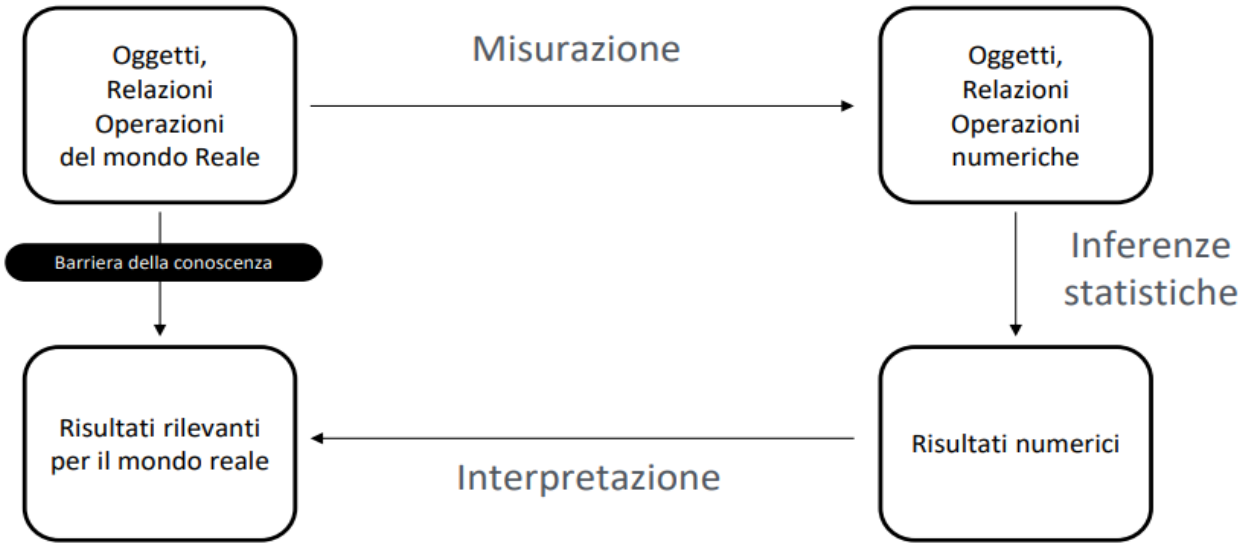
TEORIA DELLA MISURA

Perché è importante misurare?
Tra le varie cose, misurare serve a:
1) **Caratterizzare**, ovvero estrarre informazioni ben precise su qualche caratteristica di un prodotto.
2) **Comparare**, ovvero capire se lo sviluppo di un prodotto A sta andando meglio, peggio o come lo sviluppo di un altro prodotto B con caratteristiche analoghe.
3) **Controllare** o **monitorare** un prodotto.
4) **Valutare**, ovvero dare valore a qualche caratteristica di un prodotto, come la sua difettosità sulla base dei dati raccolti durante il suo sviluppo.
5) **Predire**, ovvero anticipare il valore che assumerà qualche caratteristica di un prodotto, come ad esempio il suo tempo di consegna.

La misurazione, in breve, ci permette di ottenere dei risultati rilevanti per il mondo reale (come una considerazione, una legge fisica o il risultato di un esperiemento) a partire dall'osservazione degli oggetti del mondo reale:



Notiamo che non è possibile avere dei risultati rilevanti per il mondo reale senza ricorrere a un processo di astrazione caratterizzato da operazioni numeriche e risultati numerici e, quindi, senza misurazione. Questo "vincolo" è noto come barriera della conoscenza.

