a queste considerazioni, per ridurre il tempo medio di accesso, è necessario ridurre il tempo di seek e pertanto si preferiscono algoritmi di schedulazione che, istante per istante, selezionano il trasferimento che riguarda una delle tracce più vicine a quella su cui è posizionata la testina.

Struttura logica del sottosistema di I/O



Livello dipendente dai dispositivi

- Questo livello del sottosistema di I/O ha il compito di nascondere ai livelli soprastanti tutti i dettagli relativi ai controller e ai relativi dispositivi definendo un'**interfaccia *indipendente dai dispositivi (driver)***.
- Ogni dispositivo è rappresentato mediante una **struttura dati** *detta* ***descrittore di dispositivo*** a cui è possibile accedere mediante le funzioni che fanno parte del driver.
- Ciascuna di queste funzioni, spesso realizzata in linguaggio assembly, invia gli opportuni comandi ai registri del controllore del dispositivo mediante le istruzioni di I/O, e coordina in tal modo le operazioni del dispositivo.
- Poiché esiste una grande varietà di dispositivi e molteplici modi di funzionare, i driver hanno interfacce con caratteristiche differenti, in base al tipo di dispositivo.

- Per esempio generalmente le funzioni di accesso ai **dispositivi a blocchi** sono diverse dalle funzioni con cui si accede ai **dispositivi a carattere** o ai **dispositivi di rete** (vedi figura). Nel caso di dispositivi a blocchi si accede ai dispostivi tramite funzioni del tipo **read, write**, **seek**, mentre l'accesso a un dispositivo a carattere avviene con funzioni del tipo **get o put**.
- Alcune funzioni appartenenti all'interfaccia del driver hanno le stesse *"firme"* delle funzioni del livello di interfaccia applicativa (spesso si aggiunge il carattere _ davanti al nome). Ad esempio le due tipiche funzioni di accesso in lettura e scrittura su un dispositivo, possono avere la seguente firma:

```
n = _read (dispositivo, buffer, nbytes);
n = _write (dispositivo, buffer, nbytes);
```

dove, rispetto alle corrispondenti funzioni dell'interfaccia applicativa è diverso il modo di identificare il dispositivo, non più mediante nomi simbolici ma con indirizzi (fisici o virtuali) e ora il buffer è posto nel kernel e non nell'area virtuale del processo applicativo.

