

Controlli contro le minacce dei programmi

Lezione 11 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Studi in Informatica applicata, AA 2006-7

Indice

1. Controlli contro le minacce dei programmi
2. controlli per lo sviluppo del software
3. alcuni principi di ingegneria del software
4. architetture del processo produttivo
5. modello a cascata
6. modelli incrementali
7. prototipazione rapida
8. modelli evolutivi
9. modello a spirale
10. riferimenti

controlli per lo sviluppo del software

lo sviluppo di software sicuro è in larga misura un **problema di progettazione di qualità**:

progettare il processo produttivo di un prodotto che abbia desiderate caratteristiche di qualità (di sicurezza, per ciò che qui interessa)

motivazioni del problema:

non esiste un tipo universale di processo produttivo adatto a tutte le situazioni
caratteristiche di qualità del prodotto sono conseguibili solo se il processo produttivo ha caratteristiche di qualità ad esse corrispondenti
mediazione fra **obiettivi di qualità** del prodotto e **vincoli** posti dal contesto produttivo

esaminiamo dapprima alcuni **principi di ingegneria del software**, frutto di decenni di esperienza nel settore, in quanto generalmente utili al conseguimento di prodotti di qualità

riconsidereremo quindi più in dettaglio il problema del progetto del processo produttivo, passando in rassegna i modelli più diffusi di **architettura del processo produttivo**

alcuni principi di ingegneria del software

principi risultanti dalla pratica di decenni di esperienza di costruzione di software:

rigore formale
separazione di aspetti diversi
modularità
astrazione
anticipazione del cambiamento
generalità
incrementalità

vedere le note della prima lezione di Ingegneria del software per una breve introduzione

architetture del processo produttivo

concetto di **ciclo di vita** del software:

modello di riferimento per il processo produttivo

schema di organizzazione delle attività di base (fasi) dello sviluppo produttivo

"filosofia" o modo di vedere e costruire il processo di sviluppo

tratti essenziali del processo di sviluppo:

suddivisione in **parti** (fasi, attività, etc.)

determinazione di **relazioni** fra dette parti

definizione di **modi di interazione** fra le parti stesse

questi sono i costituenti di ciò che intendiamo per **architettura del processo produttivo**

ne passiamo in rassegna i modelli più diffusi

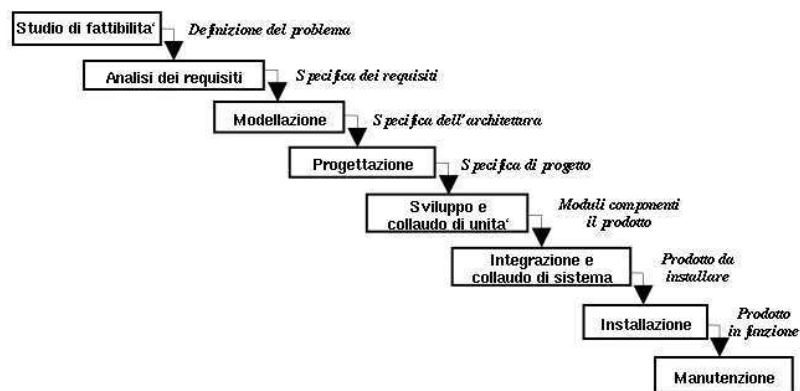
modello a cascata

sequenza di **fasi** che elaborano **semilavorati**

variabilità delle fasi e dei loro confini

possibili **ricicli** nel modello originario di Royce (1970)

pregi e limitazioni del modello



un esempio di modello a cascata

modelli incrementali

early subset, early delivery

realizzazione del prodotto per progressivi incrementi di funzionalità

vantaggi:

- economici

- feedback precoce da utenti o committenti

criteri di scelta delle priorità di realizzazione:

- dipendenze fra le funzionalità

- stabilità dei requisiti

- etc.

prototipazione rapida

throwaway prototype (prototipo usa-e-getta)

The management question [...] is not whether to build a pilot system and throw it away. You will do that. The only question is whether to plan in advance to build a throwaway, or to promise to deliver the throwaway to customers ...

Frederick P. Brooks, Jr., The Mythical Man-Month, Addison-Wesley (1975)

l'interfaccia di utente come prototipo

prototipazione evolutiva

modelli evolutivi

evoluzione dell'uso del prodotto

progettazione partecipativa

sviluppo incrementale con prototipi successivi

evoluzione delle tecnologie usate nel prodotto

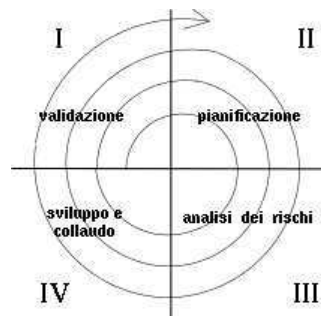
sviluppo per componenti specificati da interfacce

modularità

stratificazione

modelli trasformativi

modello a spirale



modello a spirale

tratti salienti:

iterazione

contrazione delle fasi di sviluppo

interazione con gli utenti

metamodello

riferimenti

Scollo (2006) :

Metodologie di progettazione del software

Note del corso di Ingegneria del software 1, Comiso (RG)