

Ingegneria del Software

Angelo Passarelli

October 23, 2023



Appunti basati sulle lezioni e dispense della professoressa Laura Semini ¹

¹<http://didawiki.cli.di.unipi.it/doku.php/informatica/is-a/start>

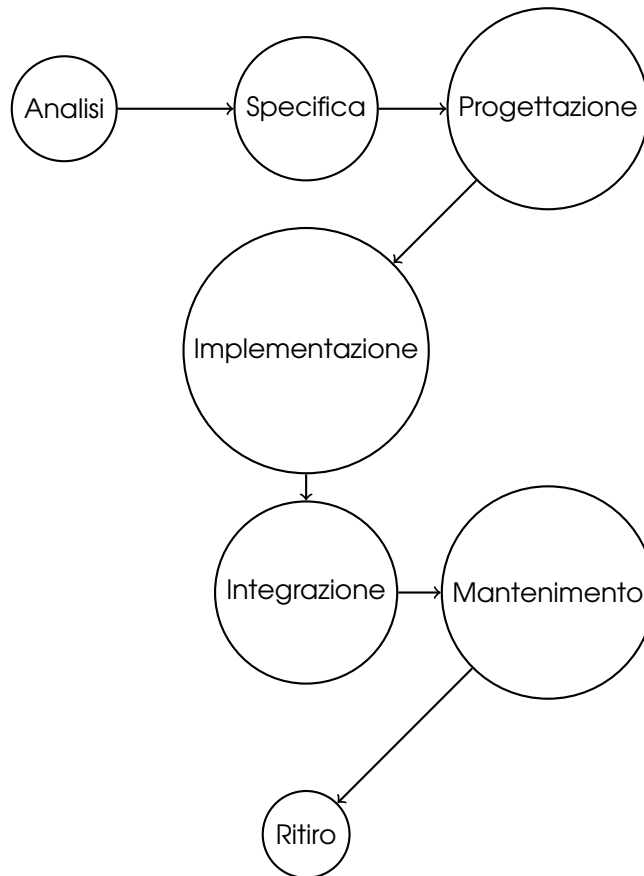
Contenuti

0	Introduzione	4
1	Modelli di Ciclo di Vita	5
1.1	Modelli Sequenziali	5
1.1.1	Build-and-Fix	5
1.1.2	Modello a Cascata	6
1.1.3	Modello a V	6
1.2	Modelli Iterativi	7
1.2.1	Rapid Prototyping	7
1.2.2	Modello Incrementale	7
1.2.3	Modello a Spirale	9
1.3	Unified Process	10
1.4	Processi Agili	10
1.4.1	Il Manifesto di Snowbird	11
1.4.2	eXtreme Programming	11
1.4.3	SCRUM	12
2	Analisi dei Requisiti	14
2.1	Studio di Fattibilità	14
2.2	Dominio	14
2.3	Requisiti	14
2.4	Documento dei Requisiti	15
2.5	Fasi dell'Analisi dei Requisiti	15
2.5.1	Acquisizione	15
2.5.2	Elaborazione	15
2.5.3	Convalida	16
2.5.4	Negoziiazione	17
2.5.5	Gestione	17
2.6	Casi d'uso	18
2.7	User Stories	18
3	Linguaggio UML e Casi d'Uso	19
3.1	UML	19
3.2	Diagramma dei Casi d'Uso	19
3.3	Narrativa dei Casi d'Uso	20
3.3.1	Inclusione	21
3.3.2	Estensione	22
3.4	Classi e Oggetti	23
3.4.1	Diagramma delle Classi	23
3.4.2	Relazioni	24
3.4.3	Aggregazione e Composizione	26
3.4.4	Generalizzazione	26
3.4.5	Classi Astratte	27
3.4.6	Interfacce	27

3.4.7	Dipendenze	27
3.4.8	Classi Associazione	27
3.4.9	Classi di Analisi	28
3.4.10	Diagramma degli Oggetti	29
3.5	Diagramma delle Attività	29
3.5.1	Segnali & Eventi	30
3.5.2	Sotto-Attività	31
3.5.3	Partizioni	31
3.6	Macchina a Stati	32
3.6.1	Eventi	32
3.6.2	Stato Composito Sequenziale	34
3.6.3	Stato Composito Parallelo	35
3.6.4	Sottomacchine	35
3.6.5	Pseudostati	36
4	Architetture Software	38
4.1	Vista Comportamentale	38
4.1.1	Stili Architettureali	40
4.2	Vista Strutturale	41
4.2.1	Vista Strutturale a Strati	41
4.2.2	Vista Strutturale di Generalizzazione	41
4.3	Vista Logistica	41

0 Introduzione

Fasi del progetto



Specificità del Software

1. **Fault tolerance**: capacità del software di essere tollerante ai guasti.
2. **Difetto latente**: difetto nascosto che si trova difficilmente in fase di testing; e anche nel caso comparisse è quasi impossibile da ritrovare.
3. **Robustezza**: capacità di funzionare anche con input non previsti e/o non testati.
4. Il software non presenta **costi materiali** e nemmeno **costi marginali**, ovvero il costo di un'unità del prodotto.

5. Infine il software non si consuma nel tempo, ma potrebbe diventare **obsoleto**.

La Manutenzione

Costi La fase di manutenzione è quella che richiede costi più alti. Per evitare uno spreco durante questa fase è necessario studiare bene l'analisi dei requisiti, in quanto un errore in questa fase si propagherà in modo esponenziale, in termini di costi, nelle fasi successive.

La manutenzione si divide in:

- **Manutenzione Correttiva**: rimuove gli errori, lasciando invariata la specifica.
- **Manutenzione Migliorativa**: consiste nel cambiare quella che è la specifica, e a sua volta può dividersi in:
 - **Perfettiva**: modifiche per migliorare e/o introdurre nuove funzionalità.
 - **Adattiva**: modifiche indotta da cambiamenti esterni, come leggi o modifiche all'hardware o al sistema operativo.

Stakeholders

- **Fornitore**: colui che sviluppa il software.
- **Committente**: chi lo richiede e paga.
- **Utente**: chi lo usa.

1 Modelli di Ciclo di Vita

Definizione (Processo Software). Con processo software si indica il percorso da seguire per sviluppare un prodotto o più nello specifico un software. Fanno parte del processo sia gli strumenti e le tecniche per lo sviluppo che i professionisti coinvolti.

1.1 Modelli Sequenziali

1.1.1 Build-and-Fix

Il prodotto è sviluppato senza alcuna fase di progettazione preliminare, lo sviluppatore scrive il software e poi lo modifica ogni volta che non soddisfa il committente.

Contro Diventa improponibile per progetti grandi e la manutenzione diventa difficile senza documentazione nè specifica.

1.1.2 Modello a Cascata

Questo modello è stato il primo a distinguere il processo software in più fasi, evidenziando l'importanza della progettazione e dell'analisi.

Viene chiamato anche modello *document driven* dato che ogni fase produce un documento, e per passare alla successiva occorre aver approvato il documento della fase precedente.

Contro Troppo pesante da seguire, inoltre non si può tornare indietro, e mancando l'interazione con il cliente, se non è soddisfatto, va tutto ripetuto dall'inizio.

1.1.3 Modello a V

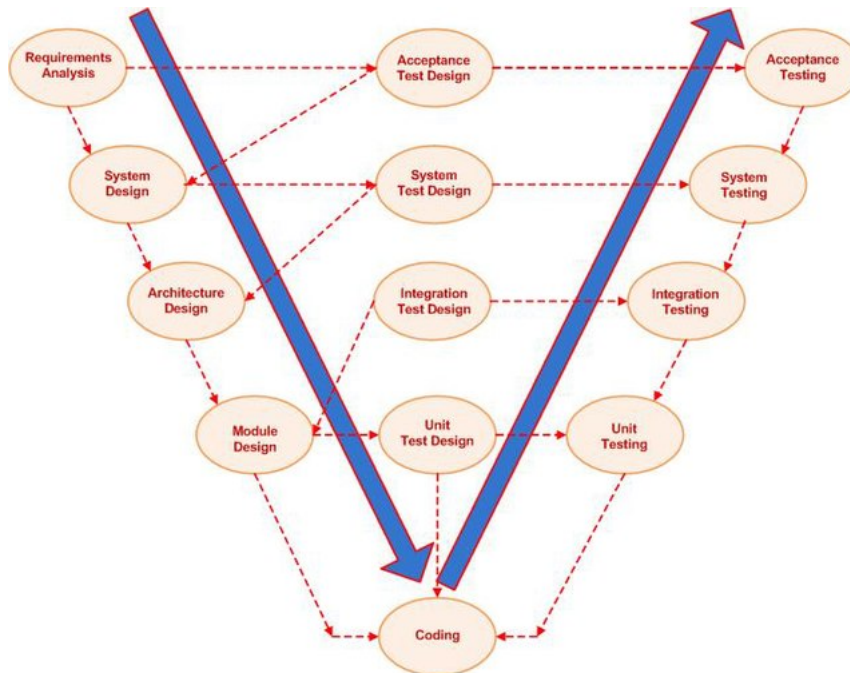


Figure 1: Le frecce blu rappresentano il *tempo*, mentre quelle tratteggiate le *dipendenze*

Questo modello evidenzia come sia possibile progettare i **test** durante le fasi di sviluppo (quelle a sinistra, prima della fase di *coding*). Mentre sulla destra sono presenti i test veri e propri che devono verificare e convalidare l'attività in corrispondenza sulla sinistra.

