

# YUINFO 2018

## ZBORNİK RADOVA

**YU** | **20**  
**INFO** | **18**

24<sup>TH</sup> CONFERENCE AND EXHIBITION  
Kopaonik



**YU INFO 2018**  
**ZBORNIK RADOVA**

Izdavač:

**Društvo za informacione sisteme i računarske mreže**

Urednik:

**Prof. dr Miodrag Ivković**

Mesto i godina izdanja:

**Beograd, 2018.**

ISBN:

**978-86-85525-21-6**



## **YU INFO 2018**

### **PROGRAMSKI ODBOR**

- Prof. dr Borko Furht, Florida Atlantic University, USA
- Prof. dr Božidar Radenković, FON, Univerzitet u Beogradu
- Prof. dr Branko Milosavljević, FTN, Univerzitet u Novom Sadu
- Prof. dr Bratislav Milovanović, Elektronski fakultet, Univerzitet u Nišu
- Prof. dr Branko Markoski, Tehnički fakultet Mihajlo Pupin, Zrenjanin
- Prof. dr Dragan Domazet, FIT, Univerzitet Metropliten, Beograd
- mr Dušan Korunović, Informaciono društvo Srbije
- Prof. dr Dušan Surla, PMF, Univerzitet u Novom Sadu
- Prof. dr Đorđe Paunović, ETF, Univerzitet u Beogradu
- Prof. dr Gyula Mester, Univerzitet u Segedinu
- Prof. dr Irina Branović, Univerzitet Singidunum, Beograd
- Dr Ivan Vulić, Vojska Srbije
- Prof. dr Jelica Protić, ETF, Univerzitet u Beogradu
- Prof. dr Ljerka Luić, Sveučilište u Zagrebu, Hrvatska
- Dr Marija Boban, Pravni fakultet, Sveučilište u Splitu
- Prof. dr Miodrag Ivković, Tehnički fakultet Mihajlo Pupin, Zrenjanin
- Prof. dr Miodrag Zivković, Matematički fakultet, Beograd
- Prof. dr Milija Suknović, FON, Univerzitet u Beogradu
- Prof. dr Mirjana Pejić Bach, Ekonomski Fakultet Sveučilišta u Zagrebu, Hrvatska
- Prof. dr Miroslav Trajanović, Mašinski fakultet, Univerzitet u Nišu
- Prof. dr Nataša Gospić, Saobraćajni fakultet, Univerzitet u Beogradu
- Prof. dr Sašo Josimovski, Ekonomski fakultet, Univerzitet St. Kiril i Metodij, Skoplje
- Prof. dr Sašo Tomažič, Faculty of Electrical Engineering, Ljubljana
- Doc. dr Siniša Nešković, FON, Univerzitet u Beogradu
- Prof. dr Slobodan Janković, Tehnički fakultet Mihajlo Pupin, Zrenjanin
- Prof. dr Leonid Stoimenov, Elektronski fakultet, Univerzitet u Nišu

- Prof. dr Veljko Milutinović, ETF, Univerzitet u Beogradu
- Prof. dr Zora Konjović, FTN, Univerzitet u Novi Sadu
- Prof. dr Zoran Jovanović, ETF, Univerzitet u Beogradu
- Prof. dr Zoran Stanković, Elektronski fakultet, Univerzitet u Nišu
- Prof. dr Vladimir Filipović, Matematički fakultet, Beograd
- Prof. dr Zlatko Čović, VTŠ, Subotica
- Doc. dr Komlen Lalović, ITS, Fakultet za primenjeni menadžment, ekonomiju i finansije – Beograd

Chairman konferencije:

- Prof. dr Miodrag Ivković

## SADRŽAJ

### E-DRUŠTVO, ZAŠTITA I SIGURNOST PODATAKA

PRIMENA SOFISTICIRANIH METODA ZA KRIPTOVANJE I DEKRIPTOVANJE PODATAKA **1**  
Saša Vulović, Slobodan Aleksandrov

IZAZOVI KOORDINACIJE SAJBER BEZBEDNOSTI U REPUBLICI SRBIJI U USLOVIMA  
KRIZNIH SITUACIJA **7**  
Goran Matić, Milan Miljković

PRIPREME ZA SOA UPRAVLJANJE U ODS "EPS DISTRIBUCIJA" **12**  
Miloš Kostić, Dejana Stefanović-Kostić, Aleksandra Tomić

UPOREDNA ANALIZA GRAPHQL I RESTFUL NAČINA IMPLEMENTACIJE VEB SERVISA **14**  
Miloš Zlatković

TEHNIKE ZAŠTITE ANDROID APLIKACIJA I KODA OD OBRNUTOG INŽENJERINGA **20**  
Petar Ljubić, Bratislav Predić, Miloš Roganović

IMPLEMENTACIONI DETALJI ALGORITMA ŠIFROVANJA CRYPTO1 **26**  
Marko Mićović, Uroš Radenković, Vladimir Jocović

PRIMENA WEB APLIKACIJE ZA OBRADU PODATAKA SA DRUŠTVENE MREŽE TWITTER  
ZA ANALIZU TURISTIČKIH POTENCIJALA – STUDIJA SLUČAJA: SMEDEREVSKA I **31**  
GOLUBAČKA TVRĐAVA  
Nikola Džaković, Nikola Dinkić, Jugoslav Joković, Leonid Stoimenov, Aleksandra Djukić

C2C MODELI ELEKTRONSKOG POSLOVANJA: PRIMER PORTALA ZA PRONALAZENJE  
PASA **35**  
Katarina Đorđević, Tamara Naumović, Lazar Živojinović, Marijana Despotović-Zrakić

UNAPREĐENJE RADA APOTEKE PRIMENOM B2C I G2B FORMI E-POSLOVANJA **39**  
Aleksandar Barbul, Tatjana Stojadinovic, Miodrag Brzaković

POBOLJŠANJE SPREMNOSTI DRŽAVNIH ORGANA REPUBLIKE SRBIJE ZA ODGOVOR NA  
SAJBER NAPADE **44**  
Marko Krstić, Dušan Raičević

DIGITALNA TRANSFORMACIJA POSLOVANJA **48**  
Predrag Matković, Mirjana Marić, Pere Tumbas, Jovica Đurković

### RAČUNARSKE PRIMENE, RAZVOJ SOFTVERA I ALATI

ACHIEVING INTEROPERABILITY IN EUROPEAN ELECTRONIC TOLL COLLECTION  
SYSTEMS (EETCS) BASED ON AUTOMATIC LICENSE PLATE RECOGNITION (ALPR) **53**  
Ivanović Miloš

