CAPITOLO 1

Introduzione

1 Considerazioni preliminari

L'affidabilità è definita come la probabilità che il *sistema funzioni correttamente per un dato intervallo di tempo, in un dato ambiente e per un determinato scopo.* In altri termini, l'affidabilità misura quanto gli utenti si fidino del sistema. Questo può significare varie cose in base al sistema, all'ambiente ed allo scopo. È anche vero che utenti diversi possono percepire una diversa affidabilità del sistema.
Nello studio dell'affidabilità di sistemi, giocano un ruolo rilevante termini quali *malfunzionamento, difetto, errore.*
Per malfunzionamento si intende, generalmente, un comportamento del sistema che si discosta dal comportamento atteso (specifiche funzionali, prestazioni, ...).
Un fallimento corrisponde ad un comportamento run-time inaspettato (ed errato) osservato da un utente del sistema. Un fault è una caratteristica del software che causa il fallimento. I fault non necessariamente causano fallimenti ma solo quando la componente errata (guasta) del sistema viene utilizzata (vedere Figura **??**). In generale, per individuare i malfunzionamenti si predispone una fase di verifica. Questi malfunzionamenti costituiscono dei difetti del sistema o delle anomalie del codice. Il debugging serve ad identificare tali anomalie all'interno di un codice. L'errore è la causa dell'anomalia; si può trattare di un errore banale, di un errore concettuale o di un errore di progetto. Un cattivo comportamento del software può dipendere, quindi, da errori presenti nel codice, dall'ambiente esecutivo o dal profilo operativo. Ovviamente l'eliminazione degli errori non può avvenire se non si evidenziano e ciò può essere fatto sollecitando il programma con opportuni stati di ingresso. La rimozione degli errori, poi dipende essenzialmente dall'efficienza con cui gli errori vengono rilevati e rimossi.
L'affidabilità migliora quando si rimuovono i fault che compaiono nelle parti del sistema usate

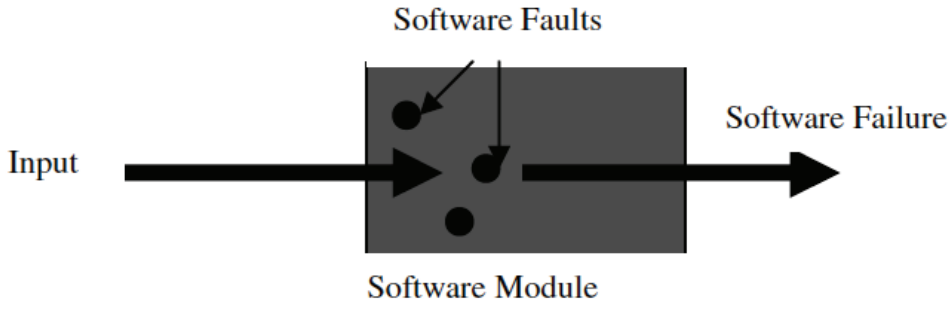

Figure 1: Relazione tra fault e fallimento del software.

più frequentemente. La rimozione di una percentuale pari all'$x\%$ di tutti i fault dal software non necessariamente comporta un miglioramento pari all'$x\%$ dell'affidabilità complessiva. Può accadere che la rimozione del 60% dei difetti migliori, ad esempio, l'affidabilità solo del 3%, così che diventa importante rimuovere i difetti che causano le conseguenze più serie.

Man mano che aumenta l'affidabilità, l'efficienza tende a diminuire. Per rendere un sistema più affidabile spesso è necessario inserire codice ridondante che effettui controlli a fissati tempi di esecuzione, comportando rallentamenti. È pur vero che spesso l'affidabilità è più importante dell'efficienza anche alla luce del fatto che i computer sono sempre più veloci ed economici. Macchine più veloci aumentano le aspettative degli utenti in termini di affidabilità. I sistemi inaffidabili non vengono usati sia perché possono essere difficili da migliorare sia perché i costi connessi a perdite di dati sono molto alti.

È opportuno osservare che l'affidabilità riferita all'hardware si discosta dall'affidabilità del software in alcuni punti essenziali. Infatti, partiamo dalla causa di malfunzionamento: per quanto riguarda l'hardware le principali cause di malfunzionamento sono sicuramente l'usura, la mancanza di manutenzione, raramente il progetto; diversamente, per il software la principale causa di malfunzionamento è il progetto, sicuramente non intervengono né l'usura, né la mancanza di manutenzione a determinare errori software. Nel caso di alcuni fallimenti software, il sistema può continuare a funzionare più o meno correttamente. Un'altra differenza è che le componenti hardware guaste possono essere sostituite con altre componenti identiche Queste osservazioni permettono di stabilire che l'affidabilità dell'hardware varia durante l'uso mentre l'affidabilità del software varia durante lo sviluppo del progetto. La prima varia in modo più o meno definito e controllabile, la seconda in modo più casuale.

Essendo l'affidabilità una funzione del tempo, è necessario stabilire quali sono le unità di tempo di interesse. A tale proposito, con riferimento alla Figura 2, possiamo facilmente immaginare che nel contesto hardware siamo interessati alle prime due scale temporali, invece per quanto riguarda l'affidabilità del software sostanzialmente interessa il tempo di CPU.

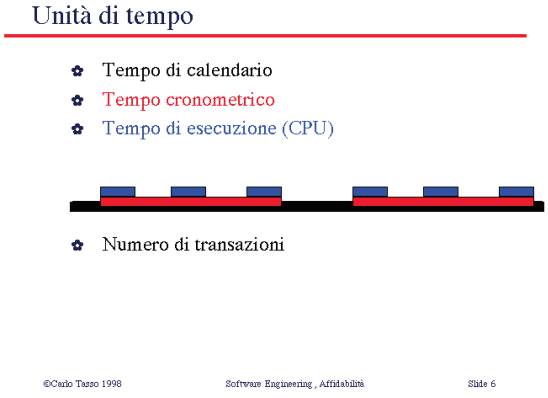

Figure 2: Scale temporali.

Nello studio dell'affidabilità si è interessati alle seguenti grandezze:

- istante di rilevamento del malfunzionamento
- intervallo di tempo tra due malfunzionamenti
- numero totale di malfunzionamenti
- numero di malfunzionamenti rilevati in un intervallo di tempo specificato.