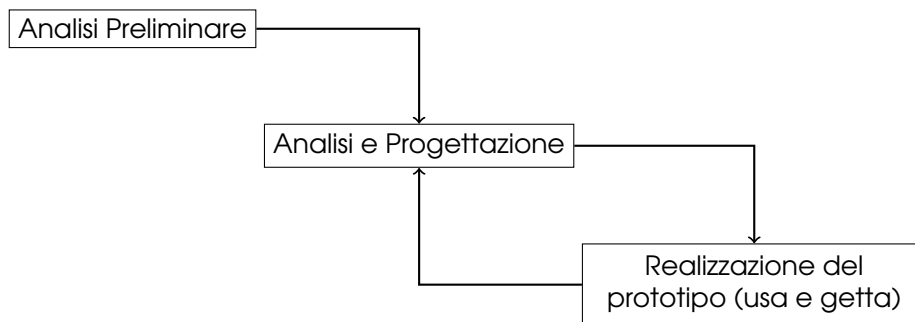
Standard SQA Questo modello è uno degli standard SQA (Software Quality Assurance), usato per descrivere le attività di test durante il processo di sviluppo.

1.2 Modelli Iterativi

1.2.1 Rapid Prototyping

L'obiettivo è quello di costruire rapidamente un prototipo del software per permettere al committente di sperimentarlo.

Questo modello diventa utile quando i requisiti non sono chiari, quindi ogni prototipo aiuterà il cliente a descriverli meglio.



1.2.2 Modello Incrementale

Il software viene costruito in modo iterativo, aggiungendo di volta in volta nuove funzionalità.

I requisiti e la progettazione vengono definiti inizialmente, per questo è possibile applicarlo solo in caso di requisiti stabili.

Contro Se non viene realizzata una buona progettazione, questo modello sfocia in un *Build-and-Fix*.

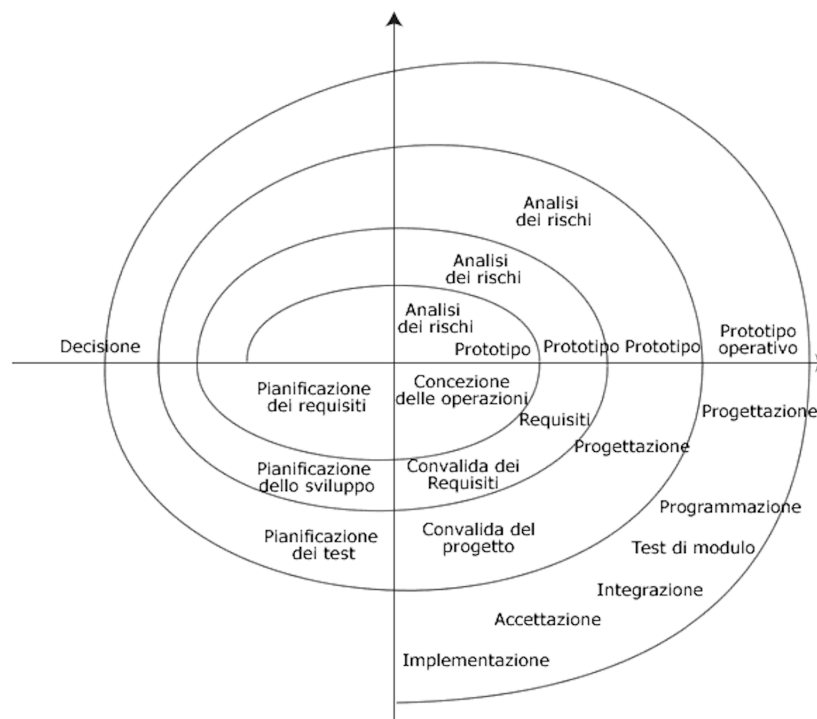


1.2.3 Modello a Spirale

In questo caso ogni iterazione è formata da 4 fasi che corrispondono ai quadranti del piano:

1. *Quadrante in alto a sinistra*: definizione degli obiettivi e dei vincoli.
2. *Quadrante in alto a destra*: analisi e risoluzione dei rischi.
3. *Quadrante in basso a destra*: sviluppo e verifica del prossimo livello.
4. *Quadrante in basso a sinistra*: pianificazione della fase successiva.

Questo modello viene anche chiamato *risk driven* in quanto è incentrato principalmente sull'analisi dei rischi. Inoltre si ispira profondamente al metodo iterativo *plan-do-check-act cycle*²



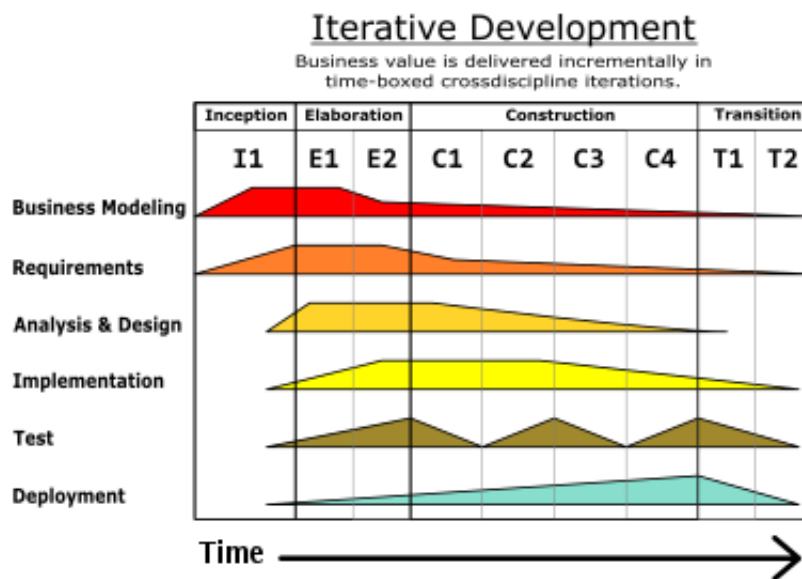
²https://it.wikipedia.org/wiki/Ciclo_di_Deming

1.3 Unified Process

In questo modello vengono distinte quattro fasi chiamate *Inception*, *Elaboration*, *Construction* e *Transition*. Ogni fase può presentare un numero variabile di iterazioni anche in base alla dimensione del progetto.

Questo modello viene definito *iterativo incrementale*, *incrementale* perchè alla fine di ogni iterazione si ottiene un rilascio del sistema con funzionalità in più o migliorate rispetto al rilascio precedente.

Inoltre viene data molta importanza all'architettura del sistema, infatti già dalle prime fasi ci si concentra soprattutto sull'architettura anche se a livello molto superficiale, lasciando i dettagli alle fasi successive. In questo modo è molto facile avere una visione generale del sistema che sarà facilmente modellabile sulla variazione dei requisiti. Per questo, piuttosto che dai requisiti, ci si fa guidare principalmente dai *casi d'uso* e dall'*analisi dei rischi*.



1.4 Processi Agili

Definizione (Metodo Agile). Con *metodo agile* si intende un metodo per lo sviluppo del software che si basa principalmente sul coinvolgimento del committente. Questa metodologia si riferisce ai principi del *Manifesto di Snowbird* del 2001.

I concetti chiave di questi processi sono:

- **Continuous Integration**: rendere il più automatico possibile la consegna e l'integrazione dei singoli moduli.
- **Continuous Delivery**: rilascio frequente e supportato delle nuove versioni del software.
- **DevOps**: *Development e Operations*, ovvero maggiore collaborazione tra sviluppatori e responsabili della manutenzione, della sicurezza e dell'infrastruttura dell'azienda.

1.4.1 Il Manifesto di Snowbird

Il *Manifesto di Snowbird* si fonda su quattro punti fondamentali:

1. **Comunicazione**: la comunicazione fra tutti gli attori del progetto è centrale, soprattutto le interazioni e la collaborazione con i clienti.
2. **Semplicità**: si mantiene il codice sorgente il più semplice possibile, ma comunque avanzato tecnicamente, in questo modo si riduce la documentazione al minimo indispensabile.
3. **Feedback**: sin dal primo giorno di sviluppo il codice viene testato, in modo da poter rilasciare versioni ad intervalli molto frequenti.
4. **Coraggio**: dare in uso il sistema il prima possibile ed implementare i cambiamenti richiesti man mano.

Di seguito sono riportati due modelli che si basano sui *processi agili*.

1.4.2 eXtreme Programming

Si basa su un insieme di consuetudini:

- *Pianificazione flessibile*: è basata su un insieme di scenari proposti dagli utenti e i programmatori vengono coinvolti direttamente.
- *Rilasci frequenti*: più o meno ogni 2-4 settimane, e alla fine si ricomincia con una nuova pianificazione.
- *Progetti semplici*: comprensibili a tutti.
- *Testing*: test basati sui singoli scenari e con supporto automatico.
- *Test Driven Development*: i casi di test vengono definiti prima della scrittura del codice.
- *Cliente sempre a disposizione*
- *Programmazione a coppie*: viene usato un solo terminale, una persona svolge il ruolo di **driver** che scrive il codice, mentre un'altra fa il **navigatore**, ovvero controlla il lavoro del *driver* attivamente.

- *No al lavoro straordinario*
- *Collettivizzazione del codice*: accesso libero e continua integrazione.
- *Code Refactoring*: modificare il codice senza cambiare il suo comportamento e commentarlo il più possibile.
- *Daily Stand Up Meeting*

1.4.3 SCRUM

Definizione (SCRUM). Con **SCRUM** si intende un processo *iterativo ed incrementale*, dove alla fine di ogni iterazione vengono fornite un insieme di funzionalità potenzialmente rilasciabili.