AUTONOMNI SAMOVOZEĆI AUTOMOBILI Gyula Mester	59
KOEFICIJENT RAZLIČITOSTI ZA REŠAVANJE PROBLEMA FORMIRANJA PROIZVODNIH ĆELIJA Miloš Danilović, Oliver Ilić	63
OBELODANJIVANJE FINANSIJSKIH INFORMACIJA JAVNOG SEKTORA NA INTERNETU Kristina Mijić	69
NEKE OD PRIMENA BESPILOTNIH LETELICA U ŠUMARSTVU I ZAŠTITI ŽIVOTNE SREDINE Dejan Pavlović	74
UPRAVLJANJE PROMENAMA U DINAMIČNOM OKRUŽENJU Miroslav Stefanović, Sanja Maksimović	80
KVANTIFIKOVANJE RELEVANTNOSTI PREDIKTORA, PREDIKTIVNOG MODELA ODRŽAVANJA AVIONSKOG MOTORA Olivera Janković, Đorđe Babić	83
IDENTIFIKACIONI SISTEM ZA PREPOZNAVANJE DUZICE OKA ZASNOVAN NA UPOTREBI VISTAF2 BIOCAM Nedjeljko Lekić	89
METOD MERENJA FAKTORA SNAGE IMPLEMENTIRAN U VATMETRU VISOKE KLASSE TAČNOSTI Ljubiša Jovanović	95
RIZICI KORIŠĆENJA ANDROID APLIKACIJA Mirko Kosanović, Miloš Kosanović, Vesna Kosanović	98
KORIŠĆENJE ARCGIS I HEC-RAS PROGRAMSKIH PAKETA ZA DEFINISANJE PLAVNIH ZONA Boris Krunić, Nevena Cvijanović	104
ADVANCED PROFILING FOR DSP APPLICATIONS Nives Kaprocki, Jelena Kovačević, Nenad Pekez	107
KONFIGURABILNE ARITMETIČKO LOGIČKE JEDINICE REALIZOVANE KORIŠĆENJEM PROTOČNE OBRADNE Filip Hadžić, Zaharije Radivojević, Marko Mićović, Uroš Radenković	111
RADNI OKVIR ZA AUTOMATIZOVANO MODELOVANJE PODATAKA Maja Milić, Petar Bjeljaj, Marjan Maruna, Vladimir Maruna	117
<b>RAČUNARSKE MREŽE I TELEKOMUNIKACIJE, VEŠTAČKA INTELIGENCIJA I SIMULACIJA</b>	
REGULATORNI IZAZOVI U PROCESU UVOĐENJA M2M/IOT USLUGA Zoran Janković, Milosav Grubović	123

CENTRALIZOVANA DETEKCIJA NEISPRAVNIH VEZA U MEŠOVITOJ TELEFONSKOJ MREŽI Vladimir Matić, Aleksandar Lebl, Dragan Mitić, Žarko Markov	128
UTICAJ NEIDEALNE ESTIMACIJE KANALA NA PERFORMANSE CELULARNOG POKRIVANJA PREKO UAV-OVA Uglješa Urošević, Zoran Veljović	134
SINGLE RAN U MREŽI "TELEKOM SRBIJA" PODRUČJE KOPAONIKA Danijela Aleksić, Saša Gavrić, Nemanja Protić, Miljana Milić	138
SIMULACIONI MODEL ORGANIZACIJE PREVOZA GRAĐEVINSKOG MATERIJALA NA PLOVNIM PUTEVIMA Katarina Milović, Danijela Pjevčević, Vladislav Maraš, Aleksandar Radonjić	142
BEŽIČNO UPRAVLJANJE MOBILNOG ROBOTA POMOĆU WI-FI MREŽE PUTEM RASPERRY PI3 UREĐAJA Filip Ilić, Đorđe Nisić, Dušan Đorić	147
SOFTVERSKI SISTEM ZASNOVAN NA BIOFEEDBACK METODI Milana Prodanov , Marija Punt, Nadica Miljković, Sanja Delčev	152
PREGLED KORIŠĆENJA INTELIGENTNIH ŽELEZNIČKIH SISTEMA Dragica Jovanović, Marko Bursać, Zoran Bundalo	157
SOFTVERSKA INTEGRACIJA CFP MODULA U NMS SISTEM SUNCE-O ZA OTN/DWDM PLATFORMU OTP100G IRITEL Marko Radivojević, Petar Knežević, Branislav Tomić, Mihailo Stanić, Dejan Drajić	163
IMPLEMENTACIJA SISTEMA ZA PRIKUPLJANJE PODATAKA, GENERISANJE KLASTERA I PREPORUKA POMOĆU MAŠINSKOG UČENJA Dražen Drašković, Nemanja Kojić, Marko Mićović, Uroš Radenković	167
<b>RAČUNARSKE PRIMENE U VOJSCI</b>	
KOMPARATIVNA ANALIZA KOMPLEKSNIH UPITA NAD BAZOM PODATAKA I SKLADIŠTEM PODATAKA Atanasijević Jordan, Stanković Nevena	173
GRADIJENTNA METODA ZA PROCENU USPEŠNOSTI SJEDINJAVANJA KOLOR I MONOHROMATSKIH SLIKA Rade Pavlović, Vladimir Petrović	179
ANALIZA PERFORMANSI PID REGULATORA SA FILTRIMA ŠUMA MERENJA Nikola Savkić, Momir Stanković, Stojadin Manojlović	184
INFORMACIONI SISTEM ZA VOĐENJE EVIDENCIJE POKRETNIH STVARI Stefan Đurić, Petar Lukić, Ivan Tot	189
UPOTREBA RAZVIJENIH MIDDLEWARE U ARHITEKTURI IOT Ivan Tot, Dušan Bogičević, Komlen Lalović	192

ODREĐIVANJE GPS KOORDINATA, SLANJE NMEA REČENICE PUTEM GPRS I PRIKAZ LOKACIJE NA MAPI Lazar Stevanović, Lazar Đorđević, Stefan Đurić	<b>196</b>
ADD-IN ZA SELEKTIVNO ŠIFROVANJE TEKSTA U OKVIRU MICROSOFT WORD DOKUMENTA Jovana Mihailov, Boriša Jovanović, Boban Mihailov	<b>199</b>
ANALYSIS AND IMPLEMENTATION OF AES CRYPTOGRAPHIC ALGORITHM ON CUDA GRAPHIC PROCESSING UNITS Boriša Jovanović, Ivan Tot, Slavko Gajin	<b>204</b>
ELASTICSEARCH KLASER I INDEKSIRANJE FAJLOVA Zoran Denda, Željana Vučetić	<b>210</b>
PROCENA SLIČNOSTI DOKUMENATA KOMBINACIJOM RAZLIČITIH METODA EKSTRAKCIJE TEMA IZ TEKSTA Željana Vučetić, Zoran Denda	<b>214</b>
VIRTUELNE SIMULACIJE U VOJNOM OBRAZOVANJU Goran Šimić, Tamara Gajić, Stefan Vukadinović	<b>220</b>
IMPLEMENTACIJA I VERIFIKACIJA AES ALGORITMA NA ATMEGA32 MIKROKONTROLERU Stefan Sretenović, Stefan Božanić, Dejan Kršljanin, Radomir Prodanović, Vladimir Kekić	<b>226</b>
POVEZIVANJE ANDROID APLIKACIJE SA ARDUINO-OM UPOTREBOM MQTT PROTOKOLA Stefan Božanić, Mladen AntoniĆ, Stefan Sretenović, Vladimir Kekić	<b>230</b>
MODELOVANJE PROCESA SAMOVOĐENJA RAKETA U MATLAB-SIMULINK PROGRAMSKOM OKRUŽENJU Vladimir Kekić, Filip Nikolić, Stefan Božanić, Stefan Sretenović	<b>234</b>
MIKROSEGMENTACIJA U CLOUD-U Vladimir Dobrosavljević, Mladen Veinović, Mladen Trikoš	<b>239</b>
SISTEM IDENTIFIKACIJE SLEDEĆE GENERACIJE Mladen Trikoš, Vladimir Dobrosavljević, Dejan Simić, Dejan Savić	<b>242</b>
FLEKSIBILNOST: KLJUČNI FAKTOR UPOTREBLJIVOSTI WEB APLIKACIJA Nebojša Đorđević, Dejan Rančić, Olivera Pronić-Rančić, Uwe Siart	<b>245</b>
PRIMENA LABVIEW-A U PROCENI OBELEŽJA POKRETNOG CILJA U SISTEMU SA JEDNIM INFRACRVENIM VIDEO SENZOROM Davorin Mikluc, Milenko Andrić, Boban Bonžulić, Srđan Mitrović	<b>250</b>
OBJEKTIVNA PROCENA KVALITETA SLIKA SA VIŠESTRUKIM DISTORZIJAMA Nenad Stojanović, Boban Bondžulić, Vladimir Petrović, Davorin Mikluc	<b>256</b>
ZNAČAJ UPRAVLJANJA DOKUMENTIMA U MO I VS I DOSTIGNUTI STEPEN RAZVOJA Dejan Milenković, Dejan Kršljanin	<b>262</b>