Queste grandezze sono definite da variabili aleatorie sia per quanto riguarda il software che per quanto concerne l'hardware. Infatti, non si può localizzare l'errore, le condizioni di esecuzione sono non predicibili ed inoltre la relazione tra localizzazione degli errori nel codice e stati nell'esecuzione è molto complessa. Per quanto riguarda l'hardware, possiamo immaginare che i componenti del sistema si guastino per effetto di cause aleatorie comportando che le misure di affidabilità risultino tutte variabili aleatorie. L'utilizzo delle misure di affidabilità sono necessarie

- per valutare quantitativamente le metodologie di sviluppo software,
- per stabilire lo stato di avanzamento della fase di verifica di un progetto software,
- per migliorare le prestazioni operative dei programmi e controllare l'impatto dell'aggiunta di nuove parti di codice al pacchetto base,
- per valutare in modo quantitativo un parametro di qualità del software.

Queste considerazioni possono trasferirsi in maniera quasi diretta anche all'affidabilità nel contesto hardware.

Un andamento tipico della distribuzione dei malfunzionamenti è mostrato in Figura 3.

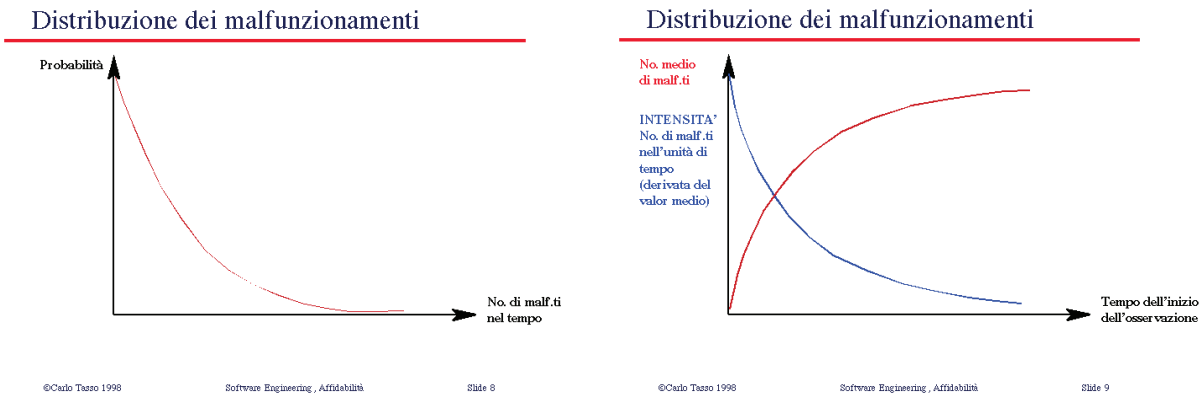

Figure 3: Distribuzione del numero di malfunzionamenti a sinistra, numero medio di malfunzionamento e intensità dei malfunzionamento a destra.

2 Sistemi e qualità

Le reti, gli impianti e i sistemi informatici, anche quelli che non vediamo, sono alla base della società moderna in quanto determinano la qualità della vita sociale. Infatti, oltre a controllare altri impianti più tradizionali (nucleari, elettrici, telefonici, idrici, ...), gli impianti e i sistemi informatici sono alla base dei sistemi bancari, dei sistemi di produzione, di distribuzione, di trasporto, di traffico aereo. Anche la medicina e la sanità sono controllati da impianti e sistemi informatici a partire dal governo degli ospedali, a quello dell'emergenza, al governo dei complessi macchinari di terapia medica. Perfino nei moderni edifici gli impianti e i sistemi giocano un ruolo fondamentale.
Sebbene nel quotidiano si abbia spesso la percezione di avere a che fare con un impianto informatico è pur vero che non sempre è chiaro che cosa può comportare un cattivo funzionamento dell'impianto stesso. Quando l'impianto con cui abbiamo a che fare ha dimensioni trascurabili, come può essere un PC, si può sopperire ad un comportamento non soddisfacente cambiando il sistema, scegliendo ad esempio un PC più veloce. La sensazione di un problema più complesso sorge quando si ha a che fare con un impianto di dimensioni *dipartimentali* (una scuola, un'università, un ente, un'azienda) a cui si accede attraverso un terminale.
Il comportamento anomalo di impianti e sistemi informatici è stato spesso alla base di incidenti nucleari, di black-out di sistemi telefonici e di sistemi di distribuzione di energia elettrica, di disservizi di sistemi di prenotazione e di controllo aerei e ferroviario, di errori nella gestione di attrezzature mediche che hanno portato pazienti alla sovraesposizione a terapie radianti, allo scambio di nomi e dei relativi dati, alla produzione di errati risultati di analisi di laboratorio...
Pertanto, è evidente quanto sia importante tener conto della qualità degli impianti di reti e di sistemi informatici sia in fase di progetto che di governo. È anche vero che con lo sviluppo delle attività industriali e con il crescere della complessità degli impianti, i problemi di affidabilità e di sicurezza del funzionamento dei sistemi e dei loro componenti sono diventati oggetto di studi sistematici.

Senza introdurre la differenza tra impianto, sistema informatico e rete, possiamo dire che un impianto o sistema è un insieme complesso di componenti hardware e software che deve essere progettato avendo in mente la qualità, ossia un indice $\mathbf{Q}$ multi-attributo definito tramite un vettore $\mathbf{Q} = (f_1, f_2, \ldots, f_n)$ le cui componenti f_i sono dette attributi. Ad esempio, un indice di qualità a sei attributi è il vettore $\mathbf{Q} = (f_1, f_2, \ldots, f_6)$ in cui

$f_1 =$ prestazione (performance) $\quad f_2 =$ usabilità (usability) $\quad f_3 =$ flessibilità (flexibility)
$f_4 =$ ampliabilità (scalability) $\quad f_5 =$ adeguatezza (adequacy) $\quad f_6 =$ evolubilità (*evolubility*)

il cui complesso determina la qualità dell'impianto. È necessario tener conto di questi attributi sia in fase di progetto e di sviluppo che in fase di uso e di governo di impianti già esistenti.
Il fattore $f_1 =$ prestazione (performance) è uno dei più articolati in quanto è definito attraverso un insieme di sotto-attributi, che per brevità chiamiamo ancora attributi, che determinano l'efficienza, la sicurezza e l'economia di un impianto. La Tabella 1 definisce la prestazione attraverso una

gerarchia di tre livelli in cui gli attributi del primo livello sono l'efficienza (effectiveness) e la predicibilità (dependability). L'efficienza è, a sua volta, definita in termini di 6 attributi e quattro attributi definiscono la predicibilità. La quarta colonna mostra le unità di misura dei vari attributi.