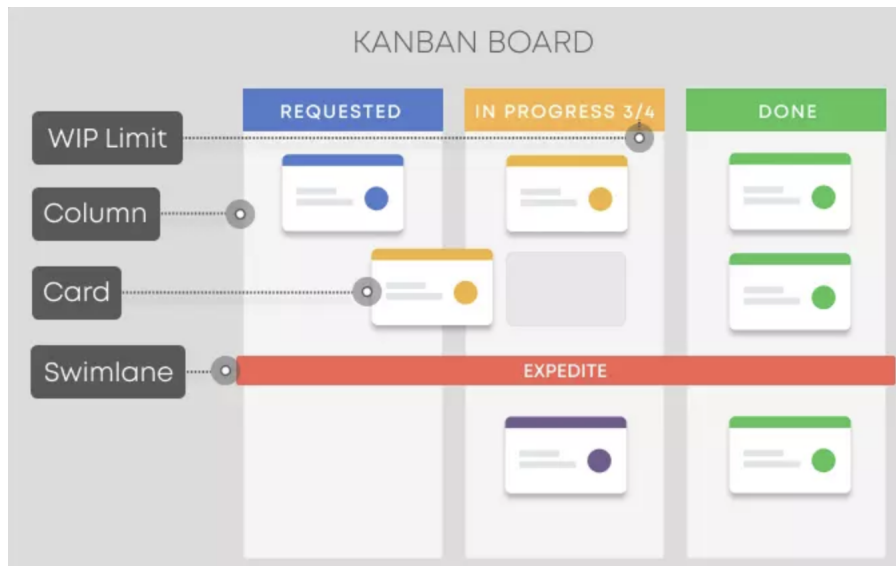
Il processo è diviso in tre fasi:

1. **Pre-game phase**:
 - (a) **Planning sub-phase**: viene creata una *Product Backlog List* che contiene tutti i requisiti conosciuti.
 - (b) **Architecture sub-phase**: viene già pianificato il design di alto livello e l'architettura del sistema.
2. **Development phase**: in questa fase il sistema viene sviluppato attraverso una serie di *Sprint*, ovvero cicli iterativi nei quali vengono sviluppate o migliorate una serie di funzionalità, e ogni sprint può durare circa 1-4 settimane. Lo *Sprint* ovviamente include le classiche fasi di sviluppo del software.
3. **Post-game phase**: il prodotto viene preparato per il rilascio, ovvero si prepara l'*integrazione*, i *test*, la *documentazione* per l'utente e la preparazione del materiale di *marketing*.

I ruoli principali durante l'esecuzione di un processo **SCRUM** sono tre:

- **Product Owner**: ci si riferisce a quella persona responsabile di accettare o rifiutare i risultati di un lavoro e di poter terminare uno *Sprint*, inoltre fa da raccordo fra tutti soggetti interessati nel progetto.
- **Membri del Team**: i membri decidono cosa fare in ogni *Sprint*, ogni team è indipendente e i membri non fanno capo ad alcun project manager. Ogni membro ha diverse specializzazioni (*cross-functional*), in modo tale da non avere persone con troppo carico di lavoro e ognuno si occupa di un singolo lavoro alla volta.
- **Scrum Master**: non ha alcuna autorità sul team, ma si occupa di supportarlo e motivarlo, garantendo anche le condizioni ambientali per lavorare al meglio.

Kanban Board Questa lavagna permette di gestire al meglio il flusso del lavoro. Come mostrato in figura è presente un *Work In Progress Limit* che definisce un limite alla quantità di post-it che possono essere presenti in ogni colonna. Questo limite permette di completare più velocemente i singoli lavori, in modo tale di dare qualcosa al cliente il prima possibile e di individuare facilmente i *colli di bottiglia* che possono rallentare gli altri lavori. Inoltre permette di ridurre il *task switching*, ovvero il lavoro su più task contemporaneamente.



Gli eventi che fanno parte di uno *Sprint* sono i seguenti:

1. **Sprint planning**: il *product owner* gestisce l'evento di pianificazione dello *Sprint*.
2. **Daily meeting**: i membri del team e gli SCRUM master si ritrovano davanti la *kanban* e discutono delle difficoltà che hanno riscontrato.
3. **Review**: alla fine di una modifica concreta al software, questo viene ispezionato in collaborazione con gli utenti per ottenere un feedback e per discutere su cambiamenti o nuove idee.
4. **Retrospettiva**: questa fase permette di riflettere, studiare e adattarsi per lo *Sprint* successivo.

2 Analisi dei Requisiti

Definizione (Analisi dei Requisiti). Si intende il processo di studio e analisi delle esigenze del committente e dell'utente per giungere alla produzione di un documento che definisce il *dominio* del problema e i *requisiti* del software. In alcuni casi si definiscono anche i *casi di test* e il *manuale utente*.

Prima di passare alla fase vera e propria di *analisi dei requisiti* occorre seguire una fase preliminare per stabilire la realizzabilità del progetto software.

2.1 Studio di Fattibilità

Si basa principalmente sulla descrizione del software e delle necessità dell'utente. In seguito vengono svolte due analisi:

- **Analisi di Mercato**: si fa un confronto con il mercato attuale e si stimano i costi di produzione e quanto l'investimento può essere remunerativo.
- **Analisi Tecnica**: si studiano tutti gli strumenti per la realizzazione del progetto, come i software, le architetture, gli hardware e gli algoritmi. Inoltre si studia come deve essere fatta la prototipazione del software e la futura ricerca.

2.2 Dominio

Il **dominio** è il contesto in cui il software opera. Per definirlo occorre costruire un **glossario**, ovvero una collezione di definizioni di termini rilevanti in quel dominio specifico e che può essere riusato in progetti successivi nello stesso dominio. Inoltre occorre definire un **modello statico**, quindi come interagiscono fra loro gli elementi del dominio staticamente, e un **modello dinamico**, ovvero come si comporta il dominio in base all'avvenire di un determinato evento che può coinvolgere gli utenti. Questi due modelli possono essere descritti sia tramite l'uso del linguaggio UML ³, sia usando la semplice descrizione testuale.

2.3 Requisiti

Definizione (Requisito). Il requisito è una proprietà che deve essere garantita dal sistema per soddisfare una qualsiasi necessità dell'utente.

I requisiti possono dividersi in due categorie:

³https://it.wikipedia.org/wiki/Unified_Modeling_Language

- **Requisiti funzionali:** quelli che descrivono le funzionalità e il comportamento del software.
- **Requisiti non funzionali:** descrivono le proprietà del software o del processo di sviluppo. Ad esempio le caratteristiche di efficienza e affidabilità, l'interfaccia, il linguaggio di programmazione e l'ambiente di sviluppo scelti, i vincoli legislativi e i requisiti hardware o di rete.

I requisiti possono essere descritti mediante l'uso di diversi linguaggi, formali o meno. In questo caso si vede la descrizione dei requisiti mediante la produzione di un documento scritto in linguaggio naturale.

2.4 Documento dei Requisiti

Questo documento è un contratto tra lo sviluppatore e il committente, che elenca i requisiti e i vincoli che il software deve soddisfare, e specifica anche una *deadline* per la consegna del progetto.

2.5 Fasi dell'Analisi dei Requisiti

L'*analisi dei requisiti* viene svolta in cinque passi:

1. **Acquisizione**
2. **Elaborazione**
3. **Convalida**
4. **Negoziazione**
5. **Gestione**

2.5.1 Acquisizione

Il team di analisti incontra i membri dell'organizzazione del committente e si procede con la raccolta dei requisiti che può avvenire tramite: semplici interviste, questionari, costruzione di prototipi (anche su carta), studio di documenti o l'osservazione di possibili utenti mentre lavorano.

2.5.2 Elaborazione

Viene scritta la prima bozza del *documento dei requisiti*, dove quest'ultimi vengono trattati in modo più approfondito. La struttura del documento deve essere la seguente:

<i>Introduzione</i>
<i>Glossario</i>
<i>Definizione dei Requisiti Funzionali</i>
<i>Definizione dei Requisiti Non Funzionali</i>
<i>Architettura</i> : la strutturazione del software in sottosistemi.
<i>Specifica dettagliata dei Requisiti Funzionali</i>
<i>Modelli astratti</i> : descrivere il sistema in base a ciascun punto di vista.
<i>Evoluzione del sistema</i> : successivi cambiamenti.
<i>Appendici</i> : descrizione della piattaforma hardware, database, manuale utente e i piani di test.
<i>Indici</i> : costruire un lemmario, quindi una lista di termini che puntano ai requisiti che li usano.

Nota Bene Nella descrizione dei requisiti occorre sempre usare la forma assertiva. Esempio:

Il <sistema> deve <funzionalità>/<proprietà>

2.5.3 Convalida

Nella fase di convalida occorre revisionare il documento per far sì che vengano evitati i seguenti difetti:

- **Omissioni**: requisiti mancanti.
- **Inconsistenze**: contraddizione tra i requisiti o tra un requisito e il contesto.
- **Ambiguità**: vaghezze o requisiti che possono avere più significati. Le ambiguità all'interno del linguaggio naturale possono essere portate da **quantificatori**, **disgiunzioni** oppure possono presentarsi ambiguità di **coordinazione** (nel caso si usano sia la o che la e nella stessa frase) oppure **referenziale** nell'uso non chiaro di pronomi. Inoltre occorre sempre evitare **verbi deboli**, **forme passive**, ovvero verbi senza un soggetto esplicito ed anche **negazione** e **doppie negazioni**.
- **Sinonimi** e **Omonimi**: termini diversi con lo stesso significato e termini uguali con significato diverso.
- **Presenza di dettagli tecnici**
- **Ridondanza**: può esserci, ma solo tra sezioni diverse del documento.

