

•Paolo Cremonesi


Impianti Informatici

 POLITECNICO DI MILANO



Affidabilità empirica: misurare l'affidabilità

- MTTF
- MTTR
- life test experiment
- failure terminated
- time terminated
- con rimpiazzo
- senza rimpiazzo

2

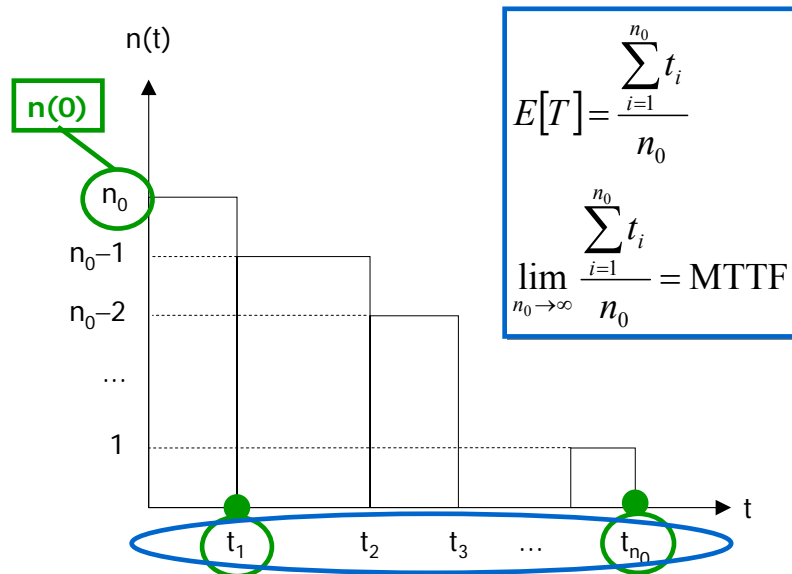
- Misurare la reliability
- Misurare la maintainability

Impianti Informatici

POLITECNICO DI MILANO

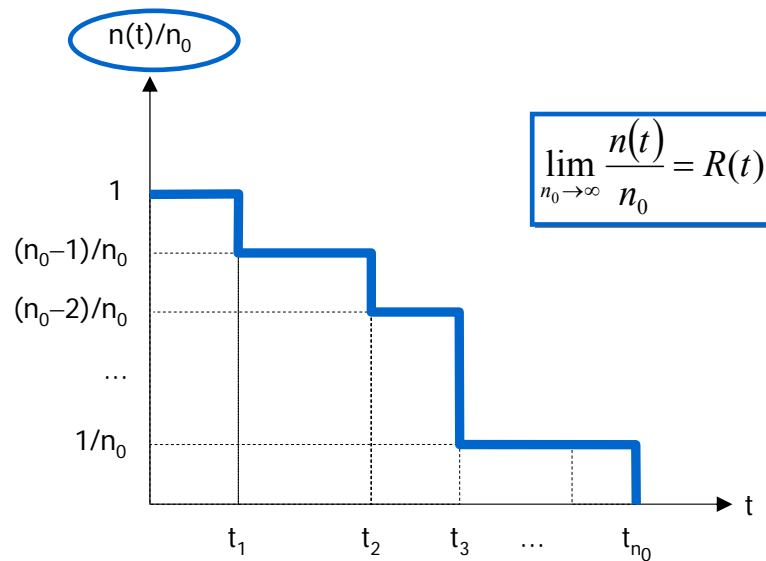
In questo modulo vedremo innanzitutto come ricavare in modo empirico la reliability di un componente e le grandezze ad essa legate (ossia, MTTF e failure rate)

- In seguito vedremo come stimare la maintainability di un componente, ed in particolare il MTTR