Fattore di qualità	Attributo di primo livello	Attributo di secondo livello	Metriche
Prestazione (Performability)	Efficienza (Effectiveness)	Tempo di attesa	Unità di tempo
		Tempo di risposta	Unità di tempo
		Lunghezza della coda	Numero di elementi
		Spazio	Unità di spazio
		Throughput	Num. elementi/tempo
		Utilizzazione	% (timeper.occup)
	Predicibilità (Dependability)	Disponibilità	% (time.perf)
		Affidabilità	Prob(time.perf)
		Safety	Prob(no.accid)
		Security	Prob(no.intru)

Table 1: Attributi di "Prestazione".

In Tabella 1 è stata usata la seguente notazione:

Numero di elementi	numero di elementi (programmi, comandi, richieste) che aspettano in coda
Num. elementi/tempo	numero di elementi serviti per unità di tempo
%(timeper.occup)	percentuale di tempo, su un fissato intervallo (timeper), in cui resta occupato un impianto o una sua componente
%(timeper.perf)	percentuale di tempo, su un fissato intervallo (timeper), in cui un impianto o una sua componente mantiene la sua prestazione
Prob(time.perf)	probabilità che un impianto o una sua componente mantenga la sua prestazione (perf) ad un dato istante di tempo (time)
Prob(no.accid)	probabilità che non si verifichino eventi catastrofici mentre l'impianto sta funzionando
Prob(no.intru)	probabilità che non si verifichino accessi indesiderati mentre l'impianto sta funzionando come richiesto

I due attributi della Prestazione possono essere studiati separatamente o in forma combinata, in questo secondo caso l'indice combinato si dice Performability. A volte, una buona efficienza può compromettere la predicibilità dell'impianto. Gli studi di performability hanno lo scopo di identificare il miglior bilanciamento (trade-off) tra efficienza e predicibilità. Quindi, si può ottenere un'alta prestazione a scapito di una predicibilità bassa, o viceversa.

Allo scopo di assicurare un giusto bilanciamento tra i due attributi il fattore f_1 di $\mathbf{Q}$ si scrive a sua volta in forma vettoriale $f_1 = (f_{1_1}, f_{1_2})$ dove la componente f_{1_1} rappresenta l'efficienza e f_{1_2} è la predicibilità. Assicurare un bilanciamento tra i due attributi significa richiedere che il modulo di f_1, definito come $|f_1| = \sqrt{|f_{1_1}|^2 + |f_{1_2}|^2}$, e il suo argomento, indicato con $\varphi = arctg(|f_{1_1}|/|f_{1_2}|)$, siano "soddisfacenti". Ciò equivale a richiedere che f_1 sia sufficientemente ampio (modulo) ma anche soddisfacentemente orientato (argomento), questo si ottiene richiedendo che i moduli di f_{1_1} (efficienza) e di f_{1_2} (predicibilità) siano a loro volta tali da superare due relative soglie di accettabilità.
Un ragionamento analogo si applica per valutare la bontà di ciascuna delle componenti, ad esempio di f_{1_2}, in quanto la predicibilità è a sua volta esprimibile con un vettore a più componenti (disponibilità, affidabilità, safety, security).
Visto che esiste una certa peculiarità della progettazione software rispetto alla progettazione di altri componenti (elettronici, meccanici), è opportuno specificare che cosa si intende quando si parla di affidabilità del software. Quando si progetta del software è opportuno tener conto di vari aspetti come ad esempio:

- Regole di progettazione per limitare l'introduzione di elementi non affidabili
- Tecniche per scovare e rimuovere difetti
- Tecniche di base per sviluppare software robusto in grado di sopportare eventuali malfunzionamenti dei suoi componenti
- Analisi delle interfacce hardware/software. In altri termini, il software si deve far carico dei malfunzionamenti del sistema, ma un malfunzionamento del software si può a sua volta propagare nel sistema.

In teoria dell'affidabilità tradizionalmente si assume che un progetto sia fatto senza errori o perlomeno che questi siano identificati e rimossi prima della messa in esercizio. Quindi gli unici guasti sono quelli casuali o di usura. Per quanto riguarda il software, ovviamente questo non si usura, né si guasta, però non esiste un approccio sistematico che garantisca l'assenza di errori nella fase di progetto. Inoltre, nei sistemi hardware si utilizzano moduli collaudati il cui funzionamento è stato verificato in passato, nei sistemi software che sono in genere esemplari unici, sebbene oggi si cominci a seguire la strada del riuso del software e/o di piattaforme standard per applicazioni di controllo processi, è necessario escogitare sempre nuove soluzioni. Una strada percorribile è il test, ma un test esaustivo è praticamente impossibile visto che da un punto di vista matematico un applicativo software è un sistema discreto con un altissimo numero di stati. Il test verifica la "compliance" (conformità) alle specifiche, ma cosa accade se le specifiche sono errate? E come testare i sistemi safety critical (sicurezza critica)? La fedeltà dei simulatori è tutta da dimostrare.

L'affidabilità, sebbene abbia origini relativamente recenti, è già stata oggetto di numerosi studi che ne hanno esaminato molteplici aspetti. Noi ci proponiamo di esaminare alcune teorie di base che consentono di impostare in maniera corretta alcuni problemi tipici dell'affidabilità.

Possiamo dividere il contenuto del corso in tre parti.
Nella prima parte, di natura introduttiva, dopo alcuni cenni storici si effettua uno studio delle funzioni e dei parametri utilizzati nello studio dell'affidabilità. Nella seconda parte vengono presentati i principali risultati che possono essere utilizzati per un approccio matematico della disciplina. Si esaminano, inoltre, alcuni risultati della teoria del rinnovo focalizzando l'attenzione sul processo dei rinnovi e su alcune politiche di manutenzione. In questo contesto, alla luce dei risultati teorici illustrati, vengono esaminati alcuni aspetti atti a migliorare l'affidabilità di un sistema. Nella terza parte ci si concentra sull'affidabilità del software, sottolinendo quali sono le analogie e le differenze tra affidabilità dell'hardware e del software e analizzando alcuni modelli utilizzati in letteratura per valutare l'affidabilità del software.