Le principali tecniche di convalida dei requisiti sono:

- **Deskcheck**
 - **Walkthrough**: ovvero il documento viene analizzato per intero sequenzialmente.
 - **Ispezione**: la lettura del documento è strutturata, utilizzando per esempio la tecnica del lemmario.
- Uso di **strumenti di analisi** del linguaggio naturale.
- Uso di **prototipi**.

Una volta trovati i difetti, è importante ricordarsi che vanno sempre risolti con il committente.

2.5.4 Negoziazione

In questa fase vengono assegnate delle priorità ai requisiti in base alle **esigenze del committente** e ai **costi** e **tempi** di produzione.

Questa fase è importante per decidere se alcuni requisiti possono essere **cancellati** oppure **sviluppati** successivamente.

MoSCoW Questa è una tecnica per dare priorità ai requisiti, i quali vengono divisi in quattro classi:

- **Must have**: requisiti irrinunciabili per il cliente.
- **Should have**: non necessari ma utili.
- **Could have**: non molto utili, da realizzare solo se c'è tempo.
- **Want to have**: da sviluppare in successive versioni.

2.5.5 Gestione

Questa fase si occupa di tre aspetti principali:

- **Identificazione**: ad ogni requisito viene assegnato un identificatore univoco.
- **Attributi**: ad ogni requisito vengono assegnati attributi relativi allo **stato**, **priorità**, **sforzo** in termini di giorni e/o personale da impiegare, **rischio**, e la **versione destinazione** per quanto riguarda lo sviluppo incrementale.
- **Tracciabilità**: ovvero la capacità di descrivere e seguire la vita di un requisito. Viene costruita una mappa tra i requisiti e le **componenti del sistema**, il **codice** ed i **test**.

Contratto Il documento dei requisiti precede la stipula del contratto.

2.6 Casi d'uso

I **casi d'uso** sono un altro modo per acquisire i requisiti, valutando le interazioni degli utenti col sistema e indicando al committente i risultati attesi. I casi d'uso oltre ad includere la sequenza corretta di eventi attesi devono anche presentare i comportamenti inattesi, ovvero le **eccezioni**.

2.7 User Stories

Sono un'altra tecnica di raccolta dei requisiti utilizzata principalmente nei **processi agile** e consiste nell'utilizzo di **user story cards** per scrivere i requisiti, che in linea generale hanno questa forma:

*Nel mio ruolo di <ruolo utente>, ho bisogno che il sistema
<funzione>, al fine di <beneficio>*

Contro Il problema principale delle *user stories* è la **scalabilità**, ovvero sono difficili da trasporre su grandi progetti e problematiche se il team è distribuito geograficamente. Inoltre, essendo informali e brevi non sono adatte per raggiungere degli accordi legali e raramente includono i *requisiti non funzionali*.

3 Linguaggio UML e Casi d'Uso

Definizione (Modello). Un *modello* è un'astrazione del dominio, usato per specificarne la natura e il comportamento.

I modelli possono classificarsi in:

- **Modelli Statici**: vengono rappresentate le *entità* e le *relazioni* fra esse per permettere di descrivere al meglio il dominio, le componenti architettureali e le classi da realizzare.
- **Modelli Dinamici**: vengono modellati i comportamenti delle entità descritte nel *modello statico*.

Un modello può essere:

- Una *bozza* o *sketch*, quindi un modello molto incompleto, usato principalmente per descrizioni iniziali.
- Un progetto dettagliato chiamato *blueprint*, che permette ai programmatori di realizzare direttamente il software senza prendere decisioni di progettazione.
- Un *eseguibile*, talmente preciso e completo da poter generare il codice in automatico partendo solo dal modello.

3.1 UML

Definizione (UML). L'*Unified Modeling Language* è un linguaggio di modellazione unificato che ha il compito di supportare la descrizione e il progetto di software, nello specifico di applicazioni *object oriented*, ma permette anche di descrivere i modelli da più punti di vista in modo molto comprensibile sia dai clienti che dagli utenti.

3.2 Diagramma dei Casi d'Uso

Permette di descrivere i *requisiti funzionali* del sistema, catturando nello specifico le funzionalità viste dall'esterno (lato utente).

Definizione (Attore). Un **attore** è un'entità esterna al sistema, che interagisce con esso. Gli attori possono essere classificati in:

- Un *utente umano* che possiede un determinato ruolo.
- Un altro *sistema*.
- Il *tempo*.

All'interno del diagramma gli attori sono delle classi e sono indicati con un nome in maiuscolo. Dato che sono classi è possibile fare delle generalizzazioni sugli *attori*, ovvero è possibile creare delle gerarchie.

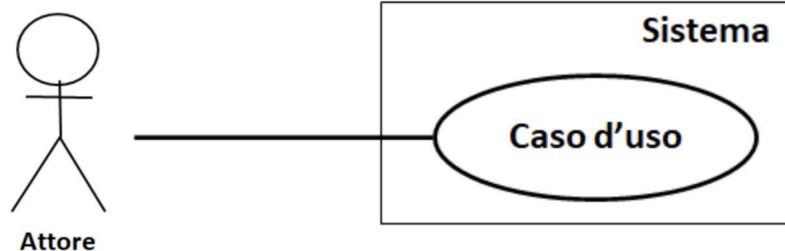
Definizione (Caso d'Uso). Un **caso d'uso** è una funzionalità o un servizio offerto dal sistema a uno o più attori, e viene espresso tramite un insieme di *scenari*.

All'interno del diagramma, anche i casi d'uso sono scritti in maiuscolo, e per descriverli vengono usati dei *verbi* che ne indicano il compito.

Il *diagramma dei casi d'uso* oltre ad essere composto da *attori* e da *casi d'uso*, presenta anche:

- **Relazioni:** tra gli attori e i casi d'uso che rappresentano un'interazione.
- Il **confine del sistema:** un rettangolo disegnato intorno ai casi d'uso per indicare il confine del sistema.

È importante specificare che un caso d'uso è sempre iniziato da un solo attore, chiamato **attore principale**. Inoltre, possono essere presenti casi d'uso non collegati ad alcun attore.



3.3 Narrativa dei Casi d'Uso

Per poter descrivere il *modello dinamico*, viene redatto un documento che permette di rappresentare gli scenari di ogni caso d'uso dal punto di vista di ogni attore coinvolto.

La descrizione di un caso d'uso segue questa struttura:

Nome
Breve descrizione
Attore primario
Attori secondari
Precondizioni
Sequenza degli eventi principale
Postcondizioni
Sequenze alternative degli eventi

Definizione (Precondizioni e postcondizioni). Le **precondizioni** e le **post-condizioni** sono dei predicati che devono sempre essere veri in uno stato: per le *precondizioni* prima di iniziare il caso d'uso, per le *post-condizioni* alla fine. La relazione tra *precondizioni*, *postcondizioni* e sequenza principale ed alternativa ha a che fare con la *logica di Hoare*⁴, infatti è possibile costruire la seguente *trippla di Hoare*:

$$\{Precondizione\} Sequenza Principale \{Postcondizione\}$$

Ciò significa che per ogni stato σ che soddisfa la *precondizione*, se l'esecuzione della *sequenza principale* nello stato σ termina producendo uno stato σ' , allora la *postcondizione* nello stato σ' deve essere vera.

Questo però significa che se l'esecuzione della *sequenza principale* non termina o termina in modo inaspettato come indicato nella *sequenza alternativa*, allora la *postcondizione* non è garantita.

Definizione (Scenario). Uno **scenario** è un'istanza di un caso d'uso, ovvero una sequenza di interazioni tra il sistema e gli attori che produce un risultato osservabile.

Gli scenari descritti dalla *sequenza degli eventi principale* sono quelli che portano alle *postcondizioni*.

La *sequenza degli eventi principale* elenca i passi che compongono il caso d'uso ed ogni passo presenta la seguente sintassi:

<numero>. <soggetto><azione><complementi>

Il primo passo, inoltre, è sempre compiuto dall'*attore principale*. All'interno della sequenza possono anche presenti *condizioni* e *cicli*, scritti in pseudocodice.

3.3.1 Inclusione

L'*inclusione* permette di creare una relazione di dipendenza tra casi d'uso.

Il caso d'uso *incluso* può essere *istanziabile* (o *completo*), quando è avviato da un attore, oppure *non istanziabile*, quando viene eseguito solo quando è incluso.

⁴https://it.wikipedia.org/wiki/Logica_di_Hoare

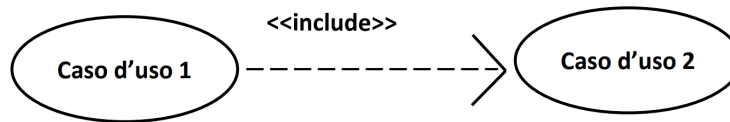


Figure 2: Il Caso d'uso 1 include il Caso d'uso 2.

Nota Bene È importante non usare la relazione di inclusione per fare decomposizione di un caso d'uso.

3.3.2 Estensione

L'*estensione*, a differenza dell'*inclusione*, non è una dipendenza, ma permette a un caso d'uso di incorporarne opzionalmente un altro.