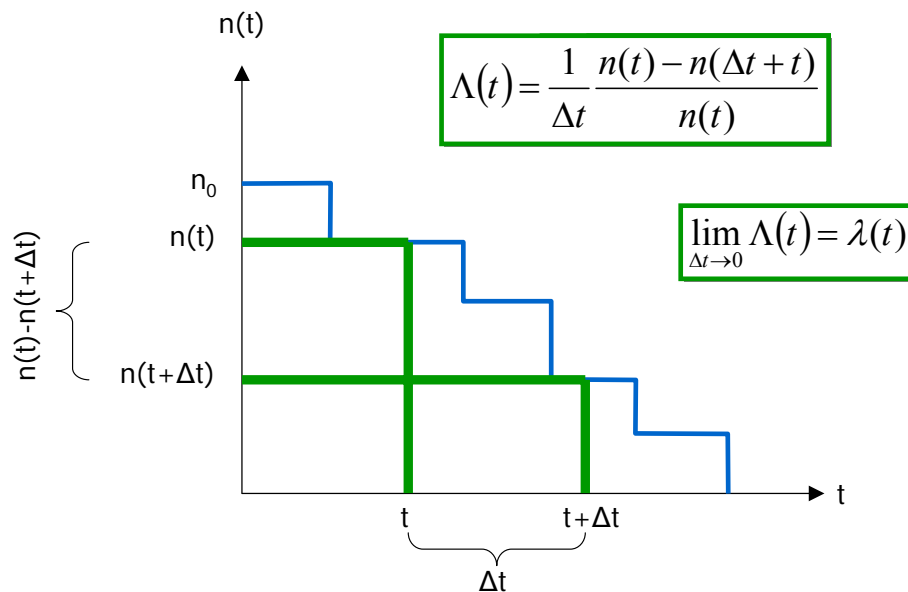
Consideriamo n_0 elementi indipendenti e statisticamente identici che vengano messi in esercizio al tempo $t=0$ alle stesse condizioni

- Indichiamo con $n(t)$ il numero di elementi che, al tempo t , non si sono ancora guastati
- Avremo che $n(0) = n_0$
- Indichiamo con t_1 l'istante di tempo in cui si è guastato il primo elemento
- E' evidente che per $t = t_1$ il numero di elementi ancora funzionanti è pari a $n_0 - 1$
- In modo analogo indichiamo con t_2, t_3 e così via gli istanti di tempo in cui si sono guastati il secondo, poi il terzo e componente, e così via
- Indichiamo infine con t_{n_0} l'istante di tempo in cui si è guastato l'ultimo degli n_0 elementi
- I tempi al guasto (ossia, t_1, t_2, t_3 fino a t_{n_0}) sono valori indipendenti della variabile casuale T che rappresenta il tempo al guasto dell'elemento. In altre parole, t_1, t_2, t_3 e così via sono valori campionati dalla distribuzione che misura la reliability dei componenti. Infatti gli n_0 elementi, essendo identici, hanno tutti la stessa reliability
- A questo punto possiamo calcolare in modo empirico il MTTF come media aritmetica degli n_0 valori t_1, t_2, t_3 e così via. Per $n_0 \rightarrow \infty$ il valore calcolato converge al valore teorico del MTTF



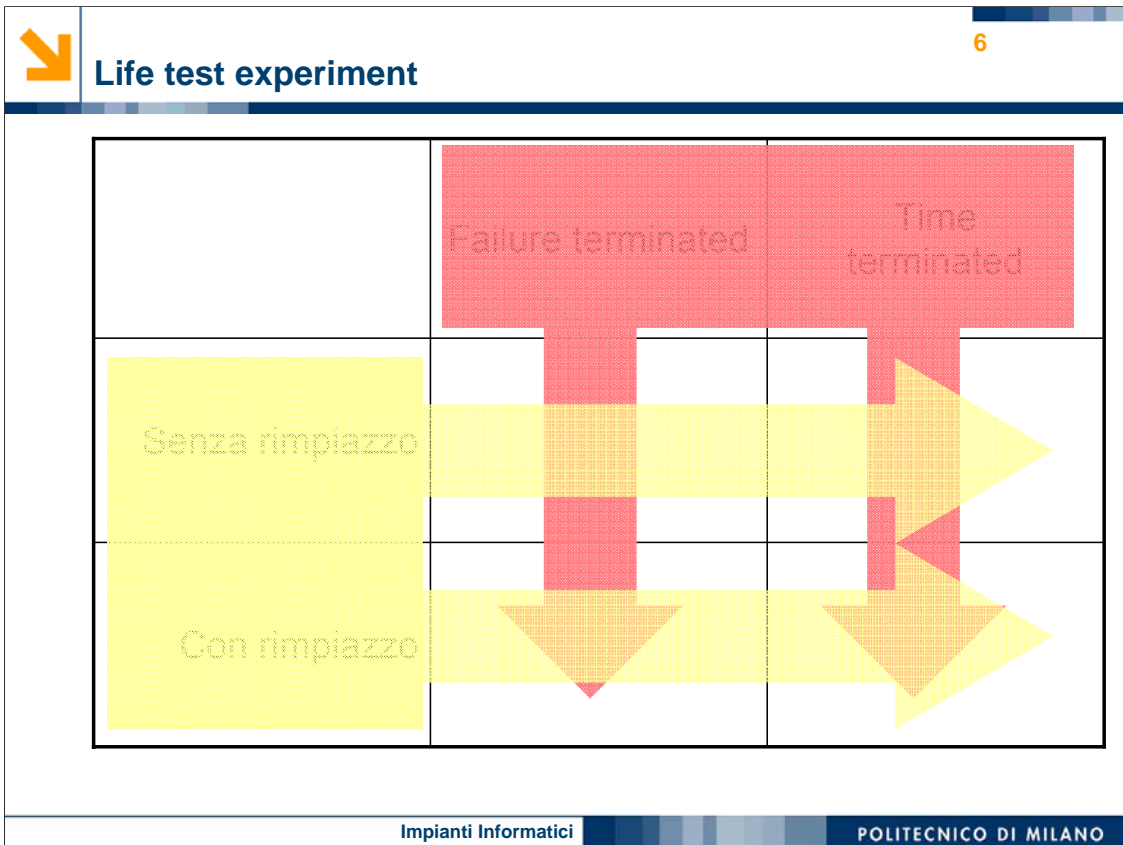
Supponiamo ora di normalizzare il numero dei componenti funzionanti rispetto a n_0 .

