



Softversko inženjerstvo

Elektronski fakultet Niš

Verifikacija i
validacija (V&V)



Elektronski fakultet u Nišu



Ciljevi

- Uvesti pojmove verifikacije i validacije softvera i diskutovati razlike između njih
- Opisati proces inspekcije programa i njegovu ulogu u V&V



Elektronski fakultet u Nišu



Šta je verifikacija, a šta validacija?

- **Verifikacija**
 - Da li na pravi način gradimo proizvod?
 - Softver treba da bude usaglašen sa svojom specifikacijom
- **Validacija**
 - Da li gradimo pravi proizvod?
 - Softver treba da radi ono što korisnik stvarno traži



Elektronski fakultet u Nišu



Ciljevi V&V procesa

- Postoje dva glavna cilja
 - Otkrivanje defekata u sistemu
 - Procena da li je sistem upotrebljiv i koristan u realnim uslovima
- Verifikacija i validacija treba da utvrdi da softver odgovara nameni
 - To **NE ZNAČI** da je softver bez defekata
 - To **ZNAČI** da je softver dovoljno dobar za poslove kojima je namenjen

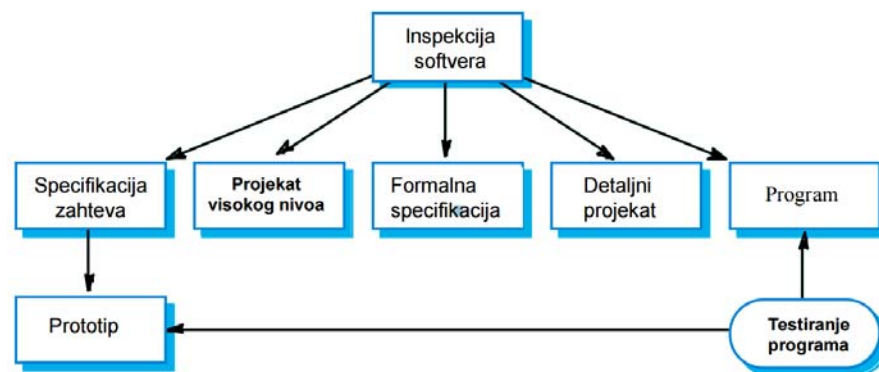
V&V poverenje

- Nivo poverenja zavisi od namene softvera, očekivanja korisnika i marketinškog okruženja
 - Funkcije softvera
 - Nivo poverenja zavisi od toga koliko je softver kritičan za organizaciju
 - Očekivanja korisnika
 - Korisnici mogu imati mala očekivanja od neke vrste softvera
 - Marketinško okruženje
 - Izneti proizvod ranije na tržište može biti važnije od nalaženja defekata u programu

Statička i dinamička verifikacija

- Inspekcija softvera
 - Odnosi se na analizu statičkih reprezentacija sistema da bi se otkrili problemi (statička verifikacija)
 - Mogu se koristiti alati za analizu koda i alati za pregledavanje dokumentacije koja je predmet inspekcije
- Testiranje softvera
 - Odnosi se na izvršenje i posmatranje ponašanja proizvoda (dinamička verifikacija)
 - Sistem se izvršava sa test podacima i posmatra se kako se ponaša u radu

Statička i dinamička V&V



Testiranje programa

- Može otkriti prisustvo grešaka, a NE njihovo odsustvo
- Jedina tehnika validacije nefunkcionalnih zahteva budući da se softver izvršava da bi se videlo kako se ponaša
- Može se koristiti zajedno sa statičkom verifikacijom da bi se u potpunosti pokrila V&V