ANALIZA MOGUĆNOSTI PRIMENE KROS-KORELACIJE U VERIFIKACIJI KORISNIKA NA OSNOVU OTISKA PRSTA Lazar Đorđević, Lazar Stevanović, Boban Bondžulić, Ivan Tot, Mladen Trikoš	<b>266</b>
DIGITALNA KONTROLA BRZINE JEDNOSMERNOG MOTORA PRIMENOM TIRISTORA I SOFTVERA LABVIEW Milinko Srećković, Davorin Mikluc	<b>272</b>
OBJEKTIVNA PROCENA KVALITETA VIDEO SEKVENCI SA PAKETSKIM GUBICIMA Marko Novičić, Boban Bondžulić, Boban Pavlović, Jovan Bajčetić, Ivan Tot	<b>278</b>
ANALIZA EFEKATA KONAČNE DUŽINE DIGITALNE REČI PRI IMPLEMENTACIJI IIR FILTERA Filip Mladenović, Boban Bondžulić, Milenko Andrić, Davorin Mikluc	<b>284</b>
UTICAJ WRED MEHANIZMA NA KVALITET SERVISA U PAKETSKIM MREŽAMA Katarina Manojlović, Boban Pavlović	<b>290</b>
PRISTUP SPECIFIKACIJI ZAHTEVA ZA RAZVOJ SISTEMA "FAKTURISANA REALIZACIJA U ZDRAVSTVENOJ ZAŠTITI" Rajko Terzić, Milosav Majstorović	<b>294</b>
INFORMACIONI SISTEM USTAVNOG SUDA SRBIJE Đuro Klipa, Radovan Bezbradica, Rade Dragović	<b>301</b>
PRIMENA GIS ALATA U KARTIRANJU RIZIKA OD POPLAVA Nevena Cvijanović, Boris Krunić, Vojislav Antonić	<b>307</b>

# PRIMENA SOFISTICIRANIH METODA ZA KRIPTOVANJE I DEKRIPTOVANJE PODATAKA

## APPLICATION OF SOPHISTICATED METHODS FOR ENCRYPTING AND DECRYPTING DATA

Saša Vulović<sup>1</sup>, Slobodan Aleksandrov<sup>2</sup>

*Webelinx, Niš<sup>1</sup>*

*Visoka tehnička mašinska škola strukovnih studija Trstenik<sup>2</sup>*

**Sadržaj** – Razvojem nauke i tehnologije, a posebno ekspanzijom Interneta i njegovih servisa, potreba za sigurnijim prenosom podataka dobija najviši prioritet u računarskim sistemima. Bez obzira na prenosni medijum u razmeni podataka, postoji mogućnost presretanja ili čak izmene originalne informacije. Jedan od načina zaštite poruke je primena kriptografije u cilju povećanja bezbednosti kod prenosa informacija. U ovom radu dat je pregled savremenih kriptografskih metoda. Razvijena je aplikacija za kriptovanje i dekriptovanje podataka bazirana na blok šifrotorima i DES algoritmu.

**Abstract** - With the development of science and technology, and in particular the expansion of the Internet and its services, the need for more secure data transfers is becoming the highest priority in computer systems. Regardless of the transfer medium in the data exchange, there is the possibility of intercepting or even altering the original information. One way to protect the data is the application of cryptography in order to increase the security of information transmission. This paper presents an overview of modern cryptographic methods. An application for encryption and decryption of data based on block ciphers and DES algorithm has been developed.

### [1] UVOD

Uparedo sa razvojem i implementacijom globalnih računarskih mreža, razvijaju se i različiti mehanizmi zaštite specijalizovanih za odbranu od pojedinih vrsta napada. Računarske mreže, pored toga što omogućavaju izuzetno povećanje efikasnosti rada i smanjenje troškova, predstavljaju kritičnu tačku bezbednosti date organizacije sa stanovništva bezbednosti računarskih sistema. Metode za zaštitu podataka postajale sve složenije i naprednije. U savremenom informacionom društvu kriptologija ima ključnu ulogu za bezbedan prenos podataka. Kriptografija i kriptanaliza proučavaju metode za šifrovanje, prenos i dešifrovanje informacija. Kriptografija je veoma široka oblast, a u praksi se bazira na upotrebi kripto-sistema koji se sastoje od algoritama za kriptovanje, jednog ili više ključeva, sistema za upravljanje ključevima, podataka u vidu standardnog i kriptovanog teksta. Na složenost dodatno ukazuju i činjenice da se kripto-sistemi mogu realizovati hardverski, softverski ili hardversko-softverski, kao i to da se prilikom realizacije moraju zadovoljiti osnovni sigurnosni servisi. Za realizaciju kriptografskih algoritma, koji su danas u upotrebi, koriste se složeni matematički izrazi kao i znanja iz elektronike i programiranja. Uprkos tome, napredak u postojećim kriptografskim algoritmima

nastavlja se rastućim tempom, da bi zadovoljio potrebe širenja informatičko-tehnološkog društva u kome živimo. Teško je zamisliti ozbiljnu računarsku aplikaciju koja u sebi nema implementiran neki sigurnosni algoritam, počev od bankarskih aplikacija, internet trgovine, pa sve do operativnih sistema. Kod prenosa podataka pošiljalac transformiše podatke koristeći unapred dogovoreni ključ. Taj postupak naziva se šifriranje ili kriptovanje, a dobijeni rezultat je šifrat (*eng. ciphertext*). Sledeći korak je slanje šifrata preko nekog komunikacijskog kanala. Presretač može prisluškivanjem da dođe do kriptovanog teksta, ali bez ključa ti podaci su neupotrebljivi. Primalac kome su namenjeni podaci pomoću prethodno dogovorenog ključa može dekriptovati i koristiti originalne podatke.

Savremene metode kriptovanja zasnivaju se na upotrebi ključa. U zavisnosti od načina korišćenja ključa, razvijeni su simetrični i asimetrični algoritmi kodiranja. Osnovna razlika je u tome da simetrični algoritmi koriste isti ključ za kriptovanje i dekriptovanje neke poruke, dok asimetrični algoritmi koriste različite ključeve za kriptovanje i dekriptovanje iste poruke. Simetrični algoritmi imaju dve grupe: šifrotori toka i blok šifrotor. Kod šifrotora toka kriptovanje se vrši bit po bit, dok se kod blok šifrotora kriptovanje vrši po blokovima podataka. Dekriptovanje se najčešće vrši inverznim kriptovanjem, odnosno algoritam je isti, ali se podključevi kriptovanja koriste obrnutim redosledom. Asimetrični algoritmi poznati su kao algoritmi sa javnim ključem (*eng. public-key algorithms*). Razlog za ovaj naziv je taj što je dozvoljeno da se jedan od ključeva potreban za kriptovanje/dekriptovanje objavi javno. Ono što je specifično za ovaj tip algoritma je to da se koriste dva ključa za kriptovanje, odnosno dekriptovanje poruke. Princip je sledeći: osoba A objavi svoj javni ključ preko nekog medija. Osoba B, koja želi da osobi A pošalje tajnu poruku, najpre vrši kriptovanje svoje poruke ključem koju je korisnik A javno objavio, a zatim tu kriptovanu poruku šalje. Jedino osoba A sa svojim privatnim (tajnim) ključem može dekriptovati ovu poruku.