3 Cenni storici

La nascita ufficiale dell'affidabilità viene fatta risalire all'anno 1952 quando ad un piccolo simposio tenuto a San Diego in California, Robert Lusser, allora alla R & D Division, ne forniva la prima definizione. Nel ventennio precedente (anni 1930 – 1950) erano comunque già stati affrontati con metodologie matematiche problemi inquadrabili nell'area dell'affidabilità quali ad esempio:

- Manutenzione di macchine: studiati da Khintchine (1932) e successivamente da C. Palm (1947);
- Prove di vita e di fatica dei materiali, soprattutto ad opera di W. Weibull che nel 1939 propose una distribuzione (detta proprio di Weibull) per descrivere la durata di vita di un materiale;
- Sostituzione dei pezzi di ricambio come applicazione della teoria dei rinnovi, da parte di Lotka nel 1939 e successivamente di Campbell (1941) e Feller (1941, 1949).

Comunque, i primi interessi verso tali metodologie si svilupparono durante il secondo conflitto mondiale; successivamente, durante la Guerra Fredda queste metodologie subirono un forte impulso legato all'apporto di nuove tecnologie nel campo militare, aeronautico, spaziale. Lo sviluppo di tali studi si tradusse nell'introduzione di normative Military Standard su tali argomenti intorno agli anni '50 in seguito alle esperienze sviluppate nell'ultimo conflitto mondiale. Infatti, il malfunzionamento di sistemi militari, che diventavano sempre più complessi, produceva effetti negativi dal punto di vista sia operativo che economico. Un'indagine condotta negli US dalle Forze Armate condusse alla conclusione che l'inaffidabilità dei sistemi elettronici rendeva meno efficiente l'apparato militare e, al contempo, ne aumentava i costi di gestione.
Successivamente, questo patrimonio culturale e metodologico si trasferì dal campo militare al campo civile prima investendo l'aeronautica civile e successivamente l'impiantistica di produzione. In particolare, negli anni '60, a causa di esigenze di carattere economico, quale ad esempio la minimizzazione del costo globale di un servizio, gli studi sull'affidabilità invasero anche molti settori civili (delle comunicazioni, dei controlli industriali).

Sulla spinta dei successi ottenuti negli USA, negli anni '70 queste metodologie divennero patrimonio della ricerca applicata anche in Europa. Infatti, a partire dagli anni '70, con lo sviluppo dell'elettronica e la diffusione di apparecchiature di una certa complessità, l'affidabilità acquistò un significato più ampio coinvolgendo anche la qualità della vita in quanto, come già detto, l'affidabilità delle apparecchiature condiziona un numero sempre crescente di attività umane contribuendo ad aumentare il benessere e la sicurezza. Al giorno d'oggi molte attività produttive non potrebbero aver luogo senza la presenza fondamentale dell'informatica e dell'elettronica e col passare del tempo queste discipline diventano sempre più importanti nella vita quotidiana. Il computer oggi non è usato solo per la sua eccezionale capacità di calcolo, infatti esistono vari settori che sono governati da computer. Eventuali problemi tecnici ovviamente possono produrre danni più o meno importanti a seconda dei settori in cui si verificano. Sicuramente i settori più a rischio sono quelli in cui eventuali guasti provocherebbero perdite di vite umane (quello medico, quello militare e quello aeronautico). Esempi di tali errori si sono già avuti in un passato non proprio remoto:

- Durante la guerra dei sei giorni (1967 Israele contro Egitto, Siria e Giordania) un incrociatore statunitense fu bombardato per errore dall'esercito israeliano.
- Nel novembre 1979 il World Wide Military Monitoring americano segnalò erroneamente il lancio di un missile sovietico contro una metropoli degli Stati Uniti.

Episodi di questo tipo hanno evidenziato la sempre crescente necessità di investire su aspetti di affidabilità di sistemi che invece molto spesso è vista come un optional.
Allo stato attuale l'affidabilità deve ritenersi un obiettivo del sistema e un vincolo del progetto, nel senso che deve essere prevista all'atto della definizione del progetto; infatti introdurla in corso d'opera o successivamente diventa oneroso o addirittura impossibile.

4 L'attributo Affidabilità

La qualità di un sistema (elettronico) ha un'importanza crescente per il successo di un prodotto. Tra i parametri che influenzano la qualità di un prodotto è particolarmente rilevante l'affidabilità. L'affidabilità di un sistema può essere compromessa dall'insorgere di "malfunzionamenti", ossia dall'insorgere di differenze tra il comportamento reale del sistema e quello previsto o desiderato. I malfunzionamenti sono provocati da guasti originati in un qualsiasi momento precedente al manifestarsi del malfunzionamento.

All'interno di un'applicazione si possono distinguere le seguenti componenti:

- il prodotto che nel caso di sistemi elettronici è composto da componenti hardware o da componenti software;
- l'utente che è costituito da tutte le entità che interagiscono funzionalmente con il prodotto, si può trattare di una persona o di un altro prodotto;

- l'ambiente che a volte è definito non funzionale, questo interferisce con il prodotto senza, però, agire sui suoi ingressi.

Esempio 1 Consideriamo il sistema ABS di un'automobile. In questo caso il prodotto è il sistema elettronico ABS, l'utente corrisponde al conducente e al sistema idraulico di frenata, l'ambiente è invece tutto il resto che influisce sul sistema ABS con parametri quali la temperatura, l'umidità, le interferenze elettromagnetiche, il tipo di strada, ...

Esempio 2 Consideriamo un distributore di bevande. In questo caso il prodotto è il controllore. L'utente si presenta in varie forme: l'apparato elettromeccanico che gestisce le monete, le bevande, i bicchieri,..., il cliente che paga per avere una bevanda, il manutentore che fornisce bicchieri, zucchero,... e recupera le monete. L'ambiente, invece, fornisce acqua, elettricità, ...

Il prodotto deve svolgere una missione caratterizzata da una funzione e una durata (o tempo di vita operativo). Ogni prodotto ha un ciclo di vita composto da quattro fasi:

- La fase di **specifica** che permette di passare dalle richieste del committente (requirements) alle specifiche del prodotto;
- La fase di **progetto** che trasforma le specifiche nella descrizione di un sistema che le implementa;
- La fase di **produzione** che trasforma il progetto in un prodotto;
- La fase **operativa** in cui il prodotto interagisce con l'utente all'interno dell'ambiente al fine di eseguire la propria missione.