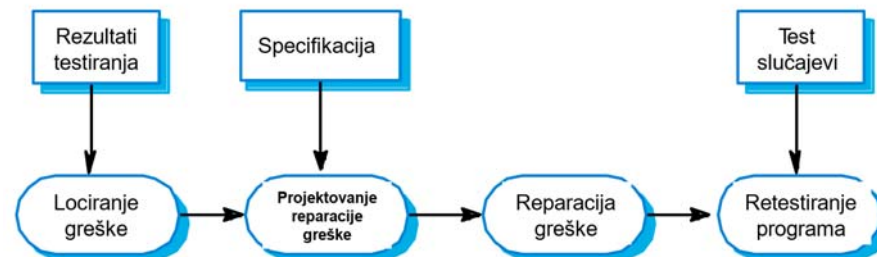
Tipovi testiranja

- Defektno testiranje
 - Testovi se projektuju da otkriju defekte u sistemu
 - Uspešan defekt test je onaj koji otkriva defekte u sistemu
- Validaciono testiranje
 - Cilj je pokazati da su ispunjeni zahtevi
 - Uspešan test je onaj koji pokazuje da su zahtevi implementirani na pravi način

Testiranje i debugiranje

- Defektno testiranje i debugging su različiti procesi
- V&V se bavi utvrđivanjem postojanja defekata u programu
- Debuging se bavi lociranjem i reparacijom ovih grešaka
- Debuging obuhvata formulisanje hipoteze o ponašanju programa, a zatim se testiranjem ove hipoteze nalaze greške

Proces debuginga



Planiranje verifikacije i validacije

- V&V je skup proces, stoga je neophodno planiranje
- Pažljivo planiranje zahteva mnogo toga što je van procesa inspekcije i testiranja
- Planiranje treba početi u ranim fazama procesa razvoja
- Plan treba da identifikuje balans između statičkog i dinamičkog prilaza verifikaciji i validaciji
- Planiranje treba da identifikuje standarde i procedure za inspekciju i testiranje, listu grešaka za inspekciju, i da definiše plan testiranja softvera



Inspekcija softvera

- Cilj je ispitivanje izvorne reprezentacije SW radi otkrivanja anomalija i defekata
- Inspekcija ne zahteva izvršenje SW tako da se može izvoditi pre njegove implementacije
- Može biti primenjena na bilo koju reprezentaciju SW (zahtevi, projekat, konfiguracioni podaci, test podaci, itd.)
- Pokazalo se da je vrlo efikasna tehnika za otkrivanje grešaka u programu



Uspešnost inspekcije

- Jednom inspekcijom se može otkriti veliki broj različitih defekata
 - Kod testiranja jedan defekt može maskirati drugi tako da je potrebno više izvršenja
- Pregledavači koriste domensko i programersko znanje tako da je velika verovatnoća otkrivanja grešaka
- Neka istraživanja govore da se
 - Inspekcijom može detektovati **>60%** grešaka
 - Najefikasnija primena je na slučajeve korišćenja



Inspekcija i testiranje

- Inspekcija i testiranje su komplementarne verifikacione tehnike
- Obe se koriste u V&V procesu
- Inspekcija **može** proveriti saglasnost sa specifikacijom, a ne sa korisničkim zahtevima
- Inspekcija **ne može** proveriti nefunkcionalne zahteve



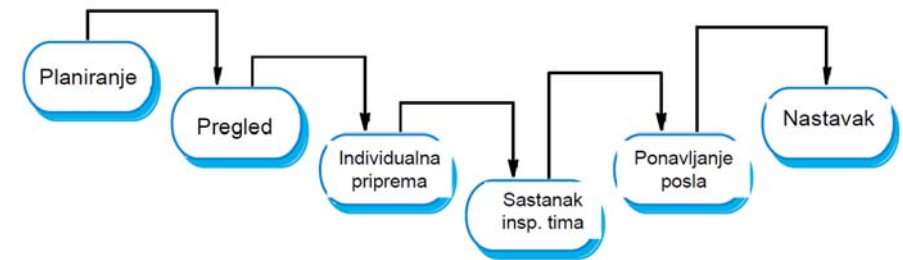
Inspekcija programa

- Formalizovani prilaz pregledavanju dokumenata
- Eksplicitno orijentisan **detekciji defekata** (ne korekciji)
- Defekti mogu biti logičke greške, anomalije u kodu ili nesaglasnost sa standardima