Simetrični algoritmi su po svojoj prirodi brži jer se njihova implementacija na računaru brže odvija od implementacije asimetričnih algoritama. Međutim, zbog prednosti koje poseduju asimetrični algoritmi u praksi se koriste obe vrste algoritama, koje se mogu kombinovati u cilju bolje zaštite poruka. Obično se asimetrični algoritmi koriste za kriptovanje slučajno generisanog broja koji služi kao ključ za kriptovanje originalne poruke metodama simetričnih algoritama.

## [2] REŽIM RADA BLOK ŠIFRATORA

Blok šifrotori vrše kriptovanje odnosno dekriptovanje tako što obrađuju podatke blok po blok. U zavisnosti od algoritma blokovi su različite veličine, na primer za RC5 koriste se 2 bloka od po 32 bita, za DES (*eng. Data Encryption Standard*) i 3DES koristi se jedan blok od 64 bita, dok se kod AES (*eng. Advanced Encryption Standard*) koristi takođe po jedan blok ali od 128 bita [2]. Da bi se povećala sigurnost definisani su određeni režimi rada koji se implementiraju sa algoritmima. Ovi režimi mogu da se koriste sa bilo kojim blok šifrotorom. U okviru razvoja aplikacije implementiran je CBC režim rada sa DES blok šifrotorom.

ECB (*eng. The Electronic Codebook Mode*) originalni tekst deli se na blokove odgovarajuće veličine i nakon toga svi blokovi se kriptuju istim ključem. Upravo zbog ove osobine ovaj režim rada nije dovoljno siguran, zbog korišćenja istog ključa identični originalni blokovi nakon kriptovanja postaću identični kriptovani blokovi. Zbog toga ECB režim nije pogodan za dugačke poruke. Ako se prisluškuju poruke i zna se da poruka počinje unapred definisanim poljima napadač će moći posle određenog broj poruka da otkrije o kojoj se šifri radi.

CBC (*eng. Cipher Block Chaining*) - režim ulančanih blokova je sigurniji od ECB režima zato što je kod CBC režima ulaz u algoritam rezultat logičke operacije „ekskluzivno ILI“ (XOR operacija) između tekućeg bloka za kriptovanje i predhodno kriptovanog bloka. Na ovaj način postiže se da se blokovi modifikuju pre samog procesa kriptovanja i samim tim isti blokovi originalnog teksta neće se kritovati u iste blokove kriptovanog teksta.

CFB (*eng. Cipher Feedback*) - režim šifrovanja sa povratnom spregom je sličan režimu ulančanih blokova. Ulaz u algoritam za kriptovanje je vrednost veličine  $b$  bitova koja se naziva i vektor inicijalizacije. Izlaz iz ove funkcije smešta se u poseban registar. Najznačajnijih  $s$  bitova vrednosti koja se nalazi u registru se XOR-uje sa prvim blokom otvorenog teksta  $P_1$  pri čemu se dobija prvi blok kriptovanog teksta  $C_1$ , koji se zatim prenosi. Nakon toga sadržaj registra se pomera za  $s$  bitova u levo, a  $C_1$  se postavlja na mesto najmanje značajnih bitova vrednosti koja se nalazi u registru. Ovaj proces se ponavlja do kraja kriptovanja. Proces dekriptovanja se obavlja na sličan način, samo u obrnutom redosledu.

OFB (*eng. Output Feedback*) režim rada je sličan režimu šifrovanja sa povratnom spregom. Vektor inicijalizacije ( $IV$ ) se kriptuje odgovarajućim algoritmom. Izlaz nakon kriptovanja se XOR-uje sa prvim blokom originalnog teksta čime se dobija prvi blok šifriranog teksta, ali se isti taj blok dalje koristi u novoj fazi kriptovanja. Ovaj postupak se ponavlja sve dok se ceo tekst ne šifrira.

U svim navedenim režimima rada, osim kod ECB-a, u procesu kriptovanja, odnosno dekriptovanja  $i$ -ta faza ne može da počne dok se  $i-1$  ne završi. Blokovi su međusobno povezani i samim tim nije moguće izvršiti paralelno izračunavanje [2]. Jedan od režima rada u kome

je moguće paralelizovati kriptovanje odnosno dekriptovanje podataka je CTR (*eng. Counter mod*). Kod ovog režima koristi se poseban brojač koji mora da generiše različite vrednosti za svaki blok poruke koja se kriptuje. Uglavnom taj brojač se postavlja na neku vrednost  $a$  onda se samo inkrementira. Vrednost brojača se kriptuje određenim algoritmom, a onda se izlaz iz algoritma XOR-uje sa trenutnim blokom originalnog teksta, što znači da nema ulančavanja. Na isti način vrši se i proces dekriptovanja.

CBC režim rada enkripcije razvio je IBM 1976 godine. Suština CBC režima rada je XOR operacija koja se primenjuje nad rezultatom iz predhodnog bloka koji je prošao kroz fazu kriptovanja i narednog bloka koji tek treba da prođe kroz tu fazu. Kao rezultat dobija se kriptovani podatak. Ovaj način kriptovanja podrazumeva da postoje zavisnosti između susednih blokova tako da nije moguće izvršiti paralelizaciju proces kriptovanja ili dekriptovanja. Prvi blok nema predhodnika sa kojim bi vršio XOR operaciju tako da se kod njega koristi vektor inicijalizacije koji se naziva i  $IV$ . Vrednost  $IV$  mora biti iste veličine kao i blok koji se kriptuje kako bi XOR mogao uspešno da se izvrši. Dekripcija se obavlja na identičan način, ali u suprotnom smeru.

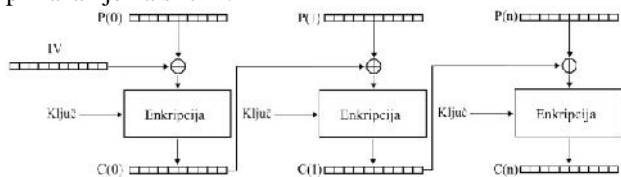
## [3] KRIPTOVANJE I DEKRIPTOVANJE

Vektor inicijalizacije ( $IV$ ) je proizvoljan broj koji može da se koristi sa tajnim ključem kao sredstvo za kriptovanje podataka. Ukoliko se ista vrednost koristi za različite poruke onda se ona naziva vektor inicijalizacije, a ako se za svaku poruku koristi različita vrednost onda se ona naziva *nonce*. Korišćenje  $IV$  vrednosti sprečava ponavljanje u procesu kriptovanja podataka i otežava napadaču da otkrije poruku, naročito ako se radi o napadu korišćenjem rečnika. Na primer, u sekvenci poruka koje se kriptuju mogu se naći dve ili više identičnih poruka. Sve identične poruke ukoliko se ne koristi  $IV$  vrednost kriptovaće se na isti način. Ako postoji ponavljanje u kriptovanim porukama napadač može da pretpostavi da su određene poruke zapravo identične. Upravo  $IV$  vrednost sprečava ovu pojavu i omogućava da iste poruke daju različite kriptovane poruke. Idealan vektor inicijalizacije je slučajno izabran broj koji je poznat i odredišnoj strani kako bi primalac poruke mogao da je dešifrira. Vektor inicijalizacije može biti unapred definisan, može da se pošalje nezavisno, da postoji treća strana koja će dodeliti ovu vrednost i pošiljaocu i primaocu poruke, a može se i nadovezati na samu kriptovanu poruku i poslati zajedno sa njom. Veličina vektora inicijalizacije treba biti jednaka veličini bloka koji se koristi u procesu kriptovanja odnosno dekriptovanja. Prilikom procesa kriptovanja korišćenjem režima ulančanih blokova koristi se poruka koja se kriptuje ( $P$ ), vektor inicijalizacije ( $IV$ ), kao i izabrani algoritam za kriptovanje podataka ( $E_K$ ). Sam proces matematički može se zapisati na sledeći način [4]:

$$C_i = E_K(P_i) \oplus C_{(i-1)}$$
$$C_0 = IV$$

Blok šifriranog teksta  $C_i$  dobija se kao rezultat kriptovanja algoritma  $E$  koji koristi ključ  $k$ . Kao ulaz u proces kriptovanja koristi se rezultat XOR operacije

između trenutnog bloka originalnog teksta  $P_i$  i zadnjeg izračunatog bloka šifriranog teksta  $C_{i-1}$ . Obzirom da za prvi korak ne može se iskoristiti predhodno izračunati blok, u ovom koraku koristi se vektor inicijalizacije  $IV$ . Proces kriptovanja korišćenjem CBC režima rada prikazan je na slici 1.