Le prime tre fasi costituiscono il **processo di sviluppo**.

La predicibilità o dependability (affidabilità di macchine) è la disciplina che studia i guasti e sviluppa tecniche per realizzare sistemi affidabili. Con il termine dependability si intende anche la proprietà che caratterizza un sistema affidabile. La dependability di un prodotto può essere valutata in modo rigoroso attraverso alcuni attributi:

- Reliability (Affidabilità)
- Maintainability (Manutenibilità)
- Testability (Collaudabilittà)
- Safety (Sicurezza)
- Availability (Disponibilità)

L'affidabilità è definita come la probabilità (condizionata) $R(t)$ che il sistema funzioni correttamente al termine dell'intervallo (t_0, t_1) sapendo che funziona correttamente all'istante t_0.
La manutenibilità è la probabilità $M(t)$ che un sistema non funzionante possa essere rimesso in condizioni di funzionare correttamente in un tempo inferiore a t.

La collaudabilità è la facilità con cui le diverse caratteristiche del sistema possono essere collaudate.
La sicurezza è la probabilità che il sistema funzioni correttamente o sia in grado di interrompere il proprio funzionamento senza creare gravi danni.
La disponibilità è la probabilità che un sistema funzioni correttamente e sia in grado di svolgere le proprie funzioni in un generico istante di tempo t.
A differenza dell'affidabilità, che si riferisce ad un intervallo di tempo, la disponibilità si riferisce ad un fissato istante di tempo. Sistemi caratterizzati da malfunzionamenti relativamente frequenti, ma rapidamente riparabili, possono avere una bassa affidabilità ma un'alta disponibilità.
L'approccio più semplice, consistente nel progettare il sistema e successivamente nel renderlo affidabile, è costoso ed inefficace; è quindi preferibile tener conto dell'affidabilità sin dai primi passi del progetto.

Le tecniche, tra loro complementari, per il progetto di sistemi affidabili sono normalmente classificate in quattro categorie:

- Fault-prevention (prevenzione d'errore)
- Fault-removal (rimozione d'errore)
- Fault-tolerance (tolleranza d'errore)
- Fault-forecasting (previsione d'errore).

Le applicazioni per le quali esistono vincoli di affidabilità ricadono normalmente in quattro categorie:

- **Applicazioni di lunga durata:** Il caso più comune è quello dei sistemi aerei e spaziali senza equipaggio (ad esempio i satelliti). Normalmente si richiede che abbiano una probabilità superiore al 95% di essere ancora funzionanti dopo 10 anni di funzionamento. Possono avere dei periodi di non funzionamento e spesso possono essere riconfigurati.
- **Applicazioni con criticità di elaborazione:** Corrispondono alle applicazioni in cui un errore di elaborazione può causare perdita di vite umane o danni economici ingenti. Un tipico requisito per queste applicazioni consiste nel garantire il corretto funzionamento su un periodo di tre ore con una probabilità superiore a 0.9999999 (0.9^7). Esempi di tali applicazioni sono sistemi di controllo di aerei, sistemi di controllo di impianti nucleari, sistemi di controllo del traffico ferroviario.
- **Applicazioni a manutenzione ritardata:** Si utilizzano quando le operazioni di manutenzione non possono essere eseguite o perché hanno dei costi elevati, o perché possono essere eseguite solo con periodicità prefissata. La tolleranza ai guasti serve allora a mantenere operativo il sistema sino all'arrivo del manutentore. Un esempio di tale applicazione è dato dai sistemi di controllo su impianti remoti (dighe).
- **Applicazioni ad elevata disponibilità:** Devono garantire il loro funzionamento con una probabilità molto elevata. Esempi tipici sono applicazioni bancarie, centrali telefoniche.

A seconda della tipologia dell'applicazione, è conveniente utilizzare tecniche di progetto diverse, che permettono di raggiungere il miglior compromesso tra costi e risultati.

5 Metodologie RAMS

I problemi di affidabilità e di sicurezza di funzionamento dei sistemi e dei loro componenti sono diventati oggetto di studio sistematico a causa dello sviluppo delle attività industriali e della crescente complessità degli impianti. Le implicazioni tecno-economiche connesse allo sviluppo dell'aeronautica civile e militare, dei veicoli spaziali, degli elaboratori elettronici, degli impianti nucleari, hanno reso evidente come gli strumenti ridondanti e i fattori di sicurezza non erano in grado di assicurare tali parametri di affidabilità per evidenti problemi di ingombro, peso e costi.
Lo studio dell'affidabilità comprende l'insieme di teorie e metodi matematici che si traducono in procedure organizzative per risolvere problemi di previsioni, stime, ottimizzazione delle probabilità di sopravvivenza, durata media della vita, percentuale di corretto funzionamento del sistema. La valutazione dell'affidabilità è condotta su basi statistiche. Questo ha condotto allo sviluppo di Metodologie RAMS:

- **R**: Reliability (Affidabilità)
- **A**: Availability (Disponibilità)
- **M**: Maintainability (Manutenibilità)
- **S**: Safety (Sicurezza)

Queste metodologie permettono di valutare a priori i parametri di affidabilità dei sistemi individuando in fase progettuale gli eventuali punti deboli e consentendo di individuare le opportune modifiche. È necessario introdurre uno strumento che, da un lato, garantisca l'affidabilità e la disponibilità di sistemi, accanto ad esigenze di sicurezza e, dall'altro, consenta lo studio di tali parametri, accompagnati dalla manutenibilità del sistema, portando ad aumentare la probabilità di successo della missione.
Esistono tre approcci per valutare l'affidabilità di un sistema:

- utilizzare le informazioni che provengono per un lungo periodo di tempo da molti sistemi uguali che funzionano sotto le stesse condizioni;
- utilizzare le informazioni che provengono dal funzionamento per un breve periodo di tempo di pochi sistemi. I dati possono fornire una stima del comportamento avente un certo grado di confidenza, ovvero una certa probabilità di risultare vera;
- utilizzare la conoscenza, se esiste, dell'affidabilità dei componenti per fare previsioni sull'affidabilità dell'intero sistema.

Tali strumenti sono di natura probabilistica. In particolare, la prima fase è realizzata con lo studio di leggi che correlano le prestazioni dei componenti e dei sistemi alle sollecitazioni loro imposte.