- Quello che stiamo facendo è di calcolare la percentuale di elementi funzionanti in funzione del tempo
- La funzione $n(t)/n_0$ è la funzione empirica di affidabilità
- Per $n_0 \rightarrow \infty$ converge all'affidabilità teorica degli elementi sotto test



Calcoliamo ora il numero di elemento che si sono guastati in un intervallo di tempo Δt

- Il numero di elemento che si sono guastati in un intervallo di tempo Δt è dato dalla differenza tra il numero $n(t)$ di componenti funzionanti al tempo t e il numero $n(t + \Delta t)$ che rappresenta il numero di componenti funzionanti al tempo $t + \Delta t$
- Se dividiamo il numero di elementi che si sono guastati nell'intervallo Δt per il numero di elementi $n(t)$ che erano funzionanti all'inizio dell'intervallo, otteniamo la **percentuale** di elementi che si sono guastati nell'intervallo Δt
- Se dividiamo questa percentuale per Δt otteniamo la frazione di elementi che si guastano nell'unità di tempo, ossia la **velocità** con cui avvengono guasti
- Questa grandezza prende il nome di failure rate empirico ed è indicato con Λ
- Si può dimostrare che il per $\Delta t \rightarrow 0$ di Λ converge al failure rate λ



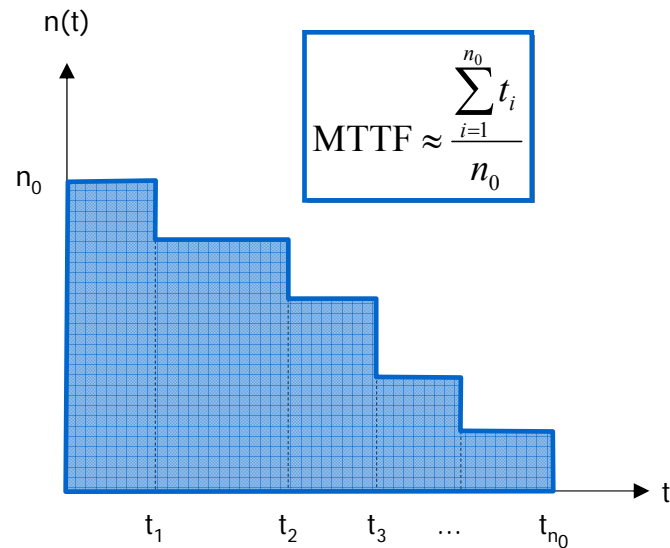
Per misurare effettivamente il MTTF di un componente si utilizzano degli esperimenti simili a quello descritto nei lucidi precedenti, in cui un certo numero di componenti identiche vengono osservate per un certo periodo di tempo e si conta quante di queste si sono guastate e quando. Questi esperimenti prendono il nome di *life test experiment*

I *life test experiment* si dividono quattro categorie ottenute come combinazione di due parametri di scelta.