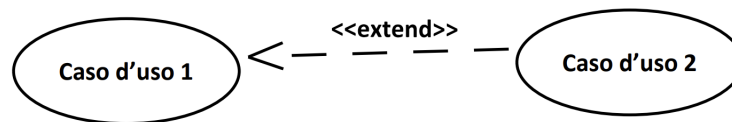
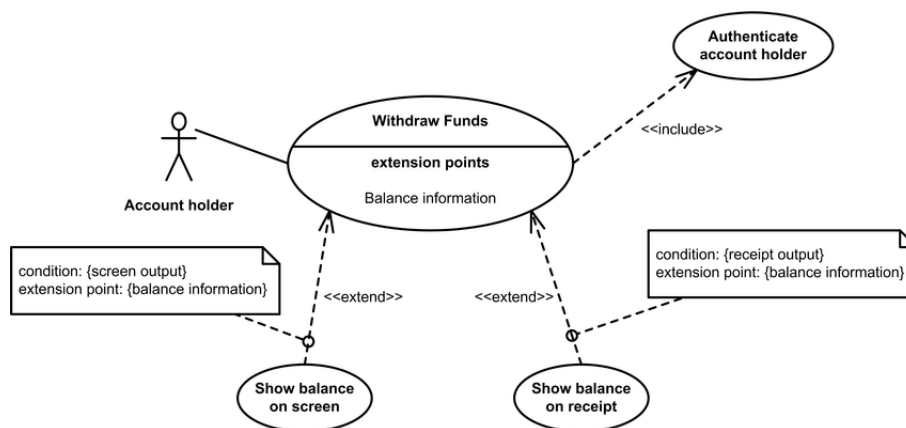


Figure 3: Il Caso d'uso 1 può essere esteso dal Caso d'uso 2.

Extension Points Gli *extension points* sono una notazione che permette di identificare quando e dove inserire l'estensione. Si collega un vincolo alla freccia <<extend>> indicando la condizione che deve essere vera affinché l'estensione venga applicata.



3.4 Classi e Oggetti

Definizione (Oggetto). Un **oggetto** è un'entità caratterizzata da un'*identità*, uno *stato*, ovvero i valori degli *attributi* dell'oggetto, e da un *comportamento*, quindi le operazioni che lo definiscono.

Definizione (Classe). Una **classe** è un insieme di *oggetti* con caratteristiche simili, quindi che hanno lo stesso tipo.

Una classe permette di catturare gli elementi del dominio del sistema.

3.4.1 Diagramma delle Classi

Descrive le *proprietà* e le *operazioni* di un classe, il *tipo degli oggetti*, e le *relazioni statiche* fra essi.

Nome della Classe
- <i>attributo: tipo</i>
+ <i>attributo: tipo</i>
+ <i>operazione(tipo): tipo</i>

Una classe viene rappresentata in questo modo, con il nome sempre in maiuscolo, la sezione che riguarda gli attributi e quella che riguarda le operazioni. Il simbolo **+** indica un attributo/operazione privata, mentre il **-** ne indica uno pubblico. Esistono anche altri due simboli per la *visibilità*: il **#**, che indica che l'attributo o l'operazione è accessibile anche alle classi discendenti nella *gerarchia*, mentre

la **~** che indica l'accessibilità solo alle classi nello stesso *package*. Inoltre, per specificare che un attributo o un'operazione sono *statici*, si sottolineano.

Nonostante ciò, quando si usa il diagramma delle classi per descrivere il dominio, sia le operazioni che la visibilità e i dettagli implementativi degli attributi si omettono.

Attributi La sintassi degli attributi è la seguente:

Visibilità Nome: Tipo[Molteplicità] = ValoreDefault {Proprietà}

La *molteplicità* indica gli array di valori, quando è uguale a 1 può essere omessa. Invece, le *proprietà* possono essere sui valori dell'attributo, oppure nel caso la molteplicità è maggiore di 1 si può usare {ordered} per indicare che nell'array l'ordine degli elementi conta, e {unique} per dire che gli elementi dell'array non devono avere ripetizioni.

Operazioni La sintassi delle operazioni è la seguente:

Visibilità Nome: (ListaParametri) : TipoRitorno

Con *ListaParametri* definita dalla seguente grammatica:

$$ListaParametri ::= \emptyset \mid DichiarazioneParametro, ListaParametri$$

$$DichiarazioneParametro ::= Nome : Tipo = ValoreDefault$$

Enumerazioni Sono usate per specificare una lista prefissata di valori che un *attributo* può assumere. In UML sono etichettate con lo stereotipo <<enumeration>>.

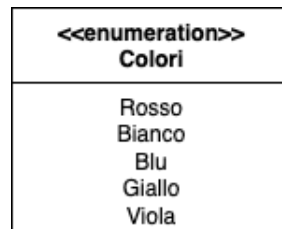


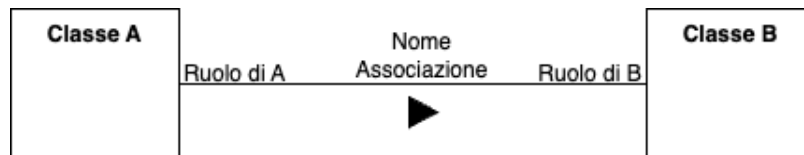
Figure 4: Esempio di enumerazione con l'attributo *colore*.

3.4.2 Relazioni

Definizione (Relazione). Una *relazione* rappresenta un legame tra due o più oggetti.

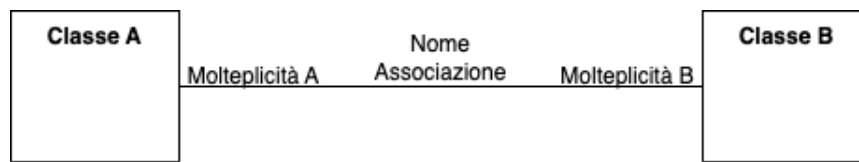
In UML viene rappresentata da una linea retta con sopra scritte il *nome dell'associazione*, il *ruolo* di ogni classe, ed eventualmente una freccia che sta ad indicare il verso di lettura dell'associazione.

In generale si usa specificare o solo il *nome dell'associazione* o solo i *ruoli*.



Molteplicità La *molteplicità* indica il numero di oggetti coinvolti in un'associazione in un dato istante. Può essere definita in uno dei seguenti modi:

- Con un numero positivo.
- Con * che indica un valore indefinito.
- Indicando gli estremi inferiore e superiore di un intervallo (es. 2..4, 0..5, 7..*).



Associazioni Riflessive Si riferiscono alla stessa classe e, in questo caso, è fondamentale il ruolo dei due oggetti.

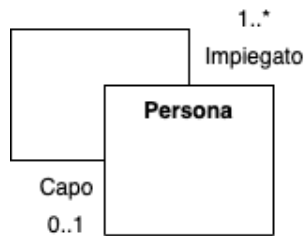


Figure 5: Esempio di associazione riflessiva.

3.4.3 Aggregazione e Composizione

L'**aggregazione** e la **composizione** sono tipi di relazioni in cui viene specificato che un oggetto di una classe *fa parte* di un oggetto di un'altra classe. L'*aggregazione* è meno forte come relazione, quindi si verifica quando le *classi parte* hanno un significato anche senza la presenza della *classe tutto*. Nella *composizione*, invece, la *classe parte* ha un senso solo se legata alla *classe tutto*.

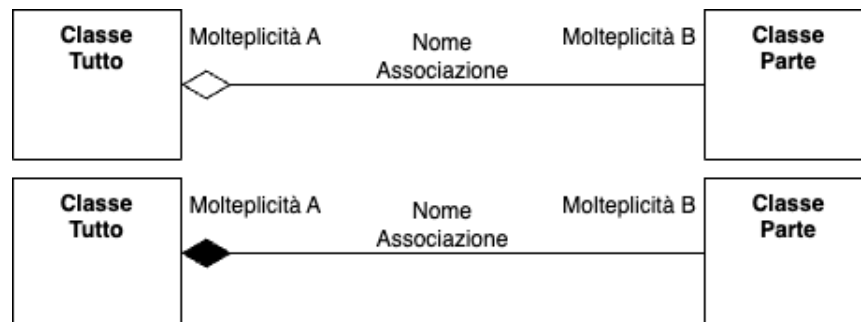


Figure 6: Sopra *aggregazione*, sotto *composizione*.

3.4.4 Generalizzazione

Consiste in una relazione tra una classe più generica e una più specializzata: la classe specializzata o *sottoclasse* eredita tutte le caratteristiche della *superclasse*, può aggiungerne delle altre, e può ridefinire delle *operazioni*.

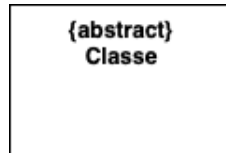
In questa relazione vale il *Principio di Sostituzione di Liskov*⁵, ovvero un oggetto della classe specializzata può essere usato al posto di un oggetto della superclasse.



⁵https://it.wikipedia.org/wiki/Principio_di_sostituzione_di_Liskov

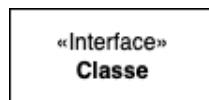
3.4.5 Classi Astratte

Le **classi astratte** definiscono delle classi che non sono implementate completamente.