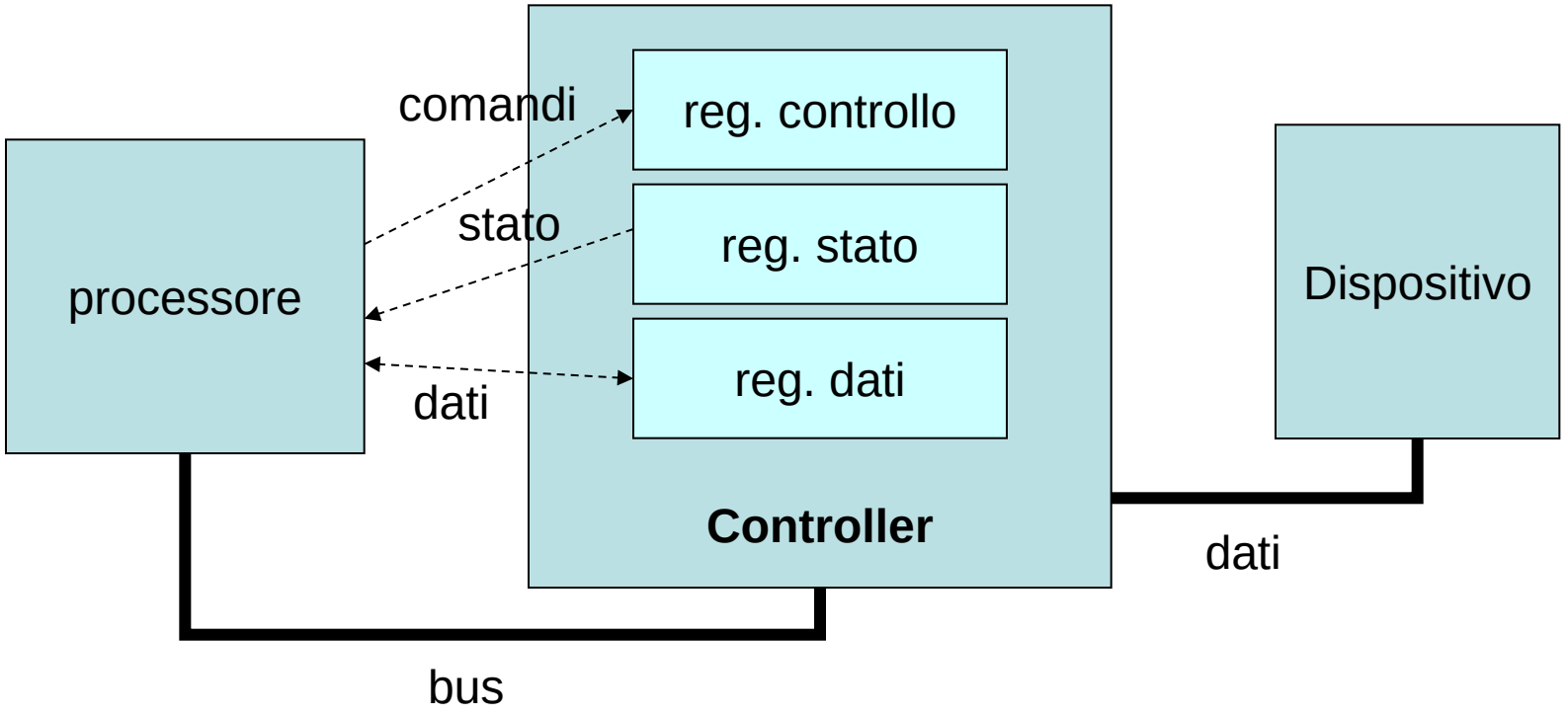
- Le principali funzioni svolte dal driver sono
  - **attivare il dispositivo;**
  - **eseguire la funzione richiesta;**
  - **gestire localmente le eccezioni che si possono risolvere o, altrimenti, interrompere l'operazione e propagarle al livello superiore;**
  - **sincronizzare il processo applicativo che ha richiesto l'operazione con la fine dell'operazione stessa;**
  - **disattivare il dispositivo alla fine dell'operazione.**

- E’ bene notare che le operazioni svolte da un dispositivo sono concorrenti e asincrone con le operazioni svolte dal processore. Infatti, generalmente il controller di un dispositivo utilizza un **processore specializzato**, che esegue i microprogrammi memorizzati nel suo **firmware**, che svolgono particolari operazioni e in modo indipendente dalla CPU.
- Pertanto le funzioni di *I/O* possono essere realizzate in modo che si comportino in modo **asincrono** nei confronti del processo applicativo che le chiama. Ad esempio la funzione **read**, quando è chiamata da un processo applicativo, attiva la lettura di dati da un dispositivo e termina restituendo il controllo al processo chiamante, il quale continua la sua esecuzione in parallelo con le operazioni svolte dal dispositivo.
- Il funzionamento asincrono è generalmente più efficiente del sincrono, ma è anche più complesso poiché, durante la sua esecuzione il processo deve poi stabilire quando termina l’operazione.

- Con la ***modalità sincrona***, invece, un processo è sospeso dopo aver chiamato una funzione di I/O, per essere riattivato alla fine dell'operazione.
- Poiché in realtà le operazione svolte da un processo applicativo sono asincrone a quelle svolte da un dispositivo, è necessario sincronizzare le loro attività ricorrendo al meccanismo hardware delle interruzioni per garantire il comportamento sincrono.
- Se infatti un dispositivo funziona a **interruzione di programma**, alla fine di ogni operazione il controller invia alla CPU un segnale di interruzione per ottenere la corretta sincronizzazione. Per questo motivo, l'insieme delle funzioni di servizio delle interruzioni provenienti dai dispositivi *(interrupt handler)* sono incluse nel ***livello dipendente dai dispositivi***.