- Il primo parametro di scelta è legato alla durata dell'esperimento: un esperimento può terminare quando si sono rotti un certo numero di componenti (in questo caso si dice che è *failure terminated*), oppure dopo un periodo di tempo prefissato (e in questo caso si dice che è *time terminated*)
- Il secondo parametro di scelta è legato a cosa si fa quando un componente si rompe durante l'esperimento. Si può decidere di non sostituire il componente rotto (e quindi man mano che l'esperimento prosegue il numero di componenti funzionanti diminuisce), oppure si può decidere di sostituire il componente rotto con un altro nuovo, in modo tale da mantenere costante durante l'esperimento il numero di componenti funzionanti. Quest'ultima soluzione ha il pregio di fornire una stima più precisa del MTTF a parità di durata dell'esperimento, ma ovviamente è una scelta più costosa perché è necessario usare un maggior numero di componenti

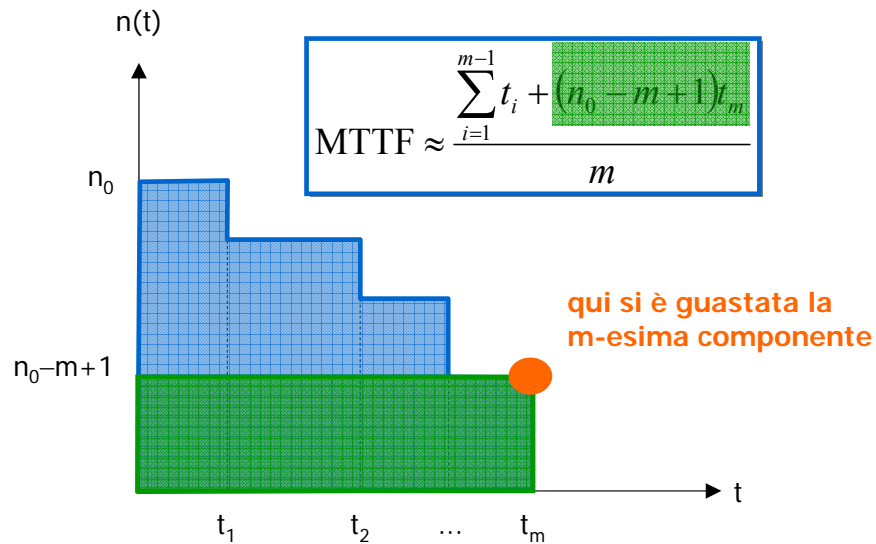
Life test experiment		
	Failure terminated	Time terminated
Senza rimpiazzo		
Con rimpiazzo		

Vediamo ora i life test experiment failure-terminated senza rimpiazzo



Questo tipo di esperimenti sono molto simili a quanto visto in precedenza per la definizione del MTTF empirico.

- Riguardando la definizione di MTTF si nota come il numeratore rappresenti l'area sottesa dalla funzione $n(t)$, ossia il tempo totale di funzionamento di tutti i componenti presenti nel sistema

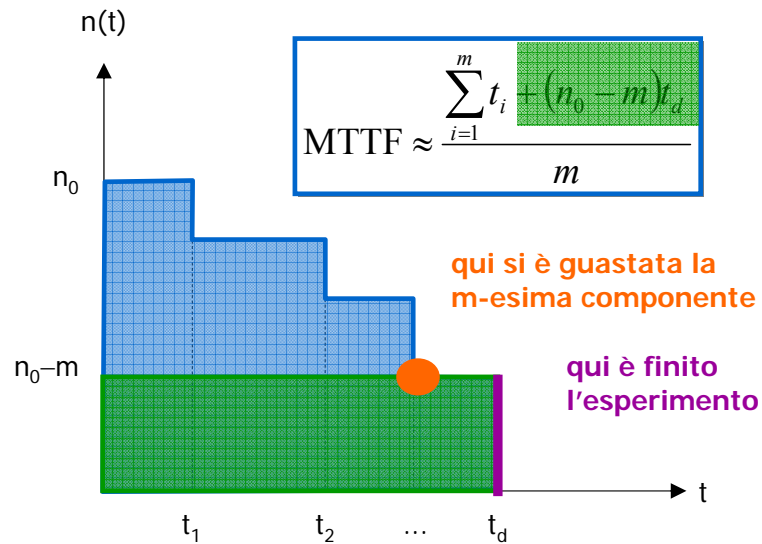


Il concetto può essere esteso agli esperimenti failure-terminated senza rimpiazzo. Questi esperimenti terminano dopo che si sono guastati un certo numero m di componenti (indichiamo con t_m tale istante).

