Univerzitet „Džemal Bijedić“ Mostar

Fakultet informacijskih tehnologija

Dinamička verifikacija softvera

- Formalne metode -

Profesor: van. prof. dr Nina Bijedić Student: Edin Pinjić

**IZJAVA O AUTORSTVU**

Ja, **Edin (Kemal) Pinjić,** student Fakulteta informacijskih tehnologija, Univerziteta „Džemal Bijedić“ u Mostaru, pod punom moralnom, materijalnom i krivičnom odgovornošću,

**izjavljujem**

da je rad pod naslovom:

**„Dinamička verifikacija softvera“**

u potpunosti rezultat sopstvenog istraživanja, gdje su korišteni sadržaji (tekst, ilustracije, tabele itd.) drugih autora jasno označeni pozivanjem na izvor i ne narušavaju bilo čija vlasnička ili autorska prava.

Mostar, datum Edin Pinjić

Sadržaj

[1. Uvod 5](#_Toc41132982)

[2. Formalne metode 6](#_Toc41132983)

[2.1. Klasifikacija formalnih metoda 7](#_Toc41132984)

[2.2. Prednosti formalnih metoda 8](#_Toc41132985)

[2.3. Nedostaci formalnih metoda 8](#_Toc41132986)

[3. Dinamička verifikacija 9](#_Toc41132987)

[3.1. Jedinično testiranje 9](#_Toc41132988)

[3.2. Integracijsko testiranje 10](#_Toc41132989)

[4. Zaključak 11](#_Toc41132990)

[5. Literatura i reference 11](#_Toc41132991)

OVDJE IDE INDEKS SLIKA

# Uvod

Od samog početka kreiranja informacijskih sistema, pa sve do njegovog završetka nastaju greške koje su u tim fazama zasigurno neizbježne. Najčešći način provjere tih grešaka, u informacijskim sistemima, je upotreba testiranja i simulacije. Ipak ove tehnike ne mogu garantirati nepostojanje nedostataka u sistemu. Metod koji je mnogo više pouzdaniji po pitanju uočavanja i otklanjanja grešaka u sistemu jeste korištenje formalnih metoda tokom procesa razvoja informacijskih sistema, na primjer, pisanjem formalne specifikacije sistema na kojem se mogu dokazati različita svojstva i matematički dokazati da se implementacija sistema pridržava specifikacije. Cilj ovog završnog rada jeste prikazati dinamičku verifikaciju softvera upotrebom formalnih metoda, te prikazati šta su formalne metode i kako mogu smanjiti broj grešaka u sistemu. U pomenutim formalnim metodama postoje dvije vrste verifikacija, odnosno testiranja softvera, a to su dinamička i statička verifikacija. Statička verifikacija softvera je vrsta testiranja koje se izvršava kako bi se provjerili nedostaci u softveru bez izvršavanja samog softvera. Međutim, kod dinamičke verifikacije je obratno, tj. kôd softvera se pokreće i na taj način se otkrivaju anomalije istog. Treba napomenuti da je statičko ispitivanje, za razliku od dinamičkog mnogo jeftinije, a i greške ispitivanja su lakše uočljive i pogodnije za ispravljanje, jer vrši se u ranoj fazi razvoja samog softvera. Kada se govori o dinamičkoj verifikaciji, zavisno o pogledu testiranja, mogu se kategorizirati tri familije. Prva je „Unit testing“, tj. testiranje jedinki, gdje se vrši testiranje na malo, odnosno testira se samo jedna funkcija ili klasa. Moglo bi se reći da je ovaj način testiranja ujedno i najjednostavniji. Druga familija testiranja jeste testiranje na veliko u koje spadaju modul testiranje i integracijsko testiranje. U ovoj familiji se vrši testiranje grupa klasa, dakle ili jedan modul ili više modula. I treća familija testiranja jeste test prihvatljivosti koji je ustvari formalni test koji je definiran da provjerava prihvatljivosti kriterija samog softvera. U pomenutoj familiji pripadaju dva testiranja, a to su test funkcionalnosti i test nefunkcionalnosti. U ovom završnom radu će biti prikazana dinamička verifikacija korištenjem integracijskog testiranja nad već postojećim sistemom pod nazivom „Studentski servis“ u razvojnom okruženju Visual Studio 2019. Međutim, prije samog integracijskog testa, potrebno je uraditi i jedinično testiranje, što će se u daljem radu i prikazati.