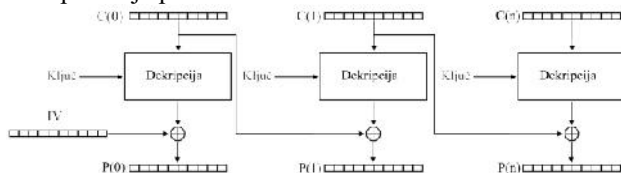
Slika 1. Proces kriptovanja u CBC režimu [5]

Slično procesu kriptovanja odvija se i proces dekriptovanja podataka. U procesu dekriptovanja koristi se kriptovani tekst ( $C$ ), vektor inicijalizacije  $IV$  kao i algoritam za dekriptovanje podataka koji koristi ključ  $k$  ( $D_{-}(K)$ ). Takođe proces dekriptovanja može se zapisati matematički na sledeći način [4]:

$$P_i = D_{-}(K)(C_i) \oplus C_{(i-1)}$$

$$C_0 = IV$$

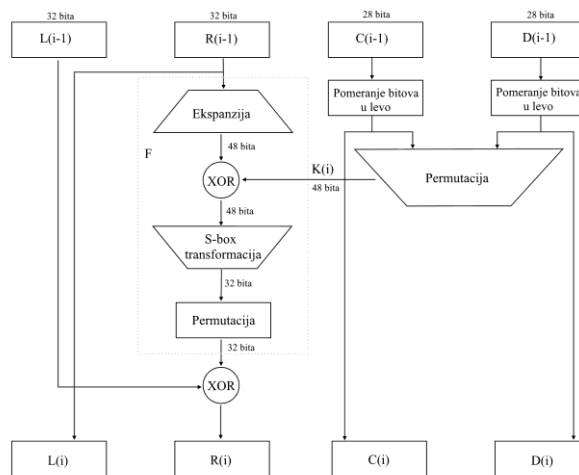
Originalni blok  $P_i$  dobija se kao rezultat XOR operacije između izlaza iz algoritma za dekriptovanje  $D_k$  i predhodnog bloka šifriranog teksta  $C_{(i-1)}$ . Ulaz u algoritam za dekriptovanje je trenutni blok šifriranog teksta  $C_i$  i ključ  $k$ . Kao i u procesu kriptovanja i ovde se u prvom koraku koristi vektor inicijalizacije. Upravo zbog toga je veoma važno da obe strane znaju koja je vrednost korišćena za  $IV$ . Na slici 2 prikazan je proces dekriptovanja podataka u CBC režimu rada.



Slika 2. Proces dekriptovanja u CBC režimu [5]

#### [4] DES ALGORITAM

DES algoritam je jedan od najviše korišćenih algoritama za kriptovanje za zaštitu u mrežnim komunikacijama, skladištenjima podataka, lozinkama i sistemima za kontrolu pristupa. DES je blok šifратор direktno implementiran po Fajstellovoj definiciji šifratora. On uzima blok fiksne dužine, kriptuje ga kroz niz operacija i na kraju vraća kriptovani tekst iste dužine. Kod DES-a podatak se deli na blokove dužine 64 bita. Kao ulaz u algoritam se koristi blok od 64-bitna izvornog teksta i 56-bitni ključ. Izlaz iz algoritma je 64-bitni kriptovani tekst koji se dobija nakon 16 iteracija koje se sastoje od identičnih operacija. Ključ od 56 bita se formira od originalnog 64-bitnog ključa ignorisanjem svakog 8 bita, tj. odsecanjem ukupno 8 bitova. Na slici prikazan je DES algoritam.



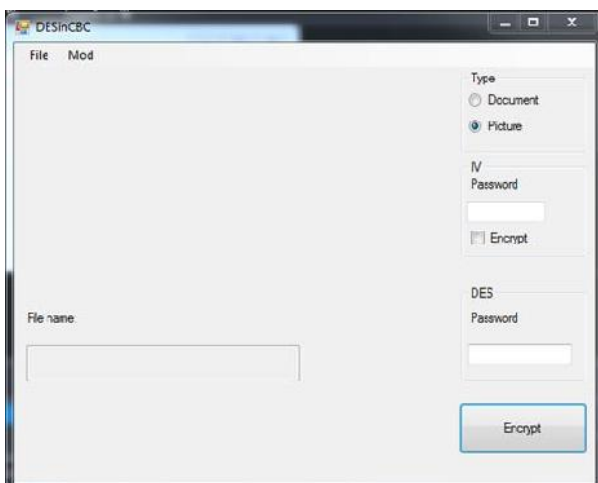
Slika 3. Izgled runde DES algoritma [1]

Kriptovanje pomoću DES algoritma se sprovodi u nekoliko koraka. Prvo se bitovi ulaznog bloka dužine 64 bita permutuju početnom permutacijom. Radi se o permutaciji koja jednostavno vrši zamenu mesta bitova. Permutovan ulazni blok deli se na dva dela od po 32 bita, levi  $L0$  i desni  $R0$  deo. Nad desnim delom bloka se obavlja funkcija  $f(R0, K1)$ , gde je  $R0$  desnih 32 bita, a  $K1$  je 48-bitni ključ. Ova funkcija generiše 32-bitni rezultat. Nad dobijenim rezultatom funkcije  $f$  i  $L0$  vrši se operacija XOR. Rezultat XOR operacije predstavlja novu 32-bitnu vrednost  $R1$  koja se koristi za dalje operacije. Kao levi deo  $L1$  se koristi vrednost  $R0$  iz prethodne iteracije. Nakon ponavljanja 16 istovetnih koraka, blokovi međusobno menjaju mesta te se spajaju. Na kraju se obavlja konačna permutacija koja je inverzna početnoj. Dobijena 64-bitna vrednost čini kriptovani blok podataka. Funkcija  $f$  kao ulaze ima pola početnog bloka podataka (32 bita) i podključ od 48 bitova i ima sledeće korake [3]:

1. Proširenje početnog polu-bloka (eng. Expansion) — 32-bitni ulazni podataka treba proširiti na 48 bita koristeći takozvane ekspanzione permutacije koje dupliraju neke od bitova.
2. Mešanje sa ključem (eng. Key mixing) - rezultat koraka 1 se sada kombinuje sa podključem koji odgovara tekućoj rundi, koristeći XOR operaciju. Tekući ključ i rezultat koraka 1 su 48-bitni tako da se nad njima direktno može izvršiti XOR nad bitovima.
3. S-box transformacija (eng. Substitution) - nakon mešanja sa ključem dobijeni 48-bitni blok se podeli na osam grupa po 6 bitova i nad svakom od njih se vrši S-box transformacija sa odgovarajućom S-box tablicom. Svaka od 8 S-box tablica zamenjuje šestobitni ulaz četvorobitnim izlazom u skladu sa nelinearnom transformacijom koja je u njoj zapisana. S-box tablice se koriste kao lookup tabele. Ulazni podatak je šestobitan, a izlazni četvorobitan.
4. Permutacija (eng. Permutation) — na kraju, izlaz iz S-box transformacije (32 bita) se preuređuje uz pomoć P-niza, koji uvodi fiksnu permutaciju nad bitovima.