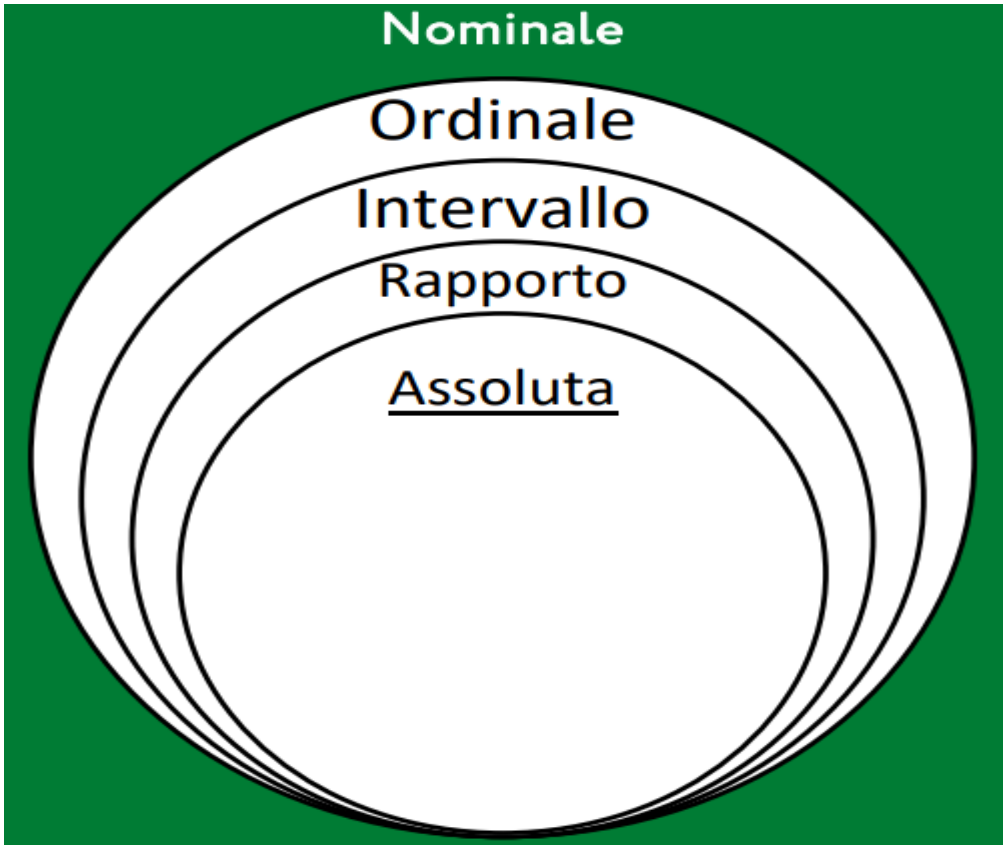
Definizione
Un **sistema relazionale** consiste in una tupla definita da:
- Un insieme di oggetti.
- Relazioni tra tali oggetti ("è uguale a", "è più di", "è meno di").
- Operazioni binarie tra tali oggetti (somma, sottrazione).

Definizione
Sia **A** un sistema relazionale di oggetti fisici, sia **B** un sistema relazionale di oggetti formali e sia **m** una misura da A a B (vedere più avanti per la definizione di misura). Allora la tupla (A, B, m) è una **scala** se:
- Relazioni in A equivalgono a relazioni in B.
- Ogni operazione in A ha una corrispondente operazione in B.

Tipi di scale

Tipo	Uso	Relazioni	Operazioni	Esempio
Scala nominale	Dare nomi alle cose.	Uguaglianza	-	Numeri sulle t-shirt dei giocatori da calcio (dove non c'è un numero che ha più valore di un altro).
Scala ordinale	Dare nomi in un ordine specifico.	- Più di - Meno di	-	Podio olimpionico (dove la medaglia d'oro vale di più di quella d'argento ma è impossibile assegnare un valore numerico alle varie medaglie).
Scala intervallo	Assegnare numeri al fine di rendere significativo un intervallo.	Somiglianza, ottenibile tramite relazioni matematiche.	- Mediana - Media	Temperatura su scala Celsius, dove: Celsius*1,8 + 32 = Fahrenheit
Scala rapporto	Effettuare un rapporto tra due misure.	Somiglianza, ottenibile tramite relazioni matematiche.	- Mediana - Media	Lunghezza in metri di un oggetto, che è ottenuta dal rapporto della dimensione dell'oggetto stesso e la dimensione (di 1 metro) della barra di platino-iridio conservata a Sèvres.
Scala assoluta	Trattasi di una scala utilizzata quando si ha un unico modo per misurare oggetti.	Somiglianza, ottenibile dalla funzione identità.	- Mediana - Media	Conteggio (non esistono più modi per contare il numero di oggetti).