Controller di un dispositivo

- La figura seguente mostra una schema semplificato di un controller di un dispositivo.
- Come già descritto, la CPU comunica con il controller tramite i registri di cui esso è dotato e che sono indirizzati mediante le istruzioni macchina di I/O e/o con le stesse istruzioni usate per l'accesso alla memoria principale (memory mapped).
- Il numero e il tipo dei registri presenti nel controller varia a seconda del dispositivo e dipende dalla complessità delle funzioni che il dispositivo è in grado di svolgere.
- In modo molto semplificato possiamo distinguere la presenza di tre registri (o gruppi di registri) indicati con i nomi di ***registro di controllo***, ***registro di stato*** e ***registro dati*** (o buffer del controller).



Controllore di un dispositivo

- Il **registro di controllo** consente alla CPU di programmare il funzionamento del dispositivo. Tipicamente, è un **registro in sola scrittura** nel quale la CPU può scrivere valori che rappresentano i **codici operativi** che specificano le operazioni che il dispositivo deve svolgere.
- Spesso è presente un bit *(**bit di abilitazione alle interruzioni**)* che consente di abilitare il controller a inviare un segnale di interruzione alla CPU (o al DMA) alla fine dell'operazione svolta dal dispositivo.
- Il **registro di stato** è un registro in **sola lettura** ed è utilizzato dal controller per segnalare la stato in cui si trova il dispositivo, e che può quindi essere letto dalla CPU.
- Nel registro di stato è presente generalmente un bit *(**flag end_flag**)* che il controller setta alla **fine di un'operazione** da parte del dispositivo. Quando il valore del flag passa da zero a uno, se il dispositivo è stato abilitato alle interruzioni, viene inviato un segnale d'interruzione alla CPU.
- Sono presenti inoltre uno o più bit che specificano il codice dell'eccezione che può verificarsi durante le operazioni del dispositivo.

- Infine, il **registro dati** rappresenta il **buffer del controllore** nel quale la CPU inserisce i dati da trasferire in output, o dal quale preleva i dati letti in fase di input.