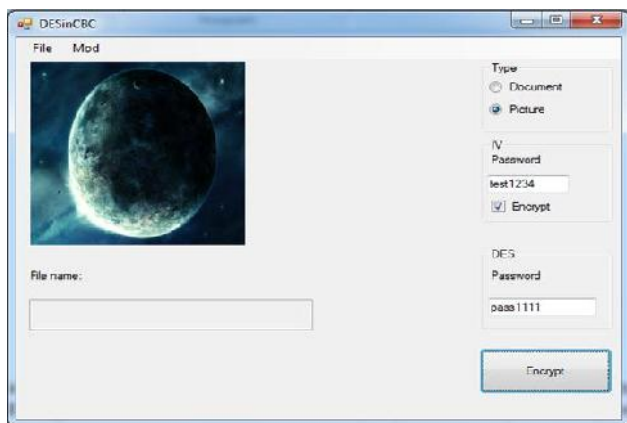
## 5. RAZVOJ APLIKACIJE ZA KRIPTOVANJE I DEKRIPTOVANJE

Aplikacija je razvijena u C# programskom jeziku (Microsoft Visual Studio 2013). U okviru aplikacije implementiran je rad DES algoritma u CBC režimu pomoću Cryptography biblioteke. Aplikacija pruža mogućnost kriptovanja slika (.bmp, .png, .jpeg) ili dokumenta (.pdf, .doc, .ppt). Glavni interfejs aplikacije prikazan je na slici 4.



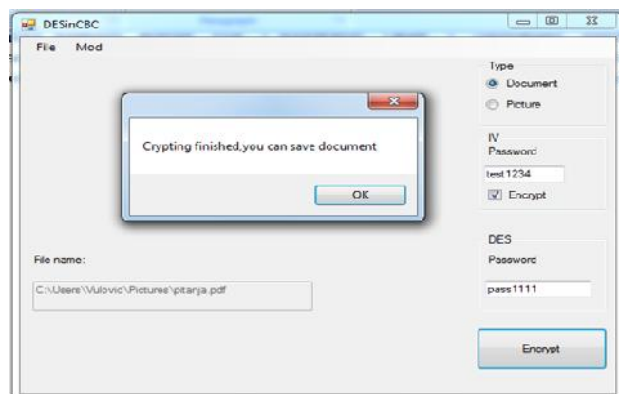
Slika 4. Glavni interfejs aplikacije

Nakon izbora slike ili dokumenta, u režimu "Mod" vrši se izbor za proces kriptovanja ili dekriptovanja. Sa desne strane nalaze se polja koja pružaju dodatne mogućnosti korisniku. Prvo polje "Type" omogućava korisniku da bira da li želi da kriptuje dokument ili da kriptuje sliku. Ispod polja "Type" nalazi se polje koje se zove "IV" i u okviru ovog polja korisnik treba da unese vrednost vektora inicijalizacije koji će se koristiti u procesu kriptovanja. DES algoritam koristi blokove veličine 64 bita, odnosno 8 bajtova, tako da vrednost IV mora biti veličine 8 bajtova, odnosno 8 ASCII karaktera. Program omogućava i kriptovanja samog vektora inicijalizacije pre procesa kriptovanja podatka i korisnik to može izabrati jednostavnim čekiranjem polja "Encrypt". IV se kriptuje posebnom šifrom koja je unapred definisana.



Slika 5. Proces kriptovanja slike

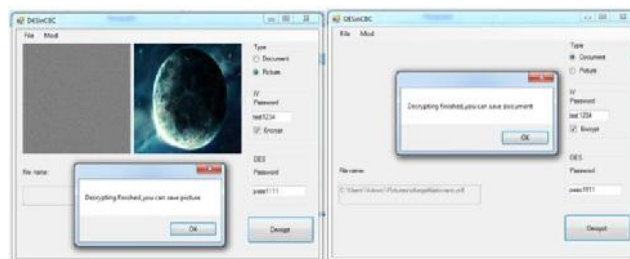
Poslednje polje je polje koje se odnosi na DES algoritam i ovde je potrebno da korisnik unese tajnu šifru koja će se koristiti u procesu kriptovanja podataka. Proces kriptovanja slike prokazan je na slici 5. Nakon učitavanja slike potrebno je postaviti vrednosti vektora inicijalizacije i tajne šifre za DES algoritam. Nakon ovih koraka vrši se proces kriptovanja jednostavnim klikom na komandno dugme "Encrypt". Kada se završi proces kriptovanja, dobija se obaveštenje da je slika kriptovana i ona se prikazuje na ekranu. Aplikacija omogućava snimanje kriptovane slike. Postupak kriptovanja dokumenata je veoma sličan što je i prikazano sa slici 6.



Slika 6. Proces kriptovanja dokumenta

Procesi kriptovanja slike i dokumenta vrše se pomoću iste funkcije. U slučaju kriptovanja slike, slika se deli na svoje 3 komponente R, G i B koje se pamte kao nizovi bajtova. Sva tri niza se prvo kriptuju, a onda spajaju kako bi kreirali kriptovanu sliku. Prilikom kriptovanja dokumenta, ceo dokument se učitava kao niz bajtova i ceo niz se prosleđuje u funkciju za kriptovanje nakon čega se dobija kriptovani dokument. Kako se u slučaju kriptovanja slike, proces odvija nad pikselima sliku je moguće otvoriti nakon kriptovanja. Kod dokumenta, to nije moguće jer je ceo fajl kriptovan uključujući i heder fajla. Međutim procesom dekriptovanja fajl je moguće rekonstruisati kao i vraćanje slike u prvobitni oblik.

Proces dekriptovanja je veoma sličan procesu kriptovanja. U ovom slučaju pre samog dekriptovanja slike u modu za dekriptovanje "Mod" bira se "Decrypt". Učitava se kriptovana slika ili dokument, postavljaju se neophodni parametri i preko komandnog dugmeta "Decrypt" dobija originalna slika, odnosno dokument koje može da snimi na računar. Na slici 7 prikazani su rezultati dekriptovanja slike, odnosno dokumenta.



Slika 7. Rezultat dekriptovanja slike/dokumenta

Listing procesa kriptovanja prikazan je na slici 8.

```
//Proces kriptovanja
//podela slike na komponente
this.SpiltImageInRGBFast bmpOrg);
DES des = new DES(this.password,
this.IvValue);

//kriptovanje komponenti slike
R = des.Encrypt(R);
G = des.Encrypt(G);
B = des.Encrypt(B);
bmpCry = new Bitmap bmpOrg.Width,
bmpOrg.Height);

//kreiranje kriptovane slike
this.CreateImageFromRGBFast bmpCry);
this.pbxCrypted.Image = bmpCry;
MessageBox.Show("Crypting finished,you can save
picture");
```

Slika 8. Proces kriptovanja slike

Listing procesa dekriptovanja prikazan je na slici 9.

```
//Proces dekriptovanja
//podela slike na komponente
this.SpiltImageInRGBFast bmpOrg);
DES des = new DES(this.password,
this.IvValue);

//dekriptovanje komponenti slike
R = des.Decrypt(R);
G = des.Decrypt(G);
B = des.Decrypt(B);
bmpCry = new Bitmap bmpOrg.Width,
bmpOrg.Height);

//kreiranje dekriptovane slike
this.CreateImageFromRGBFast bmpCry);
this.pbxCrypted.Image = bmpCry;
MessageBox.Show("Decrypting finished,you
can save picture");
```