- In questo caso il numeratore viene modificato per tener conto del fatto che alcune componenti non si sono guastate

Life test experiment		
	Failure terminated	Time terminated
Senza rimpiazzo		
Con rimpiazzo		

Vediamo ora i life test experiment time-terminated senza rimpiazzo

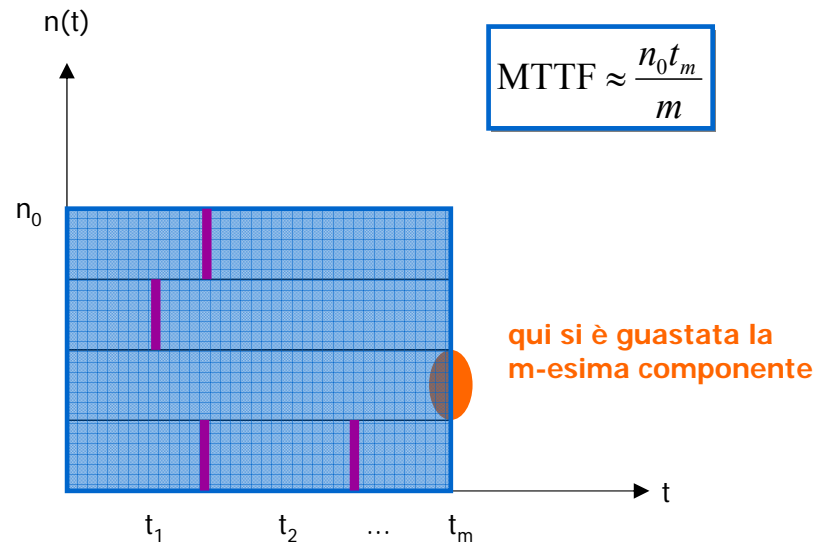


Nel caso di esperimenti time-terminated senza rimpiazzo la formula per il calcolo del MTTF è molto simile al caso precedente anche se alcuni termini cambiano leggermente di significato.

- Questi esperimenti terminano dopo un tempo prefissato t_d
- Durante questo periodo si sono guastati un certo numero m di componenti

Life test experiment		
	Failure terminated	Time terminated
Senza rimpiazzo		
Con rimpiazzo		

Vediamo ora i life test experiment con rimpiazzo failure terminated

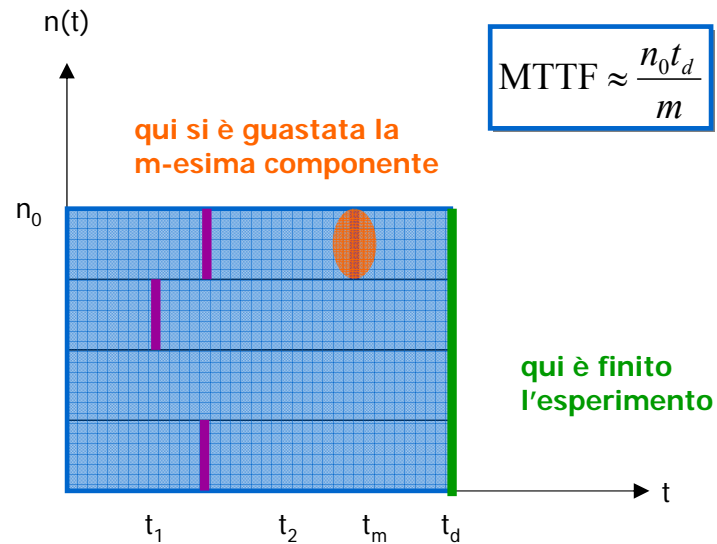


Questi esperimenti terminano al tempo t_m dopo che si sono guastati un certo numero prefissato m di componenti

- ma ogni volta che si guasta un componente questo viene sostituito con un componente nuovo
- Anche in questo caso la stima del MTTF è pari all'area che rappresenta la vita totale di tutti i componenti, diviso il numero di componenti che si sono guastati

Life test experiment		
	Failure terminated	Time terminated
Senza rimpiazzo		
Con rimpiazzo		

L'ultimo caso affrontato è quello dei life test experiment con rimpiazzo time-terminated



Questi esperimenti terminano dopo un tempo prefissato t_d e in questo intervallo di tempo si sono guastati un certo numero m di componenti

- Anche in questo caso la stima del MTTF è pari all'area che rappresenta la vita totale di tutti i componenti, diviso il numero di componenti che si sono guastati



- Componenti hardware
- Componenti software

Il MTTR, al contrario del MTTF, non può essere “misurato” empiricamente e mediante degli esperimenti controllati, ma può essere stimato in base all’esperienza e al “buon senso”.