Funzionamento del dispositivo

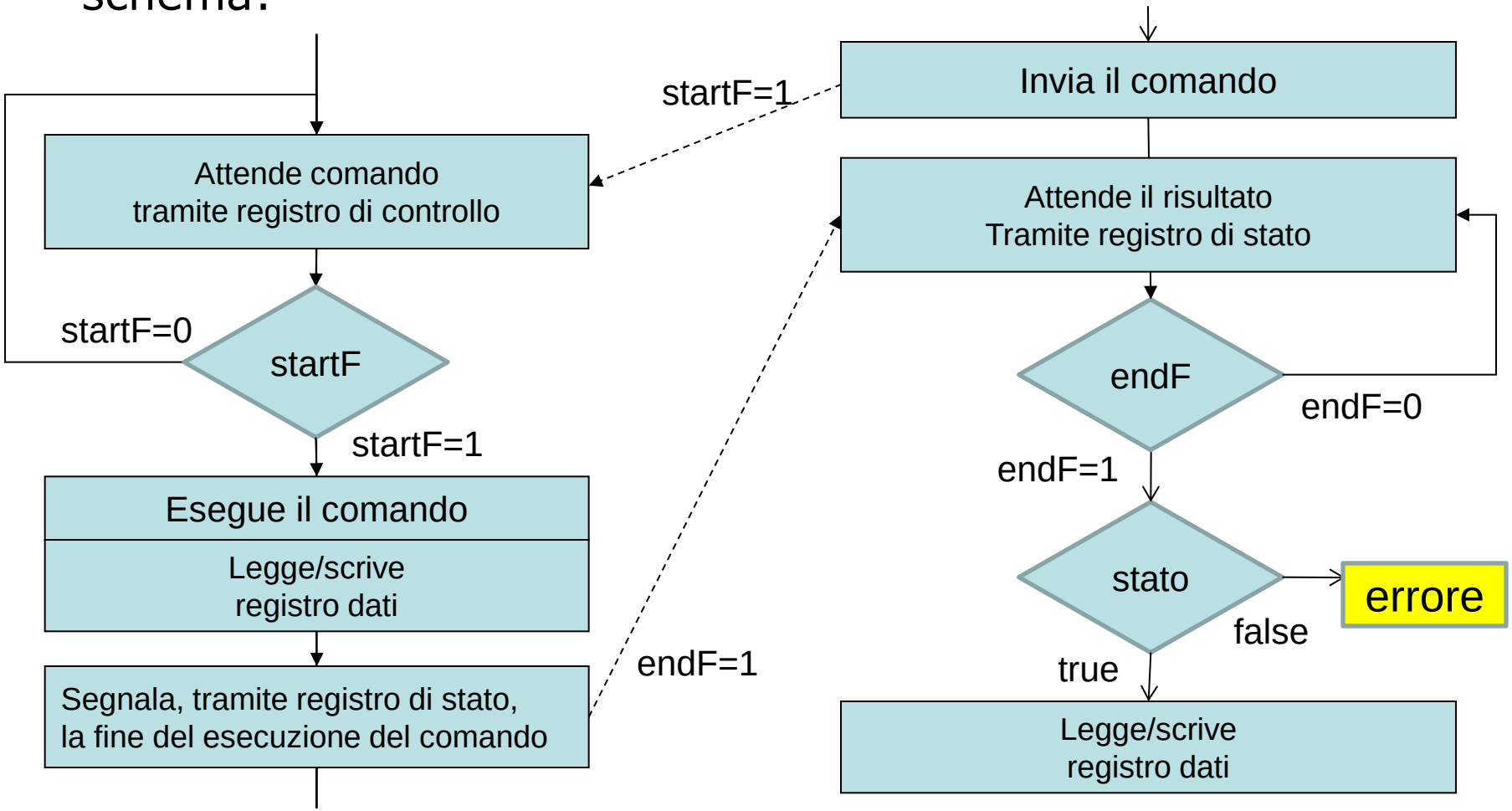
- In pratica, ogni dispositivo esegue una sequenza di operazioni relative a routine implementate nel firmware del dispositivo che funziona in parallelo alla CPU.
- Indicheremo questo processo col termine di ***processo dispositivo***. Il dispositivo esegue le seguenti operazioni:
  - **attende di ricevere un comando;**
  - **Una volta ricevuto il comando, esegue le operazioni ad esso corrispondenti, comunicando con la CPU mediante il registro dati;**
  - **alla fine dell'operazione registra l'esito nel registro di stato.**
  - **Quindi ripete il ciclo e si pone di nuovo in *stand-by* in attesa di una nuovo comando.**

- In pratica è come se il processo dispositivo eseguisse il seguente codice:

```
while (true) {
        while (startF==0);//attesa invio di un comando
        <ESEGUE COMANDO>;
        <REGISTRA ESITO DEL COMANDO>
        endF=1;
   }
```

Comunicazione tra processo e dispositivo

- Processo e dispositivo comunicano in base al seguente schema:



Gestione di un dispositivo mediante controllo di programma

In base allo schema della figura precedente, il processo applicativo esegue, per effettuare il trasferimento dei dati (ad esempio lettura di N dati), un codice del tipo:

```
endf=0;
for (i=0;i<N;i++){
    <PREPARA IL COMANDO>
    <INVIA IL COMANDO tra cui startF=1>;
    while (endF==0);  /* ciclo di attesa sul flag
                         endF */
    // attende la fine del comando
    <VERIFICA L'ESITO>;
    /* fa il test del registro di stato  per
       eventuali errori */
    if (stato)
          <LEGGI IL DATO DAL REGISTRO DATI>;
}
```

- Il processo, per N volte, deve attendere che il dato sia disponibile nel registro dati del controllore. Si tratta di un **ciclo di attesa attivo (polling)**.
- Generalmente, questo schema **non è adatto per essere usato nei SO multiprogrammati**, dove è invece conveniente sospendere un processo quando è in attesa di un particolare evento.