3.4.6 Interfacce

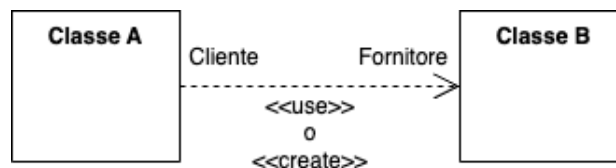
Le **interfacce** si usano in fase di *progettazione* per definire delle classi con solo operazioni e senza attributi.



Nota Bene Sia le *interfacce* che le *classi astratte* non possono essere istanziate, ma si utilizzano nelle *gerarchie* per definire la "struttura" di classi più complete.

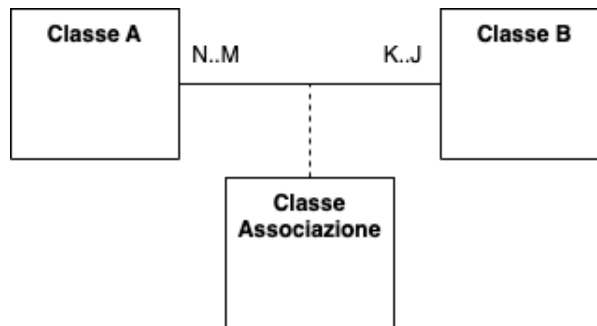
3.4.7 Dipendenze

La dipendenza è una relazione in cui le classi hanno un ruolo di *cliente* e di *fornitore*. Questo avviene quando un parametro di un'operazione della classe *cliente* è un oggetto della classe *fornitore*, o se un'operazione del *cliente* restituisce o crea dinamicamente un oggetto del tipo del *fornitore*.



3.4.8 Classi Associazione

Un'associazione può avere dei propri attributi, rappresentati con una **classe associazione**. Per ogni coppia di classi, può esistere solo una *classe associazione*.



3.4.9 Classi di Analisi

Le **classi di analisi** corrispondono ai concetti concreti del dominio, per esempio i termini del glossario. Queste classi hanno un numero ridotto di **funzionalità** e durante la loro definizione occorre evitare di:

- Definire classi "**onnipotenti**".
- Definire classi che in realtà sono delle **funzioni**.
- Definire delle **gerarchie** troppo profonde (più di 3 livelli).
- Specificare troppo i **tipi** e i **valori** degli **attributi**.

Inoltre le **operazioni** e gli **attributi** vanno indicati solo quando sono veramente utili.

Le principali tecniche di definizione delle **classi di analisi** sono:

- **Data Driven**: durante la *fase di analisi*, si identificano tutti i dati del sistema e si dividono in classi.
- **Responsibility Driven**: durante la *fase di progettazione* si identificano le operazioni e si dividono in classi.

L'analisi **nome-verbo** consiste nell'associare ai **sostantivi** le classi e gli attributi, mentre ai **verbi** le operazioni. Successivamente si individuano le relazioni fra le classi. Utilizzando questo tipo di approccio occorre prestare attenzione ai casi di sinonimia per evitare di definire classi inutili; e bisogna saper individuare le classi nascoste del dominio, cioè quelle che non vengono mai menzionate esplicitamente.

3.4.10 Diagramma degli Oggetti



3.5 Diagramma delle Attività

Sono utili per descrivere delle **attività** relative a un qualsiasi *oggetto* o *classe*, ovvero un insieme di azioni che possono essere *sequenziali*, *condizionali*, *concorrenti* e *iterative*.

Si usano sia nella fase di *analisi* per modellare un processo o un caso d'uso, ma anche per descrivere l'*operazione* di una classe o per modellare un algoritmo in fase di *testing*.

Il contenuto di un'attività è un *grafo diretto* in cui i **nodi** sono le *azioni* o i *nodi di controllo*, mentre gli **archi** sono i possibili percorsi percorribili per l'attività.



Azioni È importante sottolineare che le azioni devono essere **atomiche**, cioè non interrompibili. Inoltre per ogni azione ci può essere solo una freccia entrante e una uscente. Quando un'azione è giunta al termine avviene una transazione automatica chiamata **token** che porta all'azione successiva.

Nodi di Decisione Un nodo di decisione deve poter coprire tutti i casi possibili, in modo che il **token** non possa bloccarsi. Opzionalmente le *guardie* possono essere **mutualmente esclusive**. Inoltre, dato un *nodo decisione* non è obbligatoria la presenza di un *nodo fusione*.

Le *guardie* si scrivono sempre tra parentesi `[]`.

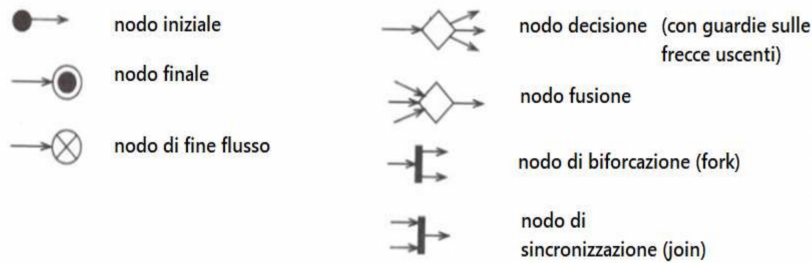


Figure 7: Nodi di Controllo

Fork & Join La *fork* moltiplica i token, producendone uno per ogni uscita. La *join* invece attende un token per ogni freccia entrante e, quando li consuma tutti, ne esce solo uno. Come per i nodo di decisione non è necessaria una *join* per ogni *fork*.

Nodo di Fine Attività Quando un qualsiasi token raggiunge questo nodo tutta l'attività termina. Solo su questi nodi, e su quelli di *fine flusso*, possono essere presenti più archi entranti; ciò sta a significare che il primo token che arriva termina l'attività.

Nodo di Fine Flusso Questo tipo di nodo non termina l'attività, ma consuma il token.

3.5.1 Segnali & Eventi

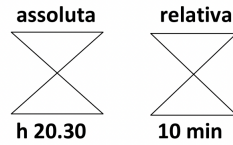
- Accettazione di un evento esterno.



- Invio di un segnale. L'invio di segnali è [asincrono](#), cioè non blocca l'attività.



- Accettazione di un evento temporale.

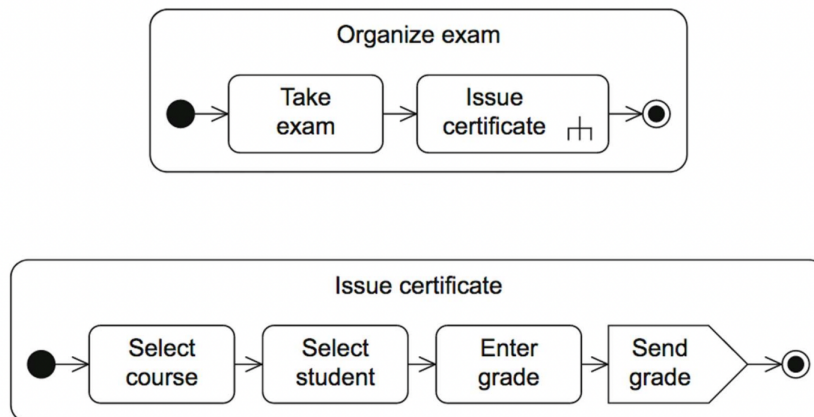


Per gli eventi **esterni** e **temporali**, gli archi entranti non sono necessari, quindi in questo caso quando si verifica quel determinato evento viene generato un token. Se invece gli archi entranti sono presenti, quando arriva il token questo attende che l'evento esterno si verifichi.

A differenza delle **azioni** che si usano quando le attività sono effettuate dalle entità di cui si sta descrivendo il comportamento, mentre i **segnali** e gli **eventi** si usano quando si comunica con un'entità esterna.

3.5.2 Sotto-Attività

Un diagramma può contenere il riferimento a delle attività secondarie, rappresentate come un'azione ma con in più il simbolo di un "rastrello".



3.5.3 Partizioni

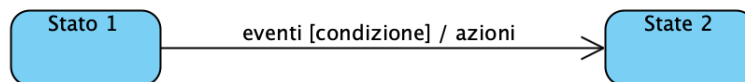
Le **partizioni** permettono di dividere le azioni, assegnandole all'entità che ne è responsabile.

3.6 Macchina a Stati

È un grafo “*stati-transizioni*” che permette di descrivere il comportamento delle istanze di una classe. A differenza dei *diagrammi delle attività* dove l’obiettivo è mettere in ordine un insieme di azioni, qui viene mostrata l’evoluzione degli oggetti in risposta a determinati eventi.

Ogni *transizione* avviene al verificarsi di un determinato evento interno, rappresentato da un’*operazione* della classe; oppure tramite messaggi inviati da altri oggetti.

In una *transizione*, gli *eventi* possono essere accompagnati anche da una *condizione* e da una sequenza di azioni.



La semantica è la seguente: se si verifica almeno uno degli eventi, e vale la condizione, si eseguono tutte le azioni e si passa nell’altro stato.

3.6.1 Eventi

Le *transizioni* possono essere *non deterministiche*, cioè da uno stato ci possono essere più transizioni con lo stesso evento.