- Questa stima richiede di distinguere tra componenti hardware e componenti software



Come stimare l'MTTR (hardware)

17

Dove si trova l'hardware	Come viene gestito	MTTR stimato
Onsite	Un operatore è fisicamente presente 24 ore al giorno, 7 giorni alla settimana (24x7)	30 minuti
Onsite	Un operatore è reperibile telefonicamente 24 ore al giorno, 7 alla settimana (24x7)	2 ore
Onsite	Un operatore è disponibile negli orari lavorativi (8-18), 7 giorni alla settimana	14 ore
Onsite	Un operatore è disponibile negli orari lavorativi (8-18), da Lunedì a Venerdì	3 giorni
Offsite	Il componente nuovo viene inviato mediante corriere espresso	1 settimana
Offsite	Un operatore deve fisicamente portare il pezzo nuovo	2 settimane

Impianti Informatici

POLITECNICO DI MILANO

La stima del MTTR di componenti hardware deve tener conto degli aspetti logistici ed umani legati all'attività di "riparazione". In generale vige la regola che MTTR brevi richiedano grossi costi. Vediamo perché

- Innanzitutto bisogna stabilire dove si trova il componente, ossia bisogna stabilire se l'hardware che si è guastato si trova onsite o offsite. Con il termine onsite si indica che l'hardware guasto si trova presso la sede principale dell'azienda, quella dove si trovano anche i tecnici addetti alla gestione operativa del sistema. Con il termine offsite si indica che il componente guasto si trova in una sede "periferica" e comunque in una sede dove normalmente non sono fisicamente presenti i tecnici addetti alla gestione operativa del sistema
- Poi bisogna valutare come viene gestito l'hardware. Per i sistemi molto importanti si può avere un sistemista presente 24 ore al giorno, 7 giorni su 7 e i pezzi di ricambio per le componenti guaste sono già presenti e disponibili presso la sede dove è avvenuto il guasto (queste componenti di ricambio vengono chiamati spare)
- Alternativamente ci deve essere una persona responsabile che sia sempre raggiungibile telefonicamente, 24 ore al giorno, 7 giorni su 7. In questo caso il MTTR deve prevedere anche il tempo necessario al sistemista per raggiungere la sede
- Nel caso in cui un sistemista sia reperibile solo nelle ore lavorative (ad esempio dalle 8 alle 18) tutti i giorni, compreso il weekend, il MTTR deve tener conto della possibilità che un sistema si guasti appena è finito l'orario di lavoro (ad esempio, alle 19) e si deve aspettare fino alla mattina successiva
- Se poi un sistemista è reperibile solo nei giorni lavorativi (ossia, da lunedì a venerdì) la stima del MTTR deve comprendere prudenzialmente un intero weekend
- Nel caso i pezzi di ricambio non siano fisicamente presenti, può essere necessario far giungere il ricambio via corriere espresso
- Abbiamo infine il caso in cui il ricambio deve essere fisicamente reperito da persone dell'azienda



Meccanismo di detection	Meccanismo di reboot	MTTR stimato
Watchdog	Il processo viene riavviato automaticamente dal sistema operativo	30 secondi
Watchdog	Il sistema esegue un reboot automatico da disco e riavvia tutti i processi	3 minuti
Nessun meccanismo	Reboot manuale da parte di un operatore	Come MTTR hardware

Nel caso di componenti software, i guasti sono spesso dovuti a bug applicativi che possono richiedere tempi lunghi per essere individuati e risolti. Per fortuna molto spesso gli errori causati da questi bug possono essere temporaneamente risolti riavviando il modulo software che ha causato l'errore. Quindi il MTTR per un modulo software può essere definito come il tempo necessario per riavviare l'applicativo dopo che si è individuato il guasto.

- Bisogna innanzitutto valutare se il sistema è dotato di meccanismi automatici in grado di individuare i moduli software malfunzionanti e di eseguire in modo automatico le operazioni di riavvio. Questi sistemi sono chiamati watchdog (ossia cani da guardia)
- In questo caso, bisogna distinguere due situazioni alternative. Nella prima situazione, in seguito all'errore è sufficiente riavviare il processo "guasto"
- Nella seconda situazione, in seguito all'errore è necessario eseguire un reboot dell'intero sistema operativo
- Infine abbiamo il caso in cui il riavvio del processo o il reboot dell'intero sistema operativo deve essere fatto manualmente da un sistemista

molte failure software vengono eliminate riavviando l'applicazione o l'intero sistema

questo non corregge il motivo che ha generato la failure