Tali scale sono caratterizzate da una relazione di inclusione tra loro:



Glossario

Termine	Significato
Entità	È un elemento dotato di realtà oggettiva. È indipendente e autocontenuta e ha dei caratteri propri. Inoltre è di un certo tipo, che può essere ad esempio un prodotto, un processo o una risorsa.
Entità misurabile	È una qualunque entità che può essere misurata. È caratterizzata da attributi misurabili.
Tipo di entità misurabile	Le entità misurabili, a loro volta, possono essere classificate a seconda del tipo. Per esempio, il processo è un tipo di entità misurabile.
Modello di entità	È un'astrazione di un'entità che viene modellata in relazione agli scopi che si hanno, al grado di conoscenza che si ha dei suoi caratteri e agli strumenti di modellazione.
Attributo	È una proprietà di un'entità che: - Concorre a determinare l'eventuale stato e gli eventuali comportamenti dell'entità. - Definisce una qualità di interesse dell'entità.
Attributo misurabile	È una proprietà di un'entità misurabile che, appunto, può essere misurata. Dimensione e produttività sono esempi di attributi misurabili.
Modello di attributo	È un'astrazione di un attributo che, come i modelli di entità, dipende dagli scopi che si hanno, dal grado di conoscenza che ne si ha e dagli strumenti di rappresentazione.
Misurazione	È il processo che si esercita su un'entità (in particolar modo su un suo attributo) con lo scopo di produrre un risultato di misurazione.
Risultato di una misurazione	È un valore associato a un attributo di un'entità a seguito di una misurazione. È tipicamente ma non necessariamente numerico: in particolare, appartiene ai valori ammessi della scala utilizzata.
Misura	È uno strumento (una funzione) che permette di associare attributi misurabili con i valori di una scala. Ad esempio, la misura "numero di requisiti" può essere utilizzata per associare un valore all'attributo misurabile "dimensione" che caratterizza il tipo di entità misurabile "progetto".
Metrica	È un termine utilizzato con diverse accezioni nell'ambito dell'ingegneria del software: - È una particolare grandezza da misurare (come una distanza o una superficie). - È l'insieme delle norme che regolano composizione e strutturazione delle misure. - È l'insieme delle misure di un settore o di un software nel suo complesso.

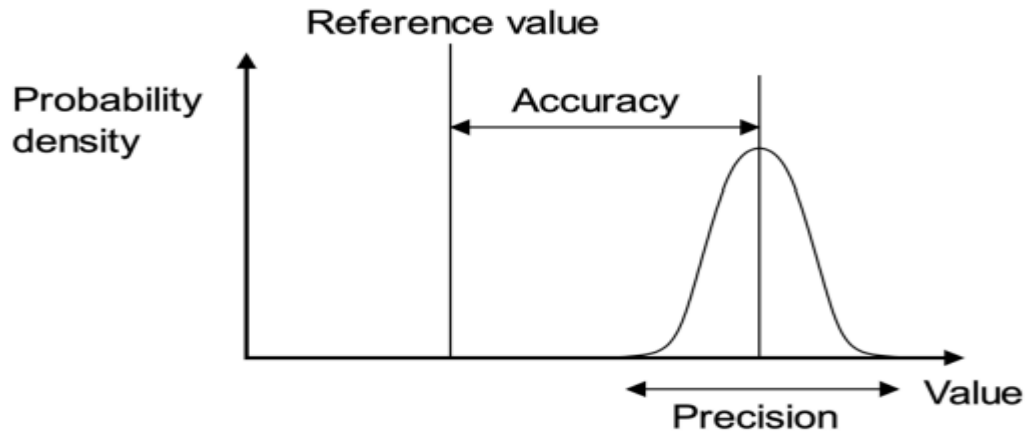
NB: Un attributo può essere:
- **Esterno** se è osservabile direttamente dall'utilizzatore dell'entità (come gli attributi public in Java).
- **Interno** se è osservabile esclusivamente nell'ambito dell'entità presa isolatamente, ma non esternamente (come gli attributi private in Java che, per essere acceduti, richiedono l'invocazione di un apposito metodo getter o setter).