# Formalne metode

Formalne metode su tehnike dizajniranja sistema koje koriste strogo određene matematičke tehnike i alate za specifikaciju, dizajn i verifikaciju softverskih i hardverskih sistema. Ovo znači da se specifikacija sastoji od dobro formiranih izjava koristeći matematičku logiku i da se formalna verifikacija sastoji od edukcija izvedenih iz te logike. Snaga formalnih metoda jeste da omogućavaju verifikaciju kompletnog prostora sistema i da dokazane osobine, koje stoje u sistemu, će stojati i za sve moguće ulaze. Kada se formalne metode ne mogu koristiti kroz čitavu fazu razvoja sistema, zbog kompleksnosti sistema, nedostatka alata ili nekih drugih razloga, one se i dalje mogu koristiti na dijelovima sistema, kao na primjer u dijelovima sistema koji su zaduženi za sigurnost kritičnih komponenti. Veliki broj različitih formalnih metoda je rezultat različitih metoda modeliranja i dokaznih pristupa potrebnih različitim domenama primjena. Također različite faze razvoja sistema mogu zahtijevati različite metode, tehnike ili alate. Iako je veliki broj razvijenih formalnih metoda rezultat istraživačkih napora na univerzitetima, sve je više formalnih metoda dostupnih izvan akademskih zajednica. Kada se novi sistem implementira obično je prvi korak pisanje specifikacije zahtjeva. Ta specifikacija treba da tačno opiše željeno ponašanje sistema te da bude kompletna i nedvoznačna, što može biti teško za izvesti. Nakon završetka specifikacije, programer, koji također razumije specifikaciju, prevodi istu u kod te ispravlja sve nejasne i dvoznačne dijelove. Programer koji piše kod može napraviti grešku u kodu, zatim sama veličina sistema, koja može biti tolika da je teško pratiti sve dijelove sistema koji moraju raditi prema uputama specifikacije. Nadalje, često se koristi više različitih timova u razvoju sistema, što također može biti izvor grešaka jer će svaki tim imati svoj način rada, svoju interpretaciju specifikacije zahtjeva i informacija dijeljenih tokom faze razvoja sistema. Tokom i nakon faze pisanja koda, obično se vrše testiranja sistema kako bi se utvrdilo da ispunjava postavljane uslove te da nema prisutnih grešaka, odnosno bug-ova. Testiranje velikih i složenih sistema može koštati mnogo vremena te zbog same veličine sistema i količine koda, iscrpno testiranje nije ostvarljivo. Uprkos tome, kada je u pitanju sistem, koji je sigurnosno kritičan, njegova ispravnost mora biti garantovana, što zahtjeva iscrpno testiranje ili način dokazivanja da je kod ispravno implementiran prema zadanoj specifikaciji. Koncept formalnih metoda nam predstavlja alate za matematičko opisivanje sistema ili dijelova sistema u specifikaciji i za dokazivanje da rezultirajući program zapravo ispunjava uslove zadane u specifikaciji. Formalna verifikacija je precizna i nema mogućnosti za pogrešnom interpretacijom. Naravno u praksi se ne može u potpunosti garantovati da implementacija nema grešaka jer same formalne metode mogu imati svoje mane ili čak može biti i greška u samom dokazu. Unatoč tome, povećano korištenje formalnih metoda i alata će rezultirati boljim implementacijama i pouzdanijim metodama i alatima. Ograničenje formalnih metoda je to što mogu samo biti korištene za dokazivanje ispravnosti sistema prema specifikaciji. Stoga, samo zato što je implementacija matematički dokazana da prati pravila specifikacije, to ne znači da je specifikacija sama po sebi ispravna i bez grešaka. Bez obzira, osobine i dalje mogu biti dokazane kako bi se pojačalo uvjerenje da specifikacija tačno predstavlja željene funkcionalnosti.