Gestione di un dispositivo mediante interruzione

- Questa tecnica, consente ad un processo applicativo di sospendersi fino a quando il dato è pronto.
- Il processo si sospende utilizzando un **semaforo inizializzato a zero** e chiamando una **wait** su tale semaforo.
- Chiamando il **semaforo *dato_pronto*** si ha:

```
semaforo dato_pronto;
dato_pronto.value = 0;
for (int=0;i++;i<N){
    <PREPARA IL COMANDO>;
    <INVIA IL COMANDO tra cui startF=1>;
    wait(dato_pronto); //attesa del dato
    <VERIFICA L'ESITO>;
    // fa il test del registro di stato status
       per eventuali errori
    if (stato)
          <LEGGI IL DATO DAL REGISTRO DATI>;
 }
```

- In base allo pseudo-codice precedente, il processo chiamando la funzione **wait(dato_pronto)** viene sospeso, in quanto il semaforo è inizializzato a **0**.
- Dovrà essere il controller del dispositivo quindi a **risvegliare il processo applicativo**, quando il dato sarà pronto.
- Il dispositivo deve essere programmato in modo che possa generare un **segnale di interruzione** quando il dato è pronto (settando il bit di abilitazione delle interruzioni nel registro di controllo).
- Quando il controller genera l'interruzione va in esecuzione la ***funzione di servizio relativa all' interruzione del dispositivo***. Questa funzione conterrà la chiamata di sistema **signal** sul semaforo che consentirà di risvegliare il processo sospeso. Per il precedente esempio eseguirà quindi **signal(dato_pronto).**