D'altra parte, un attributo può anche essere:
- **Direttamente misurabile** (come la dimensione).
- **Indirettamente misurabile** (come la produttività) se può essere misurato solo mediante il coinvolgimento di altri attributi di base.

Caratteristiche della misurazione
- **Influenza**: i sistemi, fra cui le entità che si intendono misurare, sono generalmente modificati e influenzati dalle misurazioni.
- **Ripetibilità**: in analoghe condizioni, le misurazioni dovrebbero dare luogo al medesimo risultato. In altre parole, salvo errori sistematici e/o casuali, una determinata entità, a parità di contesto, stato e attributo misurato, deve essere caratterizzara sempre dalla medesima misura.

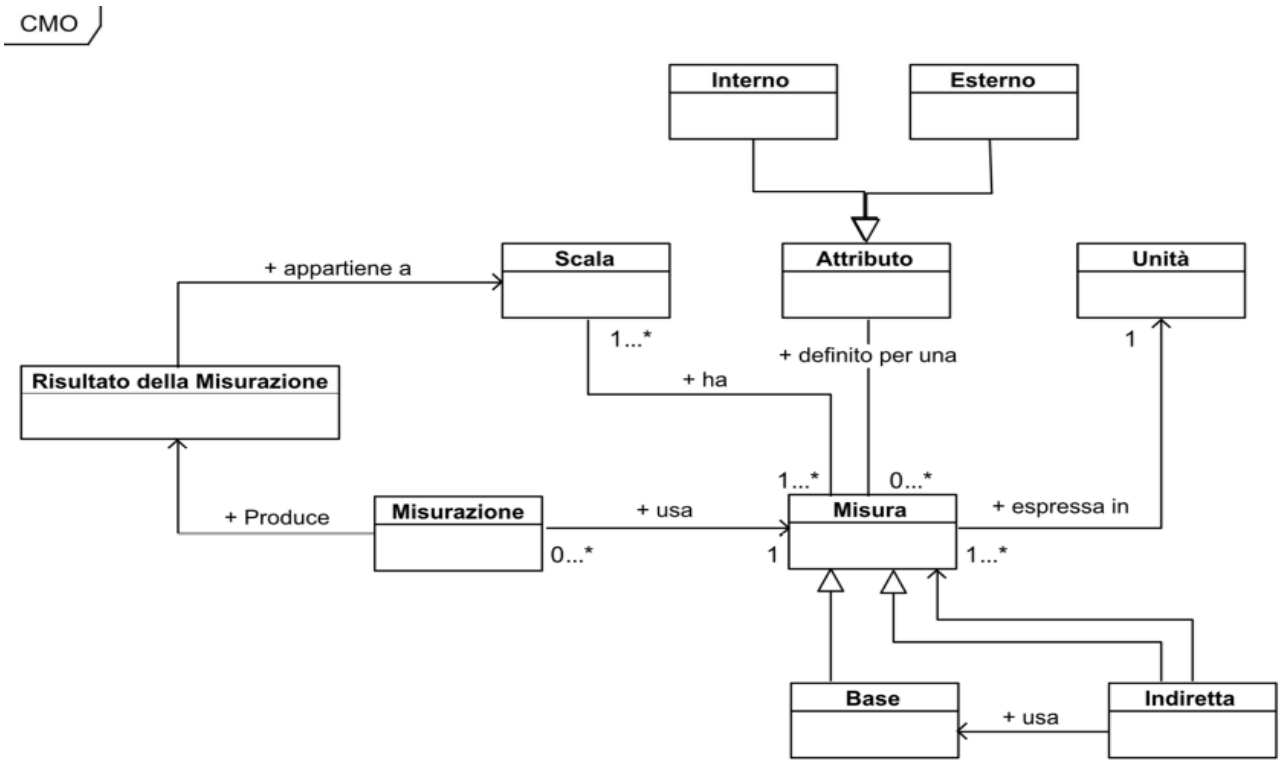
- **Errori**: gli errori di osservazione possono essere sistematici (che sono relativi alla differenza tra il valore reale della grandezza in esame e il valore assunto dal risultato della misurazione effettuata su di essa) oppure casuali (che possono essere dovuti a errori di lettura dello strumento di misurazione o di trascrizione del risultato della misurazione).