Ukratko, korištenjem formalnih metoda mogu se pronaći greške u ranim fazama razvoja sistema te se neke klase grešaka mogu skoro u potpunosti ukloniti.

## Klasifikacija formalnih metoda

Postoji nekoliko različitih klasifikacija formalnih metoda ali generalno gledajući formalne metode se koriste u dva aspekta:

• Da bi se primijenilo željeno ponašanje sistema prema specifikaciji. Specifikacija je model sistema koji opisuje kako se sistema mora ponašati, a formalne metode se koriste za validaciju metode.

• Da potvrdi da implementacija ima isto ponašanje kao što je navedeno u specifikaciji ili da dobavi implementaciju koja ima isto ponašanje kao i specifikacija. Ovdje se govori o formalnim vezama implementacije i specifikacije.

Još jedna generalna klasifikacija formalnih metoda može biti prema tome kako je model sistema opisan:

• Kao tranzicija sistema sa stanjima, tranzicija i stanje transformacije ili

• Kao neka programska logika sa pre (prije)- i post (poslije)- uslovima kao i sa aksiomima i pravilima zaključka

Treći način klasifikacije formalnih metoda je:

• Formalne metode koje se koriste za specificiranje i analizu specifikacije.

• Formalne metode koje se koriste za specificiranje i dokazivanje osobina specifikacije (formalna verifikacija).

• Formalne metode koje se koriste za specificiranje i izvođenje implementacije iz specifikacije.

• Formalne metode koje se koriste za specificiranje i transformaciju specifikacije, transformacije koje ili sakrivaju detalje specifikacije ili obogaćuju specifikaciju sa više detalje.

Još jedan način klasifikacije i posljednji u ovom radu o kojem će se govoriti je na osnovu nivoa korištenja formalnih metoda:

• Nivo 0: Kada se formalne metode koriste samo za opisivanje željene funkcije i za usmjeravanje razvoja.

• Nivo 1: Kada se formalne metode koriste za provjeru funkcija.

• Nivo 2: Kada se formalne metode koriste za provjeravanje cijelog sistema kroz sve funkcije.

## Prednosti formalnih metoda

Formalne metode su dobar način otkrivanja pogrešaka u specifikaciji, utvrđivanju tačnosti sistema i predstavljanju sistem na nedvosmislen način. Upotreba ovakve metode može smanjiti troškove ukoliko se koristi na nekim manjim, ali kritičnim dijelovima sistema za koje je bitno da su precizni, bez grešaka. Neke prednosti korištenja formalnih metoda su sljedeće:

• bolji uvid u zahtjeve, otklanjanje nesporazuma, smanjenje mogućnosti grešaka (što sve pridonosi pouzdanosti softvera);

• analiziranje matematičkim metodama (potpunost, konzistentnost);

• može služiti kao podloga za formalnu verifikaciju implementiranog sistema;

• mogućnost „animacije“ specifikacije u svrhu prototipiranja;

## Nedostaci formalnih metoda

Kao i sve drugo, ni pomenuta metoda nije bez mana. Unatoč svim gore navedenim prednostima, formalne metode ograničene su u praktičnom razvoju softvera, kako za veće sustave tako i za kritične dijelove sustava. Stoga je i malo stručnjaka koji imaju iskustva u razvoju ovakvom metodom. Razlozi za nekorištenje formalne metode su sljedeći:

• nerazumljiva je korisnicima i menadžmentu (korisnicima je teže provjeriti ispunjava li specifikacija njihove zahtjeve);

• zahtjeva posebno osposobljene softverske inženjere;

• nije pogodna za interaktivne sustave i sučelja;

• nije skalabilna, za veće sustave količina posla postane prevelika;

• nije kompatibilna s agilnom metodom razvoja softvera;

# Dinamička verifikacija

## 3.1. Jedinično testiranje

## 3.2. Integracijsko testiranje

# Zaključak

# Literatura i reference