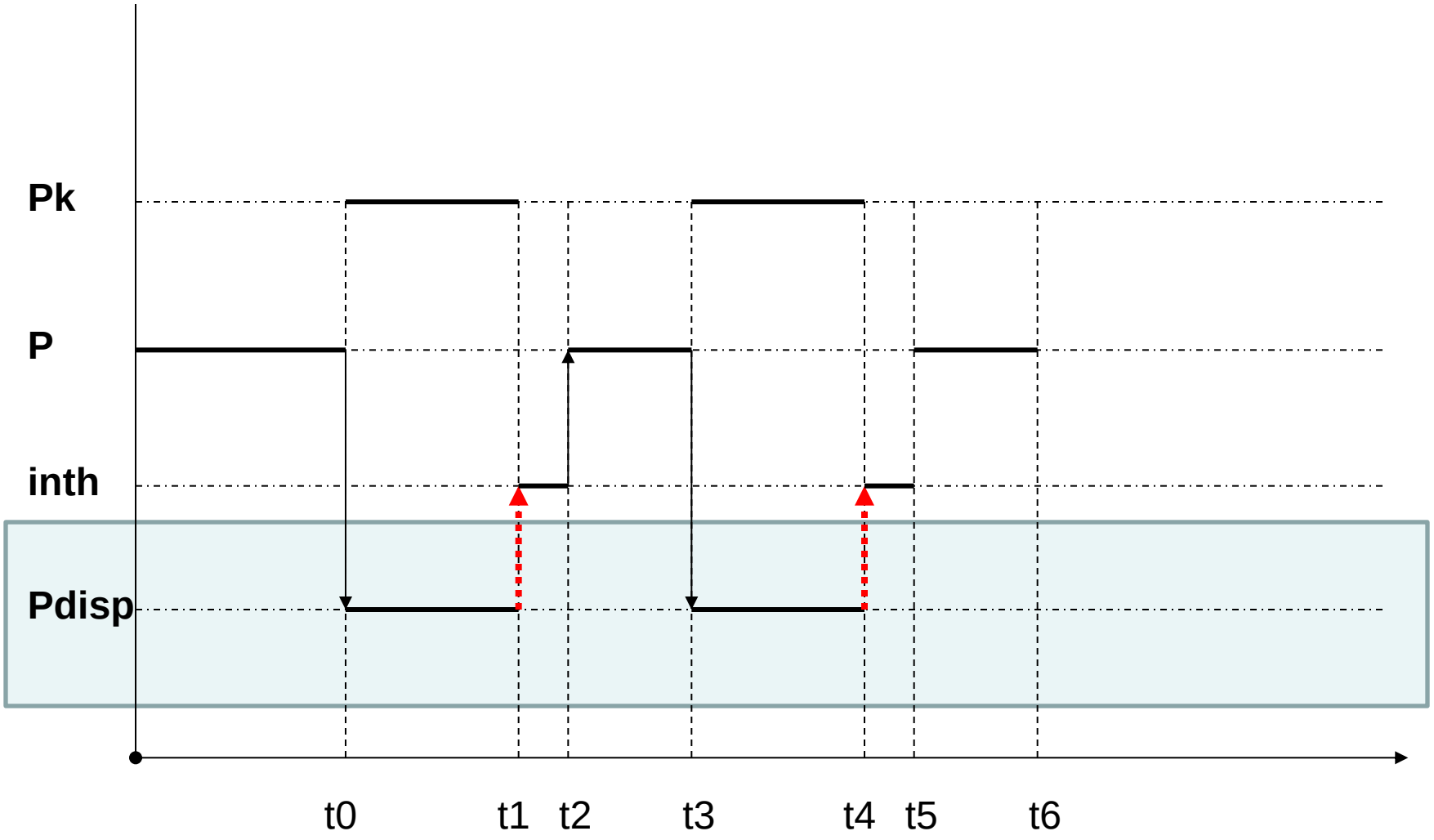


Diagramma temporale della gestione a interruzione

- La tecnica di **gestione di un dispositivo a interruzione di programma**, è poco efficiente poiché **sospende per N volte consecutive il processo applicativo** che deve eseguire il trasferimento dei dati, generando continui cambi di contesto i quali producono un eccessivo overhead.

Descrittore di un dispositivo

- Una soluzione al problema di cui sopra consiste nel fornire al processo applicativo una funzione di sistema che consenta di specificare il numero di dati da trasferire e l'indirizzo di memoria dove i dati devono essere trasferiti (o da prelevare nel caso di operazione di scrittura).
- Il diagramma temporale della figura seguente mostra il funzionamento di tale soluzione.
- Ora il processo **P** che esegue il trasferimento di dati resta bloccato fino al termine del trasferimento.
- Per ottenere questo tipo di funzionamento è necessario che la routine di interruzione **inth** riesca a distinguere tra le interruzioni intermedie che provvedono a trasferire un blocco di dati da quella finale che provvede a risvegliare il processo P.

- Una soluzione a questo problema consiste nel utilizzare una struttura dati che descrive il dispositivo alla quale possano accedere sia il processo applicativo, mediante le funzioni dell'interfaccia ***indipendente dai dispositivi***, sia la funzione **inth** che gestisce le interruzioni lanciate dal dispositivo.
- Il descrittore del dispositivo insieme alle funzioni del sistema dipendenti dal dispositivo e alla funzione di interruzione costituiscono il **driver del dispositivo**.
- Il descrittore del dispositivo ha il compito di:
  - **Nascondere le informazioni associate al dispositivo**
  - **Consentire la comunicazione di informazioni tra il processo applicativo e il dispositivo.**