Un insieme di data point (= risultati di misurazione) derivanti da misurazioni ripetute della stessa quantità si definisce:
- **Accurato (ISO Trueness)** se la media del valore dei data point è vicina al vero valore della quantità misurata.
- **Preciso** se i data point si trovano "vicini" tra loro.



In realtà, l'accuratezza ha un duplice significato poiché ISO la definisce come l'unione tra le due definizioni appena elencate, ovvero come la prossimità dei risultati di misurazione al vero valore della quantità misurata.

Classic Measurement Ontology (CMO)
È un modello di rappresentazione formale che può essere espresso col seguente diagramma UML:



FUNCTIONAL & NON FUNCTIONAL SOFTWARE METRICS

Requisiti non funzionali (NFR)
Sono requisiti che definiscono come dovrebbe essere il sistema. Si suddividono in:
- Operativi
- Revisionali
- Di transizione

Noi ci concentreremo su quelli operativi, tra cui rientrano la disponibilità, la sicurezza e l'usabilità.

Disponibilità (availability)
È la capacità di un servizio di svolgere la propria funzionalità ogni volta che viene richiesto dall'utente. Si calcola con la seguente formula:

$$Availability\% = \frac{(Tempo\ di\ servizio\ concordato\ -\ Tempo\ di\ inattività)}{Tempo\ di\ servizio\ concordato}$$

Dove:
- **Tempo di servizio concordato** = tempo previsto in cui il servizio dovrebbe essere operativo.
- **Tempo di inattività** = quantità di tempo durante il tempo di servizio concordato in cui il servizio non è disponibile.

La disponibilità può anche essere espressa tramite la cosiddetta regola dei nove:

Availability %	Downtime per year	Downtime per month	Downtime per week
90% (one nine)	36.5 days	72 hours	16.8 hours
99% (two nines)	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.9% (three nines)	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% (four nines)	52.56 minutes	4.32 minutes	1.01 minutes
99.999% (five nines)	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% (six nines)	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% (seven nines)	3.15 seconds	0.259 seconds	0.0605 seconds

Sicurezza (security)
È buona norma utilizzare i **KPI** come tecnica per tenere traccia delle metriche di sicurezza informatica, nonostante si tratti ancora di una pratica non comune e in via di sviluppo.
I KPI (Key Performance Indicator) sono degli indicatori utilizzati per misurare i risultati conseguiti da un'organizzazione. Nell'ambito della sicurezza, i due KPI più importanti sono:
- **MTTD** (tempo medio di rilevamento): è la quantità di tempo mediamente necessaria per identificare un attacco ricevuto.
- **MTTR** (tempo medio di risposta): è la quantità di tempo mediamente necessaria per contenere o risolvere il danno causato dall'attacco ricevuto.