La seconda parte viene effettuata attraverso lo studio delle leggi che correlano le prestazioni dei materiali ai processi di produzione.
La qualità è definita tramite l'insieme delle caratteristiche di un bene che conferiscono ad esso la capacità di soddisfare esigenze (del cliente) espresse o implicite; la qualità nei sistemi viene espressa da caratteristiche verificabili con tecniche deterministiche e tecniche probabilistiche.

Le caratteristiche deterministiche sono rappresentate da prestazioni di base o di specifica e la loro misurazione avviene di norma durante il collaudo che verifica del loro grado di conformità.

Le caratteristiche probabilistiche sono rappresentate da prestazioni del componente/sistema attese nel tempo, la loro misurazione avviene tramite l'utilizzo delle metodologie **RAMS** di natura probabilistica.

Le metodologie RAMS nell'impiantistica vengono utilizzate per garantire la tenuta del sistema/prodotto nell'arco del tempo e per prevenire i rischi associati ad esso, rischi che coinvolgono sia fattori umani che fattori ambientali.

L'analisi RAMS consente un aumento della Qualità, della Sicurezza e della Produzione. In particolare, denotando con Q^* la qualità teorica o di target e con R il parametro di affidabilità del sistema, si ha che la qualità effettiva è data dal prodotto

$$Q^*R = Q^* - Q^*(1 - R).$$

Definizione L'affidabilità di un componente è la probabilità che esso funzioni senza guasti per un certo periodo di tempo t con riferimento a precisate condizioni ambientali.

Per definire l'affidabilità è necessario disporre di un criterio univoco per stabilire se un componente è funzionante o meno, un'esatta definizione delle condizioni ambientali e d'impiego, individuazione dell'intervallo di tempo di ampiezza t. Una volta fissati i primi due punti, l'affidabilità diventa una funzione che dipende solo dal tempo; la forma di questa funzione dipende dalla legge probabilistica con cui le condizioni di cattivo funzionamento o di cedimento possono verificarsi nel tempo.

Più in generale, si può dire che la teoria dell'affidabilità è la scienza di prevedere, analizzare, prevenire e mitigare i guasti nel tempo. Si tratta di una scienza che ha principi e basi teoriche ben definite, tutte connesse in qualche modo allo studio e alla conoscenza dei guasti. È legata alla matematica ed in particolare alla statistica, alla fisica, alla chimica, alla meccanica e all'elettronica; e, visto che l'elemento umano è quasi sempre parte dei sistemi, spesso si ha a che fare con la psicologia e la psichiatria.

La teoria dell'affidabilità tenta di dare una risposta alla domanda: quanto durerà il sistema? Più precisamente cerca di dare una risposta alle seguenti questioni:

- Qual è la disponibilità del sistema? Più dura un sistema tra un guasto e l'altro e minore è il tempo di riparazione così che maggiore sarà la disponibilità del sistema.
- Come si possono prevenire i guasti? Possiamo prevenire potenziali guasti intervenendo sulla progettazione, sui materiali e sulla manutenzione.

- Qual è il Life Cicle Cost di un sistema? LCC include il costo iniziale, i costi di riparazione, i costi di gestione del magazzino ricambi, del trasporto, i costi-opportunità, i costi di fine servizio.
- Quali sono i rischi maggiori? I rischi maggiori sono quelli che hanno le peggiori conseguenze e che avvengono più frequentemente.

L'affidabilità coinvolge quasi tutti gli aspetti legati al possesso di un bene:

- **Costi di gestione:** L'affidabilità coinvolge sia il costo di acquisto che quello di manutenzione di un bene: l'impiego di materiali più affidabili spesso comporta un incremento del prezzo, altre volte accade che l'adozione di tecnologie più affidabili implica un parallelo decremento dei costi.
- **Soddisfazione del cliente:** Se un componente non corrisponde alle aspettative di affidabilità del cliente, può accadere spesso che ci sia una disaffezione rispetto agli altri prodotti della stessa azienda, con chiari danni di immagine.
- **Gestione delle risorse:** Meno un componente si guasta e minore è la quantità di risorse che deve essere dedicata alla gestione delle situazioni di inefficienza causate dai guasti.
- **Capacità di vendere i prodotti o i servizi:** La maggiore affidabilità dei componenti permette di aumentare la soddisfazione dei clienti e di guadagnare nuove fette di mercato.
- **Sicurezza:** L'affidabilità è strettamente connessa ad alcuni aspetti della sicurezza
- **Qualità:** Essendo la capacità di essere attinenti alle specifiche di un prodotto, una scarsa qualità può significare una bassa affidabilità.
- **Manutenibilità:** È questa la probabilità di un sistema di essere riportato in uno stato in cui possa svolgere la funzione richiesta. Ciò avviene quando la manutenzione è realizzata nelle condizioni determinate e con procedure e mezzi prescritti. In altri termini, esprime la capacità di un sistema di essere facilmente ripristinato nel caso si renda necessario eseguire un intervento di manutenzione.

6 Qualche considerazione sui guasti

Ciascun componente di un sistema ha una precisa funzione da assolvere. La specifica di un componente contiene varie informazioni tra queste la descrizione della funzione da assolvere, le interazioni con altri componenti, le condizioni ambientali in cui si trova ad operare. Il comportamento di un componente influenza il sistema a vari livelli: può assolvere correttamente la sua funzione, non assolverla, assolverla solo parzialmente, durante la sua attività può disturbare un'altra funzione o un altro componente.

Il periodo di regolare funzionamento di un dispositivo si conclude quando un qualsiasi fenomeno fisico-chimico (guasto) che si produce in una o più delle sue parti determina una variazione delle

prestazioni nominali tali da ritenere inaccettabile il comportamento del dispositivo stesso. Così il dispositivo passa dallo stato di **funzionamento** a quello di **avaria**.

Cause di guasto	**Descrizione**
Sollecitazioni, urto, fatica	Dipende dalla distribuzione temporale e spaziale delle condizioni di carico e della risposta dei materiali. Le caratteristiche strutturali del componente assumono un ruolo importante e devono essere valutate includendo anche possibili errori progettuali, realizzativi, difetti del materiale,...
Temperatura	È una variabile operativa che influisce in funzione delle caratteristiche del materiale (inerzia termica) nonché della distribuzione spaziale e temporale delle sorgenti di calore.
Usura	Si tratta di uno stato di degradazione fisica del componente. Si manifesta in seguito all'invecchiamento che accompagna la normale attività (attrito fra materiali, esposizione ad agenti dannosi, ...).
Corrosione	È un fenomeno che dipende dalle caratteristiche dell'ambiente in cui il componente opera. Queste condizioni possono portare il materiale a processi di degradazione fisica e chimica capace di rendere il componente non più idoneo.