Gli eventi possono classificarsi in:

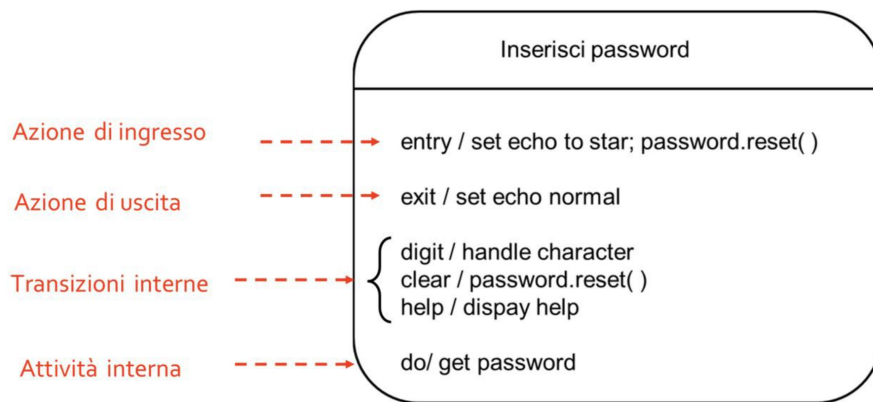
- Eventi di *operazione* o *segnale*: `op(a: T)`. Ovvero la transizione è abilitata quando riceve un segnale o avviene una chiamata di metodo con parametri `a` e tipo `T`.
- Eventi di *variazione*: `when(exp)`. La transizione è abilitata quando `exp` diventa vera.
- Eventi *temporali*: `after(time)`. La transizione è abilitata dopo che l’oggetto è stato fermo per un tempo `time` in quello stato.

Entry Anche chiamata *azione di entrata*, viene eseguita all’ingresso di uno stato.

Exit Anche chiamata *azione di uscita*, viene eseguita quando si esce da uno stato.

Transizione Interna Risposta a un determinato evento, ma si rimane nello stesso stato.

Do-Activity Azione eseguita in continuazione finchè l'oggetto si trova in quello stato. A differenza delle altre azione che sono *atomiche*, queste consumano del tempo e possono essere interrotte, ad esempio quando si esce dallo stato.



3.6.2 Stato Composito Sequenziale

Consiste nell'avere uno stato che contiene un'altra *macchina a stati*. Quando una transizione entrante nello *stato composito* termina sul bordo, vuol dire che si prosegue a partire dallo *stato iniziale* dello *stato composito*. Altrimenti la transizione può avere come *target* anche uno stato interno. Le transizioni di uscita, invece, possono anch'esse partire dal bordo, in tal caso significa che ci si può andare da qualsiasi stato interno, altrimenti quelle che partono da un singolo stato interno sono possibili solo da esso. Esiste anche una transizione d'uscita speciale chiamata di *completamento*, dalla quale ci si può passare solo una volta arrivati nello stato finale dello stato composito.

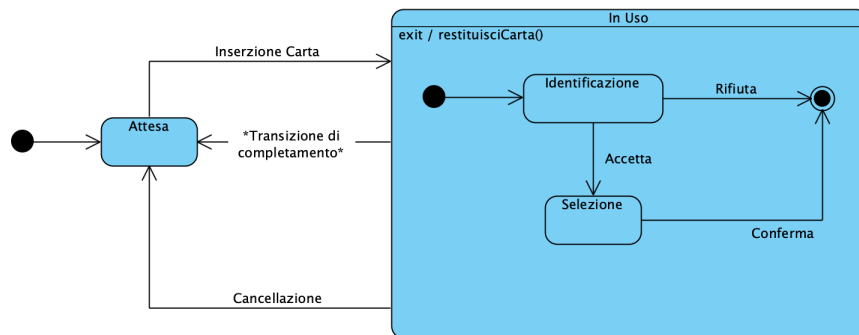
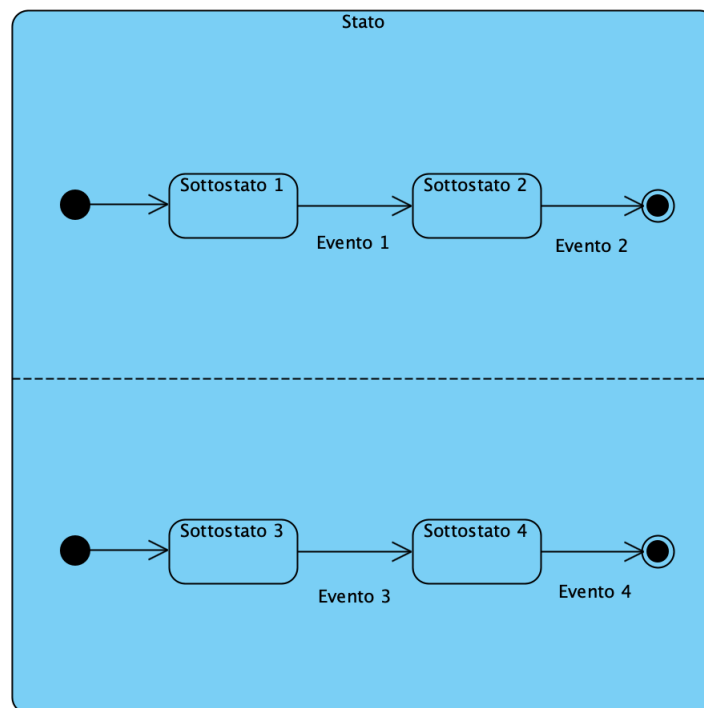


Figure 8: Esempio di macchina a stati che descrive l'uso di un sistema di pagamento con stato composito sequenziale.

3.6.3 Stato Composito Parallelo

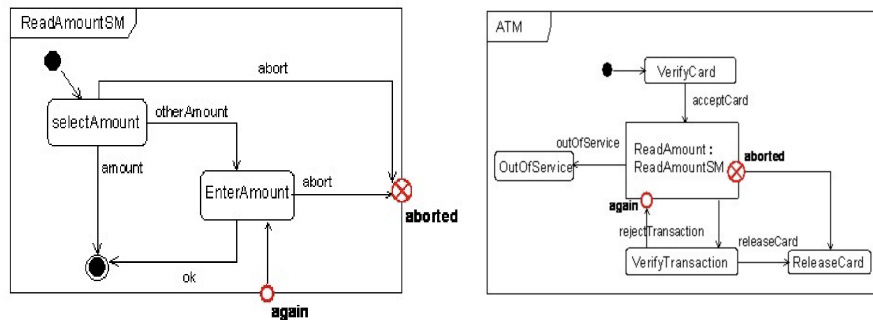
Nello *stato composito* abbiamo più sottostati che si eseguono in modo parallelo. Una transizione entrante sul bordo attiva tutti gli stati iniziali. La *transizione di completamento* può avvenire solo se si è arrivati in tutti gli stati finali. Mentre, una transizione di uscita che parte dal bordo è raggiungibile da un qualunque stato interno e fa uscire da **tutti** i sottostati. Anche un transizione che parte da un singolo stato interno fa uscire da tutti i sottostati e può avvenire solo se ci si trova in quel determinato stato.



3.6.4 Sottomacchine

Le *sottomacchine* si usano quando si vuole rappresentare uno stato composito in un diagramma a parte, in modo da poterlo riusare in più contesti. La *sottomacchina* ha un nome che ne definisce il Tipo e le sue istanze si indicano con Nome Istanza: Tipo.

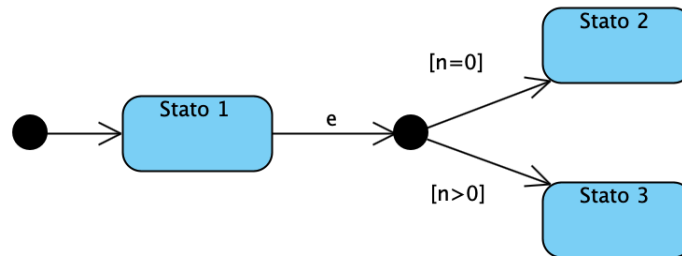
Entry & Exit Points Sono dei nodi che servono per poter collegare le transizioni della macchina principale con la sottomacchina.



In questo caso le *transizioni di completamento* possono scattare anche quando si arriva in un *exit point*.

3.6.5 Pseudostati

Giunzione Uno *pseudostato* da cui possono entrare e/o uscire due o più transizioni. Se sono presenti condizioni, queste sono valutate in modo *statico*, quindi prima che avvengano gli eventi interessati. Inoltre, se le condizioni non coprono tutti i casi, l'evento può essere ignorato e si rimane in quello stato.



Decisione A differenza delle *giunzioni*, questo sono valutate *dinamicamente*, quindi dopo che avvengono gli eventi; e devono coprire tutti i casi possibili. Ovviamente un'altra differenza con le *giunzioni* è che in questo caso la transizione entrante può essere solo una.

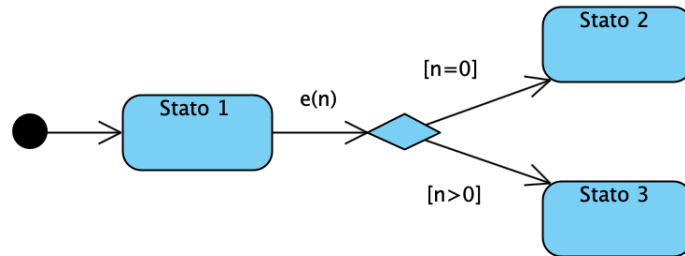


Figure 9: In questo esempio bisogna avere garanzia che $n \geq 0$.

Storia Lo stato *history* permette di memorizzare lo stato della macchina quando viene *interrotta* o *spenta*. La transizione entrante nello stato *history*, invoca il ripristino dello stato precedente, mentre se c'è una transizione uscente, questa indica lo stato in cui passare nel caso in cui la macchina non sia ancora stata mai interrotta, quindi quando lo stato *history* è vuoto.