Nonostante la loro importanza, questi due fattori non sempre vengono considerati quanto necessario e, spesso, risultano essere un fattore critico: ad esempio, nel 2017, per le società statunitensi l'MTTD medio è stato di 52 giorni, mentre l'MTTR medio è stato di 208 giorni.

Consideriamo alcune altre metriche di sicurezza rilevanti:

Metrica	Descrizione
Numero di risorse vulnerabili nell'ambiente	È una metrica di sicurezza chiave per determinare i rischi che l'azienda corre e le patch che devono essere effettuate per ridurre tali rischi.
Numero di certificati TLS configurati in maniera errata	Il monitoraggio dei requisiti di sicurezza dei certificati impedisce che essi cadano nelle mani di malintenzionati che possono sfruttare l'identità digitale dell'azienda per rubare le informazioni dei dipendenti.
Volume di dati trasferiti usando la rete aziendale	Se i dipendenti effettuano tanti download (ad esempio di software, video, film e applicazioni) usando la rete aziendale, possono lasciare la porta aperta a malware.
Numero di dipendenti con livello di accesso "super utente"	Per ragioni di sicurezza, è opportuno che i dipendenti accedano solo a dati, risorse e sistemi necessari al proprio lavoro.
Numero di giorni per disattivare le credenziali di un ex dipendente	Idealmente, l'accesso al sistema degli ex dipendenti dell'azienda dovrebbe essere revocato immediatamente.
Numero di porte di comunicazione aperte durante un periodo di tempo	Tutte le porte comuni per i protocolli che consentono sessioni remote (come SSH, Telnet e FTP) devono essere monitorate per un certo periodo di tempo; inoltre, è inopportuno tenere aperte le porte non necessarie, poiché rappresentano solo un punto di ingresso in più per eventuali attacchi o malware.
Frequenza di revisione degli accessi di terze parti alla rete aziendale	Spesso viene concesso l'accesso a terze parti nella rete aziendale per completare un progetto. È importante assicurarsi che l'accesso venga annullato al termine del progetto stesso: in caso contrario, è possibile che la terza parte decida di tornare per estrarre dati o svolgere altre attività dannose; oppure, peggio ancora, se la terza parte viene violata, anche la nostra rete aziendale può essere esposta alla stessa minaccia.
Frequenza di accesso a sistemi aziendali critici da parte di terzi	Per ragioni di sicurezza, è opportuno monitorare i tentativi di accesso a server o applicazioni che non dovrebbero essere presi di mira da utenti non autorizzati.
Percentuale di partner commerciali con politiche di sicurezza informatica efficaci	Se l'azienda investe in sicurezza ma ha partner che non lo fanno, non gode in realtà di alcun servizio di sicurezza.

Una tipologia particolare di metriche di sicurezza prevede solo due valori possibili: **vero** e **falso**.
Tali metriche tipicamente appartengono a un vasto insieme di regole (una check-list) detto **benchmark**.
Il risultato del benchmark è normalmente espresso con una scala intervallo e rappresenta il valore della "vera metrica" con cui è possibile esprimere il giudizio complessivo sull'entità oggetto di misurazione.

Due esempi di enti che offrono metriche di benchmarking sono:
- **OWASP** (Open Web Application Security Project), che è una fondazione senza scopo di lucro che lavora per migliorare la sicurezza del software.
- **Dipartimento della Difesa degli Stati Uniti** (supportato dal DISA – Defense Information Systems Agency), che prevede uno standard di sicurezza rappresentato da delle check-list che prendono il nome di STIG (Security Technical Implementation Guide). Gli STIG contengono una guida tecnica per "bloccare" i sistemi informatici e i software che potrebbero altrimenti essere vulnerabili a un attacco.