Slika 9. Proces dekriptovanja slike

Listing procesa kriptovanja i dekriptovanja dokumenta prikazan je na slici 10.

```
//provera, da li treba vrsiti kriptovanje ili dekriptovanje
if (mod == 0)
{
//Proces Kriptovanja
DES des = new DES(this.password,
this.IvValue);
this.filePom = des.Encrypt(this.file);
MessageBox.Show("Crypting finished,you can
save document");
}
else
{
```

```
//Proces dekriptovanja
DES des = new DES(this.password,
this.IvValue);
this.filePom = des.Decrypt(this.file);
MessageBox.Show("Decrypting finished,you
can save document");
}
```

Slika 10. Proces kriptovanja i dekriptovanja dokumenta

Na slici 11 prikazan je listing funkcije za kriptovanje.

```
//Funkcija za kriptovanje
public byte[] Encrypt(byte[] encrypted1)
{
//kreiranje objekta DES algoritma
//postavljanje neophodnih parametara
byte[] plaintextbytes = encrypted1;
DESCryptoServiceProvider des = new
DESCryptoServiceProvider();
des.BlockSize = 64;
des.KeySize = 64;
//koriste se password i IV koje je naveo korisnik
des.Key =
System.Text.ASCIIEncoding.ASCII.GetBytes(Key);
des.IV =
System.Text.ASCIIEncoding.ASCII.GetBytes(IV);
des.Padding = PaddingMode.Zeros;
des.Mode = CipherMode.CBC;

ICryptoTransform crypto =
des.CreateEncryptor(des.Key, des.IV);
CryptoStream mode =
CryptoStreamMode.Write;

//kriptovanje i upis kriptovanih bajtova u Memory
Stream
MemoryStream memStream = new
MemoryStream();
CryptoStream cryptoStream = new
CryptoStream(memStream, crypto, mode);
cryptoStream.Write(plaintextbytes,
0,
plaintextbytes.Length);
cryptoStream.FlushFinalBlock();

//citanje kriptovanih bajtova iz Memory Stream-a
byte[] encryptedMessageBytes = new
byte[memStream.Length];
memStream.Position = 0;
memStream.Read(encryptedMessageBytes,
0,
encryptedMessageBytes.Length);
crypto.Dispose();
memStream.Close();
memStream.Dispose();
return encryptedMessageBytes;
}
```

Slika 11. Funkcija za kriptovanje



Na slici 12 prikazan je listing funkcije za dekriptovanje.

```
//funkcija za Dekriptovanje
public byte[] Decrypt(byte[] encrypted)
{
    //kreiranje objekta DES algoritma
    //postavljanje neophodnih parametara
    byte[] encryptedbytes = encrypted;
    DESCryptoServiceProvider des = new
DESCryptoServiceProvider();
    des.BlockSize = 64;
    des.KeySize = 64;
    //koriste se password i IV koje je naveo korisnik
    des.Key =
System.Text.ASCIIEncoding.ASCII.GetBytes(Key);
    des.IV =
System.Text.ASCIIEncoding.ASCII.GetBytes(IV);
    des.Padding = PaddingMode.Zeros;
    des.Mode = CipherMode.CBC;

    ICryptoTransform crypto =
des.CreateDecryptor(des.Key, des.IV);
    CryptoStreamMode mode =
CryptoStreamMode.Write;

    // Dekriptovanje i upis dekriptovanih bajtova u
Memory Stream
    MemoryStream memStream = new
MemoryStream();
    CryptoStream cryptoStream = new
CryptoStream(memStream, crypto, mode);
    cryptoStream.Write(encryptedbytes,
encryptedbytes.Length);
    cryptoStream.FlushFinalBlock();

    //citanje kriptovanih bajtova iz Memory Stream-a
    byte[] decryptedMessageBytes = new
byte[memStream.Length];
    memStream.Position = 0;
    memStream.Read(decryptedMessageBytes,
decryptedMessageBytes.Length);
    memStream.Close();
    memStream.Dispose();

    crypto.Dispose();
    return decryptedMessageBytes;
}
```

Slika 12. Funkcija za dekriptovanje

Na slici 13 prikazan je listing programa Funkcije za kriptovanje IV.

```
//funkcija za kriptovanje IV
public string EncryptIV(string text)
{
    byte[] plaintextbytes =
System.Text.ASCIIEncoding.ASCII.GetBytes(text);
    DESCryptoServiceProvider des = new
DESCryptoServiceProvider();
    des.BlockSize = 64;
    des.KeySize = 64;

    //koristi se poseban password za kriptovanje IV
    des.Key =
System.Text.ASCIIEncoding.ASCII.GetBytes("$iFr@159"
);
    des.IV =
System.Text.ASCIIEncoding.ASCII.GetBytes("628K#mn
@");
    des.Padding = PaddingMode.Zeros;
    ICryptoTransform crypto =
des.CreateEncryptor(des.Key, des.IV);
    byte[] encryptedMessageBytes =
crypto.TransformFinalBlock(plaintextbytes,
plaintextbytes.Length);
    return
System.Text.ASCIIEncoding.ASCII.GetString(encryptedM
essageBytes);
}
```

Slika 13. Funkcija za kriptovanje IV

## 5. ZAKLJUČAK

Razvoj i primena kvantnih računara, računarskih gridova i globalnih računarskih mreža samo su jedan od nagoveštaja budućnosti. U skladu sa tim će se postavljati sve veći sigurnosni zahtevi u smislu ranog otkrivanja i sprečavanja zloupotreba. Odgovor na ove zahteve je upravo upotreba savremenih i sigurnijih kriptografskih algoritama, koji će prevazilaziti granice jednostavne bezbednosti. Od posebnog značaja je primena kriptografskih algoritama u aplikacijama za mobilne uređaje, računarske mreže i industrijske sisteme.

## LITERATURA

- [1] William Stallings: Cryptography and Network Security: Principles and Practices, 5rd edition.
- [2] Structural Binary CBC Encryption Mode, YI-SHIUNG YEH, TING-YU HUANG AND HAN-YU LIN, Department of Computer Science National Chiao Tung University Hsinchu, 300 Taiwan
- [3] Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996
- [4] Milovanović, Emina / Ćirić, Vladimir. Bezbednost računarskih mreža. cs.elfak.ni.ac.rs.[Na mreži] .[Preuzeto: 15.02.2016]  
<https://cs.elfak.ni.ac.rs/nastava/course/view.php?id=74>.
- [5] Block cipher mode of operation. Wikipedia.org .[Na mreži] .[Preuzeto: 17.02.2016]  
[https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)

# IZAZOVI KOORDINACIJE SAJBER BEZBEDNOSTI U REPUBLICI SRBIJI U USLOVIMA KRIZNIH SITUACIJA

## CHALLENGES OF COORDINATION OF CYBER SECURITY IN THE REPUBLIC OF SERBIA IN TERMS OF CRISIS SITUATIONS

dr Goran Matić, dr Milan Miljković

*Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka*

**Sadržaj** – Krizni menadžment sajber bezbednosti podrazumeva angažovanje kapaciteta državne uprave, ministarstva odbrane, ministarstva spoljnih poslova, ministarstva finansija, ministarstva unutrašnjih poslova i obaveštajno bezbednosne zajednice, čiju aktivnost koordinira telo odgovorno za koordinaciju nacionalne bezbednosne politike, ministarski komitet ili ministar nadležan za pitanje sajber bezbednosti.