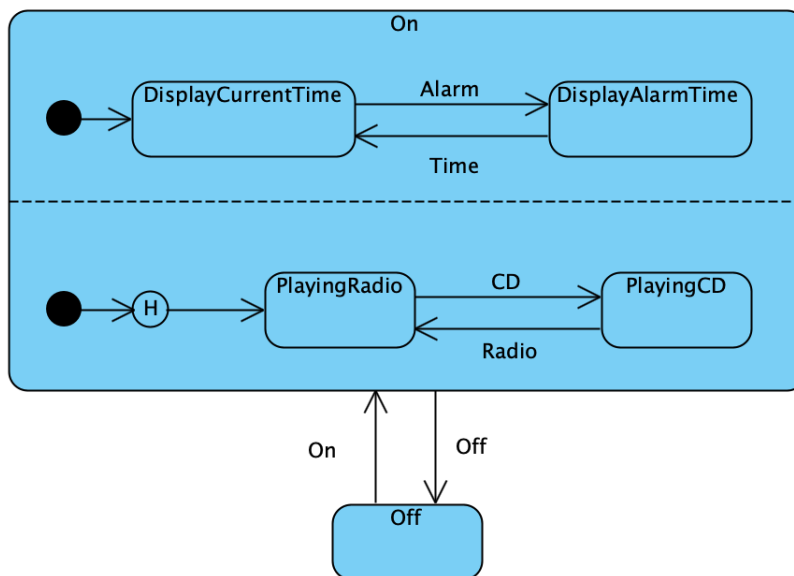


Figure 10: In questo esempio di funzionamento di un autoradio, la prima volta che si accenderà verrà riprodotta in automatico una stazione radio.

4 Architetture Software

La *progettazione* è la fase che segue la *specifica* e precede la *codifica*. Descrive in che modo deve essere realizzato il progetto. Il suo prodotto si chiama *architettura*.

Esistono due tipi di *progettazione*:

- Progettazione di *alto livello*: lo scopo è identificare e scomporre il sistema in tanti piccoli sottosistemi e definire le loro interconnessioni.
- Progettazione di *dettaglio*: si decide come ogni singolo *sottosistema* deve essere realizzato.

Quindi l'*architettura* di un sistema software è la struttura del sistema costituita dalle sue parti e dalle relazioni fra esse, più le loro proprietà visibili all'esterno. Vengono considerati anche gli aspetti *non funzionali*.

Durante questa fase il sistema viene analizzato attraverso tre punti di vista:

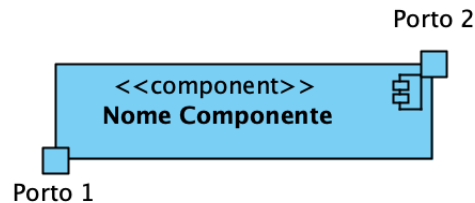
- Vista *Comportamentale* o *component-and-connector*: questa vista descrive il sistema trattandolo come composizione di altri software. Quindi si specificano tutte le componenti (i software), che presentano delle *interfacce*, successivamente si descrivono le caratteristiche dei *connettori* che collegano le varie componenti. Infine si analizza la struttura del sistema in esecuzione, infatti questa vista è molto utile per analizzare la qualità e le prestazioni del software e per documentare lo stile dell'*architettura*.
- Vista *Strutturale*: permette di descrivere la struttura del sistema vedendolo come un insieme di *classi* e/o *packages*. È utile per analizzare le dipendenze tra le *classi/packages* e per progettare i test di *unità* e di *integrazione*.
- Vista *Logica* o di *deployment*: descrive l'allocazione del software su più ambienti di esecuzione.

4.1 Vista Comportamentale

Definizione (Componente). Una *componente software* è un'unità software indipendente e che può essere riusata da altri componenti. Incapsula un insieme di funzionalità e/o di dati di un sistema, restringendo l'accesso ad essi tramite la definizione di *interfacce*.



Definizione (Porti). I **porti** identificano i punti di interazione di un componente, ogni componente ne ha uno per ogni connessione che ha con altri componenti. Un *porto* può richiedere una o più interfacce dello stesso tipo.



Le **interfacce** possono essere rappresentate in modo esteso o in modo sintetico mediante l'uso di *forchette* (quando viene richiesta un'interfaccia) o *lollipop* (quando l'interfaccia è fornita).

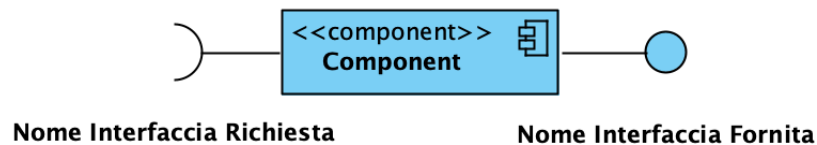


Figure 11: Modo Sintetico

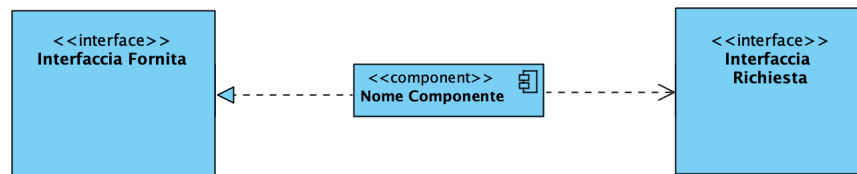


Figure 12: Modo Esteso

Definizione (Connettori). I **connettori** sono i canali di comunicazione che collegano i *porti* fra componenti diverse. Sul connettore è possibile indicare il *protocollo di comunicazione* utilizzato fra << . . . >>.

4.1.1 Stili Architeturali

Definizione (Stile). Uno **stile** è una proprietà dell'architettura che ne caratterizza una famiglia con caratteristiche e interazioni fra componenti comuni.

Pipe & Filter Le componenti sono di tipo *filtro*, ovvero effettuano delle trasformazioni sui dati che provengono dai porti d'ingresso e li mandano sui porti d'uscita. I connettori, invece, sono di tipo *pipe*, ovvero un canale di comunicazione unidirezionale e che preserva l'ordine dei dati che entrano e che escono.

Client-Server Il sistema è formato da componenti che si comportano da *client* e altri da *server*. Il client si connette a un server tramite un porto per richiedere un servizio, il server può ricevere connessioni da parte di più client.

Master-Slave È un caso particolare del modello *client-server*, in cui lo *slave* (il server) può servire un solo *master* (client).

Peer-to-Peer Tutti i componenti agiscono sia da client che da server, quindi nella rappresentazione ci sarà un solo componente.

Publish-Subscribe I componenti interagiscono tra loro tramite l'annuncio di eventi, una componente può svolgere sia il ruolo di *Publisher* (produttore di eventi) che di *Subscriber* (consumatore di eventi). Questo stile può coinvolgere anche un intermediario chiamato *broker*, che permette alle altre componenti di non interagire direttamente fra loro e quindi di non essere consapevole delle identità delle altre.

Model-View-Controller Permette di isolare il *modello*, ovvero le funzionalità e i dati del sistema, la *vista*, quindi come viene rappresentato il modello, e il *controllore*, che riceve l'input ed effettua le chiamate alle operazioni del modello.

Coordinatore di Processi Prevede l'uso di un componente noto come *coordinatore*, che conosce la sequenza per realizzare il processo. Una volta ricevuta la richiesta, chiama le componenti *server* nell'ordine prefissato e successivamente fornisce una risposta. I *server* non sono a conoscenza del loro ruolo, ma si limitano solo a fornire un servizio.

4.2 Vista Strutturale

Gli elementi di questa vista sono chiamati *moduli*, ed essendo classi o packages, le relazioni fra essi sono di ereditarietà, dipendenza o composizione. Un *package* può contenere un insieme di classi e/o di altri packages.

Questo tipo di vista è utile per fornire uno schema del codice e dei file sorgenti, non verrà utilizzato per le analisi dinamiche, effettuate con viste *comportamentali* e *logistiche*.

Nelle classi, rispetto alla descrizione del *dominio*, qui si specificano meglio le loro operazioni.

4.2.1 Vista Strutturale a Strati

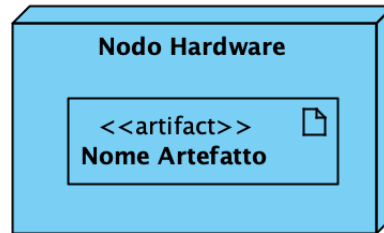
Gli elementi sono gli *strati*, ovvero un insieme di moduli, che possono essere raggruppati in *segmenti*, inoltre implementano un'interfaccia pubblica, chiamata *macchina virtuale* per i servizi che offrono. La relazione fra gli strati è di tipo `<<allowedToUse>>`, è antisimmetrica e non è transitiva.

4.2.2 Vista Strutturale di Generalizzazione

Gli elementi sono sempre i moduli, ma la relazione è solo di *generalizzazione*.

4.3 Vista Logistica

In questa vista gli elementi possono essere *hardware* (rappresentati da parallelepipedi) come l'ambiente di esecuzione, oppure *software* (con stereotipo `<<artifact>>`), chiamati *artefatti*, cioè qualsiasi file che viene utilizzato o prodotto da un software da un sistema generale. Si usa per valutare le prestazioni e per redigere una guida per l'installazione del software. Le relazioni tra i gli elementi hardware possono essere connessioni fisiche o protocolli di comunicazione.



Artefatto L'artefatto è una copia di un'implementazione di un componente che è stata installata su un ambiente di esecuzione. L'artefatto si dice che "*manifesta*" (<<manifesta>>) un componente.