Requisiti funzionali
Sono requisiti che definiscono che cosa dovrebbe fare il sistema. Sono più semplici rispetto a quelli non funzionali poiché:

- Sono meno astratti e meno ambigui, per cui normalmente non generano confusione.
- Sono più facili da misurare.
- Sono più facili da testare.
- A differenza dei requisiti non funzionali, possono essere implementati nel sistema in maniera incrementale (ovvero è possibile aggiungere sempre più funzionalità nel tempo, mentre non è possibile aggiungere servizi di sicurezza senza dover riprogettare e reimplementare tutto il sistema).

Le metriche orientate alle funzionalità (**functional software metrics**) si concentrano sulla quantità di funzionalità offerte dal software, basandosi sul calcolo del cosiddetto **punto funzione** (FP), che è appunto l'unità di misura che quantifica la funzionalità aziendale fornita dal prodotto (ma non include gli sforzi relativi ai requisiti non funzionali).

Glossario

Termine	Significato
Processo Elementare (EP)	È la più piccola unità di requisito funzionale che: - È significativo per l'utente. - Costituisce una transazione completa. - È autonomo e lascia l'attività dell'applicazione conteggiata in uno stato coerente.
Funzioni dati (data functions)	Sono costituite da risorse interne ed esterne che influiscono sul sistema, come i file logici interni (ILF) e i file di interfaccia esterna (EIF).
Funzioni di transazione (transactional functions)	Sono costituite dai processi di interscambio tra l'utente, le applicazioni esterne e l'applicazione da misurare. Esistono tre tipologie di funzioni di transazione: - Input esterni (EI). - Output esterni (EO). - Richieste esterne (EQ).
File logico interno (ILF)	È un gruppo identificabile dall'utente di dati logicamente correlati che risiedono interamente all'interno del boundary dell'applicazione. Il suo intento principale è conservare i dati attraverso uno o più processi elementari dell'applicazione stessa.
File di interfaccia esterna (EIF)	È un gruppo identificabile dall'utente di dati logicamente correlati che risiedono interamente al di fuori del boundary dell'applicazione (poiché mantenuti in un ILF da un'altra applicazione). Per ottenere i dati in un EIF, è necessario sviluppare un'interfaccia apposita.
Input esterno (EI)	È una funzione transazionale in cui i dati entrano nell'applicazione a partire dall'esterno (ad esempio, a partire da una schermata di immissione dati o da un'altra applicazione).
Output esterno (EO)	È una funzione transazionale in cui i dati escono dal sistema per essere inviati all'utente oppure ad altre applicazioni.
Richiesta esterna (EQ)	È una funzione transazionale con componenti di input e output che determinano il recupero dei dati. Di fatto, una richiesta può essere effettuata: - Da parte dell'utente verso il sistema. - Da parte di applicazioni esterne verso il sistema. - Da parte del sistema verso l'utente. - Da parte del sistema verso le applicazioni esterne.
Record Element Type (RET)	È il più grande sottogruppo di elementi identificabile dall'utente all'interno di un ILF o un EIF.
Data Element Type (DET)	È il sottogruppo di dati all'interno di un File Type Referenced. Sono univoci e identificabili dall'utente.
File Type Referenced (FTR)	È il più grande sottogruppo identificabile dall'utente all'interno dell'input esterno, output esterno o richiesta esterna a cui si fa riferimento.

Processo di conteggio dei FP

1) Determinare il tipo di conteggio.
2) Determinare il limite del conteggio.
3) Identificare ogni Processo Elementare richiesto dall'utente.
4) Determinare i Processi Elementari unici.
5) Misurare le data function.
6) Misurare le transactional function.
7) Calcolare la dimensione funzionale (conteggio dei punti funzione non aggiustato).
8) Determinare il fattore di aggiustamento del valore (VAF).
9) Calcolare il conteggio dei punti funzione aggiustato.

NB: I passaggi 8 e 9 di questo algoritmo sono facoltativi.