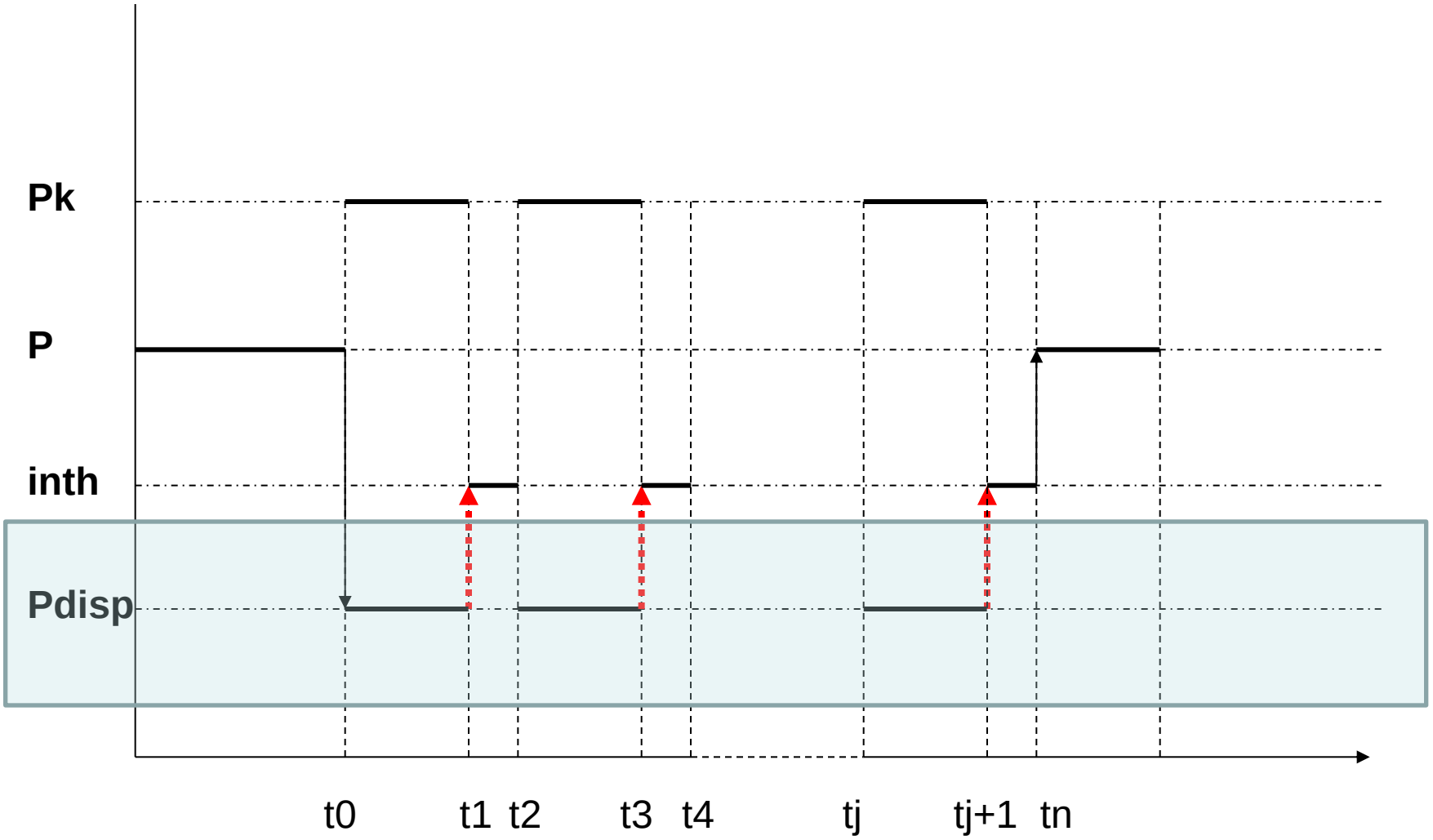


Diagramma temporale della gestione a interruzione
Trasferimento di N dati consecutivi