I **guasti infantili** o prematuri si manifestano nella prima fase di esercizio del componente. Le cause sono spesso riconducibili ad una carenza strutturale, progettuale, a difetti di istallazione oppure a cause intercorse nella fase intermedia tra produzione e cliente. I prodotti soggetti a questo tipo di guasto in genere sono sfuggiti al controllo statistico oppure si sono rotti dopo la fase di test ad esempio nella fase intermedia tra produzione e cliente. In termini di affidabilità, un impianto sottoposto alla manifestazione di guasti infantili migliora il proprio stato col trascorrere del tempo.
I **guasti accidentali** o casuali si verificano in condizioni di esercizio non nominali che mettono a dura prova i componenti, producendo delle inevitabili alterazioni con conseguente perdita delle capacità operative. Questo tipo di guasto si manifesta durante la vita utile dell'impianto e corrisponde a situazioni imprevedibili. La probabilità di manifestarsi di un guasto è indipendente dal periodo di esercizio accumulato e rimane costante per un certo periodo di tempo.
I **guasti per usura** si manifestano come alterazioni del componente per invecchiamento strutturale e materiale. L'inizio del periodo di usura è individuato da un aumento della frequenza dei guasti fino al raggiungimento del valore massimo, per poi decrescere per effetto della scomparsa della popolazione. I guasti per usura si manifestano intorno all'età media di funzionamento; l'unico modo per evitare questo tipo di guasto è quello di operare un ricambio preventivo.

Per rappresentare un fenomeno statistico è necessario raccogliere i dati e rappresentarli sotto forma di grafici e/o tabelle. Per uno studio sull'affidabilità i dati rilevanti sono connessi alla durata del componente o, meglio, del prodotto. Per avere una schematizzazione dei dati raccolti spesso si fa uso di un diagramma detto istogramma che ha lo scopo si aggregare i dati raccolti in intervalli.

Esempio 3 In Tabella 2 sono mostrati i dati relativi allo stipendio iniziale di 42 neolaureati Dai

dati si evince che lo stipendio minimo annuale è stato di 27000 euro ed è stato corrisposto a 4 neolaureati, mentre lo stipendio massimo, di 40000 euro, è stato corrisposto ad una sola persona. La cifra più frequente è stata di 32000 euro.

Stpendio iniziale	Frequenza
27	4
28	1
29	3
30	5
31	8
32	10
34	5
36	2
37	3
40	1

Table 2: Stipendi annuali iniziali in migliaia di euro.

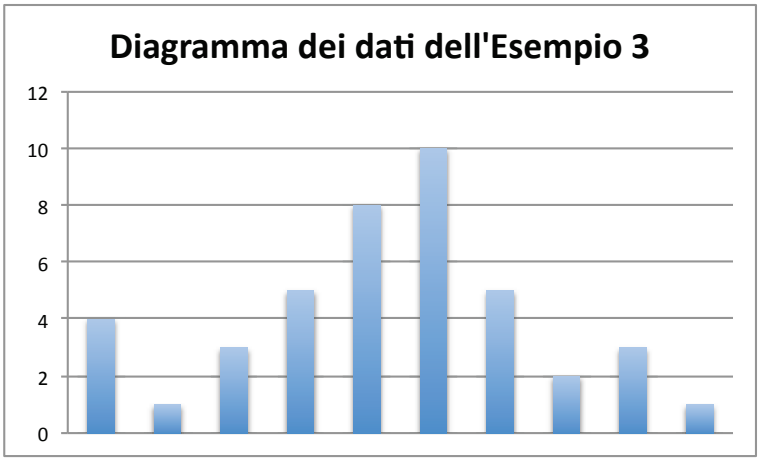

Figure 4: Con riferimento all'Esempio 3.

In Figura 5 sono riportati alcuni istogrammi rappresentanti le frequenze dei tempi di guasto di certi componenti; è evidente che l'istogramma fornisce una rappresentazione discreta, d'altra parte non potrebbe essere diversamente. Per ottenere una funzione matematica dell'affidabilità e per estrapolare i dati nel tempo è necessario approssimare l'istogramma con una curva continua (cf. Figura 6) che prende il nome di densità di probabilità dei tempi di guasto.

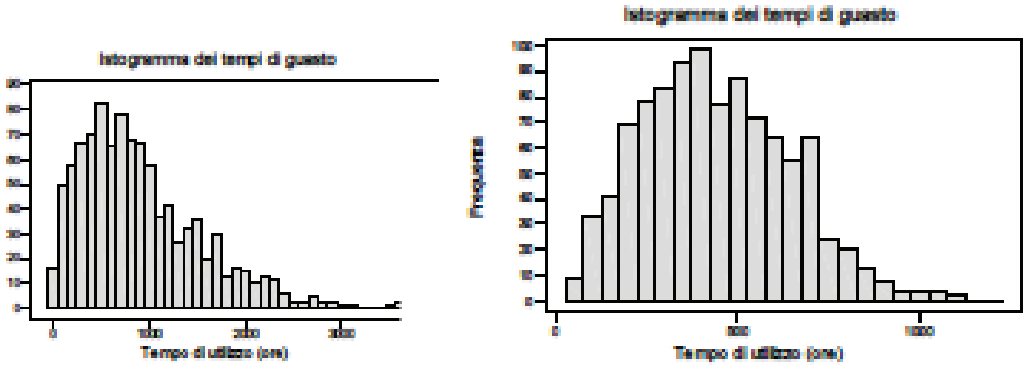

Figure 5: Esempi di istogrammi per le frequenze dei tempi di guasto.

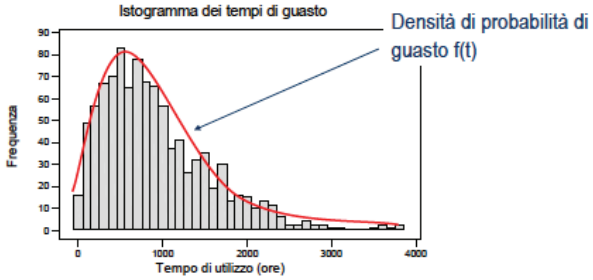

Figure 6: Esempio di densità di probabilità dei tempi di guasto.