Preduslovi za inspekciju

- Mora biti na raspolaganju precizna specifikacija
- Članovi tima moraju biti upoznati sa standardima organizacije
- Mora biti na raspolaganju sintaksno korektan kod ili neka druga reprezentacija sistema
- Treba pripremiti listu grešaka prema kojoj će se vršiti inspekcija
- Menadžment mora prihvatiti da inspekcija povećava troškove
- Menadžment ne sme koristiti inspekciju za utvrđivanje ko od osoblja pravi propuste

Proces inspekcije



Procedura inspekcije

- Kod i prateća dokumenta se unapred distribuiraju inspeksijskom timu
- Inspeksijskom timu se prezentuje softver
- Vršiti se inspekcija (program se sistematski analizira) i otkrivene greške se beleže
- Nakon reparacije otkrivenih grešaka inspekcija se može ponoviti

Inspeksijski tim

- Inspekciju programa obavlja tim
- Prema Fagan-u tim je od **4** člana:
 - **Autor:** vrši prezentaciju programa
 - **Čitač:** glasno čita kod
 - **Tester:** vrši inspekciju koda iz perspektive testiranja
 - **Moderator:** organizuje proces
- Hewlett-Packard-ov razvojni proces predviđa inspeksijski tim od **6** članova:
 - Autor ili vlasnik
 - Inspektor
 - Čitač
 - Zapisničar
 - Moderator
 - Glavni moderator

Uloge 6-članova tima

- **Autor ili vlasnik:** Programer ili projektant koji je autor programa ili nekog dokumenta. Njegov zadatak je da locira i ukloni greške koje su inspekcijom otkrivene
- **Inspektor:** Pronalazi greške u programima ili dokumentima
- **Čitač:** Prezentuje kod ili dokument inspeksijskom timu
- **Zapisničar:** Vodi zapisnik u toku sastanka inspeksijskog tima
- **Moderator:** Upravlja procesom inspekcije i obezbeđuje uslove da se inspekcija obavi. Izveštava šefa moderatora o rezultatima inspekcije.
- **Šef moderator:** Odgovoran je za poboljšanje procesa inspekcije, ažurira listu grešaka, razvija standarde, itd.

Inspeksijska lista za proveru (1)

- Data faults
 - Are all program variables initialized before their values are used?
 - Have all constants been named?
 - Should the upper bound of arrays be equal to the size of the array or Size -1?
 - If character strings are used, is a delimiter explicitly assigned?
 - Is there any possibility of buffer overflow?
- Control faults
 - For each conditional statement, is the condition correct?
 - Is each loop certain to terminate?
 - Are compound statements correctly bracketed?
 - In case statements, are all possible cases accounted for?
 - If a break is required after each case in case statements, has it been included?
- Input/output faults
 - Are all input variables used?
 - Are all output variables assigned a value before they are output?
 - Can unexpected inputs cause corruption?

Inspeksijska lista za proveru (2)

- Interface faults
 - Do all function and method calls have the correct number of parameters?
 - Do formal and actual parameter types match?
 - Are the parameters in the right order?
 - If components access shared memory, do they have the same model of the shared memory structure?
- Storage management faults
 - If a linked structure is modified, have all links been correctly reassigned?
 - If dynamic storage is used, has space been allocated correctly?
 - Is space explicitly de-allocated after it is no longer required?
- Exception management faults
 - Have all possible error conditions been taken into account?

Brzina inspekcije

- 500 izvornih naredbi/čas može se prezentovati za vreme pregleda
- 125 izvornih naredbi/čas može se ispitati za vreme individualne pripreme
- 90-125 naredbi/času može se ispitati u toku jednog sastanka inspeksijskog tima
- Inspekcija je skup proces
- Inspekcija 500 linija košta oko 40 čovek-sati