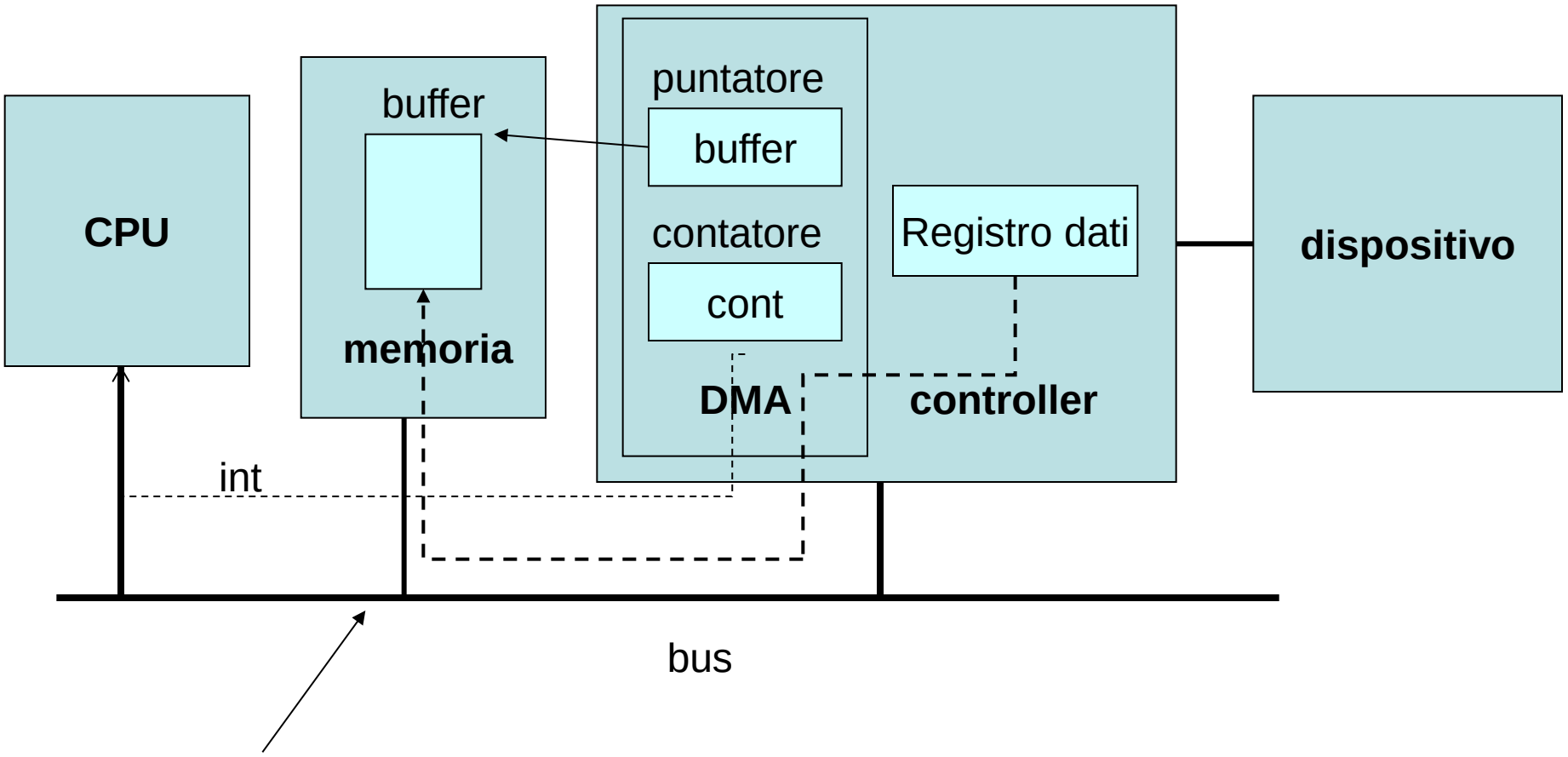
La struttura dati del descrittore di dispositivo

- Il descrittore varia molto in dipendenza della complessità del dispositivo. Una tipica struttura contiene i seguenti campi:
  - tre campi contenenti gli indirizzi dei registri del controllore del dispositivo **controllo**, **dati e stato**;
  - un campo **`dato_pronto`** di tipo semaforo per la sincronizzazione tra il processo applicativo e la funzione **inth** di risposta alle interruzioni generate dal dispositivo;
  - un campo **`contatore`** per indicare il numero di byte da trasferire;
  - un campo **`pBuffer`** per contenere l'indirizzo di memoria del buffer in cui (o da cui) trasferire i dati;
  - un campo **`stato`** per memorizzare l'esito delle operazioni svolte dal dispositivo.

Esempio di descrittore di dispositivo

Gestione di un dispositivo con DMA

- Il DMA consente di trasferire i dati dal registro del controllore direttamente in memoria tramite i bus di sistema operando in cycle stealing (cioè condivide il bus di sistema con la CPU).
- Questa tecnica riduce il tempo di trasferimento di un blocco di dati e consente alla CPU di svolgere altri compiti.
- Il DMA genera un segnale di interruzione per ogni blocco di dati, pronto per essere trasferito in memoria.
- Nel DMA sono presenti due registri **contatore** e **puntatore.** Nel primo sarà scritto il numero di byte (o parole) da trasferire e nel secondo l'indirizzo di memoria ove iniziare il trasferimento.
- Il contatore viene decrementato e il puntatore sarà incrementato per ogni byte trasferito. Quando il contatore assume il valore 0, il DMA invia alla CPU un segnale di interruzione.
- I DMA sono usati nei dispositivi a blocchi.



L'uso del bus viene condiviso tra CPU e DMA