Le tabelle e gli istogrammi consentono di realizzare una "fotografia" del fenomeno o della popolazione che si sta considerando. Molto spesso è, però necessario avere delle informazione di tipo globale dei dati rilevati; a questo scopo vengono considerati i così detti "indici statistici". Questi indici si distinguono in indici di posizione (media, moda, mediana), di dispersione (varianza, deviazione standard, range, quartili) e di forma (skewness e curtosi).

Premesso ciò, consideriamo un intervallo di tempo di ampiezza T fissata e supponiamo che agli istanti aleatori $g_k < T$ si verifichino dei guasti al sistema in osservazione. Dopo un certo intervallo di tempo, che può essere di durata variabile, necessario perché il guasto sia riparato, il sistema riprende a funzionare correttamente. Indicando con r_k l'istante in cui il sistema riprende a funzionare dopo il k-esimo guasto, si ha una situazione simile a quella mostrata in Figura 7.

Figure 7: Processo guasto - manutenzione - ripristino.

Poiché $T = \sum(t_{rk} + t_{gk})$, segue che la disponibilità del dispositivo risulta essere:

$$A = \frac{T - \sum t_{rk}}{T} = \frac{T - \sum t_{rk}}{\sum(t_{rk} + t_{gk})} = \frac{\sum(t_{rk} + t_{gk}) - \sum t_{rk}}{\sum(t_{rk} + t_{gk})} = \frac{\sum t_{gk}}{\sum(t_{rk} + t_{gk})}$$

Se si denota con F_i la frequenza con cui si presentano intervalli di ampiezza t_i, risulta che

$$A = \frac{\sum F_{gk} t_{gk}}{\sum (F_{rk} t_{rk} + F_{gk} t_{gk})} = \frac{t_g^*}{t_g^* + t_r^*},$$

dove $t_g^* = \sum F_{gk} t_{gk}$ e $t_r^* = \sum F_{rk} t_{rk}$.
Supponendo che, dopo la riparazione, l'apparecchiatura torni nelle condizioni iniziali, possiamo descrivere il processo tramite un istogramma delle frequenze (cf. Figura 8a). Tale istogramma può essere approssimato con una curva continua, la densità di frequenza (o di probabilità) del guasto o densità di guasto (cf. Figura 8b). Consideriamo come variabile il tempo di guasto di un elemento, ossia il tempo intercorrente tra l'istante iniziale e l'istante in cui si è verificato il guasto. La densità di guasto, moltiplicata per dt, approssima la probabilità con cui si verifica un guasto nell'intervallo di tempo $(t, t + dt)$ (cf. Figura 9).

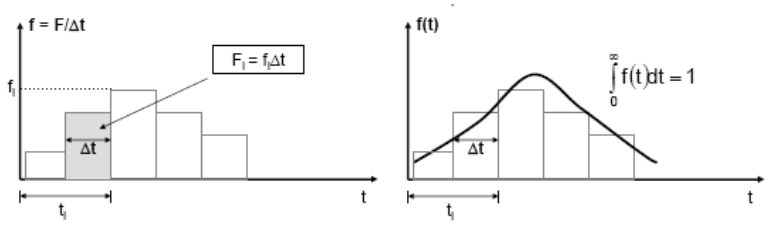

Figure 8: Istogramma delle frequenze (a sinistra), densità di guasto (a destra).

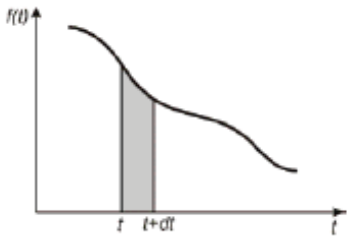

Figure 9: Relazione tra la densità di guasto e la probabilità di rottura di un elemento.

L'area sottesa alla curva $f(t)$ è unitaria; se si assume che l'intervallo di tempo sia infinitamente ampio; ciò può ritenersi abbastanza realistico visto che un elemento prima o poi è destinato a rompersi.
In natura molti fenomeni statistici si distribuiscono in accordo a densità di probabilità che hanno una forma "a campana". Esempi di distribuzioni di frequente utilizzate nella teoria dell'affidabilità sono la distribuzione normale, l'esponenziale e la distribuzione di Weibull (cf. Figura 10).

La distribuzione esponenziale è usata per descrivere l'affidabilità di un sistema durante la fase matura del dispositivo in cui i guasti si manifestano di norma per cause accidentali. Nella fase in cui il sistema è usurato si utilizza la distribuzione normale, la distribuzione lognormale si utilizza in situazioni in cui il sistema è usurato per "affaticamento". La distribuzione di Weibull, essendo particolarmente flessibile, è utilizzata nella fase di rodaggio, nella fase di vecchiaia del dispositivo

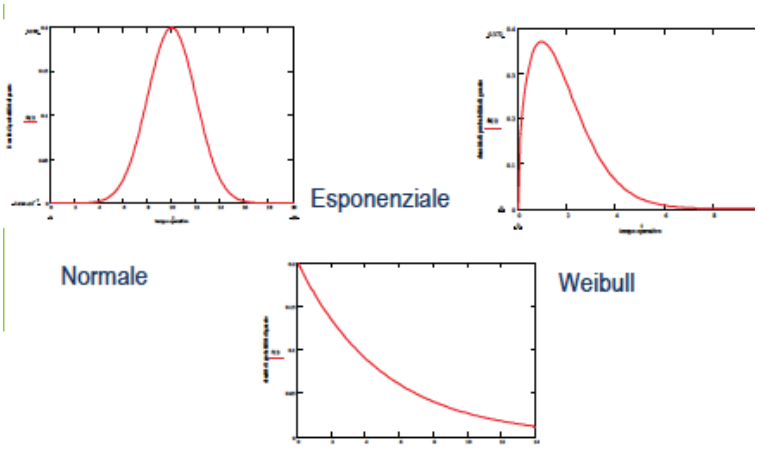

Figure 10: Alcune distribuzioni dei frequente utilizzo nella teoria dell'affidabilità.

e anche durante il periodo di vita utile in quanto, per alcune scelte dei parametri diventa una distribuzione esponenziale.