**Abstract** - *The cyber security crisis management involves engaging the capacities of the state administration, the defense ministry, the foreign ministry, the finance ministry, the interior ministry, and the intelligence and security community, whose activity is coordinated by the body responsible for the coordination of the national security policy, the ministerial committee or the minister responsible for cyber security.*

### 1. UVOD

Masovna primena informaciono-komunikacione tehnologije ima za posledicu nove rizike i pretnje koje su predstavljene fizičkim i softverskim ugrožavanjem kritičnih informacionih infrastruktura i sajber prostora od značaja za državu i njenu bezbednost. Sajber prostor određujuća je karakteristika savremenog života i ključno područje svetske ekonomije. Dnevno se zabeleži na desetine hiljada manje ili više opasnih napada u sajber prostoru, a vodeće zemlje sveta, kao i međunarodne organizacije, pokazuju rastuću svest o potrebi delovanja s ciljem povećanja stepena bezbednosti sajber prostora. Mnoge od njih već imaju svoje nacionalne strategije sajber bezbednosti i uspostavljene sisteme sajber odbrane.

Evropska unija je u februaru 2013. godine donela Strategiju sajber bezbednosti koja se zasniva na pet strateških prioriteta: 1) otpornost sajber prostora, 2) smanjenje sajber kriminala, 3) razvoj procedura i sposobnosti za sajber odbranu, 4) razvoj industrijskih i tehničkih kapaciteta za sajber bezbednost i 5) uspostavljanje internacionalne politike sajber bezbednosti. Osim toga, Evropska komisija je 2013. godine donela odluku da će aktivnosti u oblasti izgradnje zakonodavnog i drugog okvira sajber bezbednosti zemalja kandidata za članstvo u tu organizaciju, kao deo poglavlja 24, biti deo izveštaja o napretku zemalja kandidata za članstvo u EU. Pred države članice postavljeni su sledeći, minimalni zahtevi: postojanje nacionalnog autoriteta za mrežnu i

informacionu bezbednost (NIS); uspostavljanje Tima za reagovanje na incidente u sajber prostoru (CERT), usvajanje nacionalne strategije i plana saradnje u oblasti mrežne i informacione - sajber bezbednosti i međunarodna saradnja u reagovanju na bezbednosne incidente u sajber prostoru[1] <sup>1</sup>.

Takođe, analiza iskustava članica EU u organizaciji nacionalnog koncepta sajber bezbednosti ukazuje na sledeće obavezne elemente i pozitivnu praksu: izgradnja koncepta privatno-javnog partnerstva, formiranje Nacionalnog Saveta za sajber bezbednost na ministarskom nivou; postojanje posebne agencije ili interesornog koordinacionog tela radi usklađivanja koordinacije na operativnom nivou; definisanje nadležnosti i jačanje kapaciteta obaveštajno-bezbednosne zajednice, vojske i policije.

### 2. ASPEKTI BEZBEDNOSTI SAJBER PROSTORA

Za pojam sajber i sajber prostor još ne postoje precizne definicije. U nacionalnim strategijama za sajber bezbednost „sajber prostor“ se različito definiše. U vezi sa navedenim postavlja se pitanje zašto je definisanje osnovnih pojmova u vezi sa izazovima u sajber prostoru složeno i otežano. Dosadašnja iskustva ukazuju da u osnovi problema stoje različiti uglovi gledanja, različiti politički i pravni pristupi, vodećih zemalja u vezi sa ovim pitanjem, koji proizilaze iz različitih interesa globalnih aktera u vezi sa korišćenjem sajber prostora za ostvarivanje ciljeva na nacionalnom i međunarodnom planu. Iz navedenog jasno proizilazi da svaki bezbednosni problem ima tri dimenzije:

- političku (strategijsku)
- pravnu i
- tehnološku

Zaštita kritičnih infrastruktura u sajber prostoru se definiše kao strategije, politike i spremnost koja je neophodna da bi se odvratio, sprečio ili pružio odgovor u slučaju napada na kritične infrastrukture<sup>[2]</sup>. Konkretnije, zaštita kritične infrastrukture, ona ima svoj 1) politički i pravni aspekt i 2) organizacioni aspekt zaštite kritične infrastrukture i 3) izvršni aspekt.

Politički aspekt obuhvata donošenje odgovarajućih politika, strategija i zakona o sajber odbrani, in formacionoj bezbednosti, kritičnoj infrastrukturi i ostalih pravnih regulativa neophodnih da za pravno regulisanje

odvraćanja, sprečavanja i odgovor u slučaju sajber napada na kritične infrastrukture. U navedenim stratezijskim dokumentima uglavnom se pojavljuju sledeći mandati države: 1) vojne aktivnosti, 2) suzbijanje visoko tehnološkog kriminala, 3) obaveštajne i kontraobaveštajne aktivnosti, 4) zaštita kritične infrastrukture i upravljanje kriznim situacijama i 5) sajber diplomatija.

Jedno od važnih pitanja koje treba da budu definisane političkim aspektom je izbor odgovora na pretnje iz sajber prostora, dali se opredeliti za 1) ofanzivni ili 2) defanzivni pristup u sajber odbrani kritične infrastrukture. Takođe, javlja se i sledeće dileme pri izboru političkog pristupa:

- 1) podsticanje ekonomije ili poboljšanje nacionalne bezbednosti;
- 2) modernizacija infrastrukture ili zaštita kritične infrastrukture;
- 3) težište na privatnom ili javnom sektoru;
- 4) zaštita podataka ili razmena informacija;
- 5) sloboda izražavanja ili politička stabilnost.

Kada se govori o pravnom aspektu sajber odbrane kritične infrastrukture, treba pomenuti neke od značajnih pravila sajber odbrane:

- 1) *pravilo teritorijalnosti*, da su informacione infrastrukture locirane na teritoriji jedne države predmet njenog teritorijalnog suvereniteta,
- 2) *pravilo odgovornosti*, da određena država snosi odgovornost ako je sajber napad izveden sa informacionog sistema koji je lociran na njenoj teritoriji,
- 3) *pravilo saradnje*, koje podrazumeva da država sa čije teritorije izveden napad ima obavezu da saraduje sa „državom žrtvom“ i
- 4) *pravo samoodbrane*, u smislu da svako ima pravo na samoodbranu u slučaju jasne i neposredne opasnosti, uz poštovanje odredaba prava u oružanim konfliktima.

Krizni menadžment u sajber odbrani podrazumeva angažovanje kapaciteta ministarstva pravde i državne uprave, ministarstva saobraćaja, ministarstva odbrane, ministarstva spoljnih poslova, ministarstva finansija, ministarstva unutrašnjih poslova, obaveštajno bezbednosne zajednice. U tom smislu, razvijene zemlje su tokom prošle i ove godine učinile značajne korake na deklarisanju postojećih i formiranju novih civilnih i vojnih kapaciteta koji će biti nadležni za sajber odbranu, kao i definisanju interesorne saradnje i uloge privatnog sektora na tom planu.

U organizacionom smislu, vrlo je važno određivanje koordinacionog tela, najčešće tela izvršne vlasti, koja ima ulogu koordiniranja i i usmeravanja celokupne politike sajber odbrane kritične infrastrukture u državnom i privatnom sektoru. U mnogim zemljama ovu ulogu često preuzima nacionalni bezbednosni organ (NSA – National Security Authority), telo odgovorno za koordinaciju nacionalne bezbednosne politike ili ministarski komitet.

Kada govorimo o izvršnoj fazi odbrane kritične informacione infrastrukture, navešćemo da se zaštita

kritičnih informacionih infrastruktura (Critical Information Infrastructure Protection - CIIP) bazira na četiri stuba [3]:

- prevencija i rano upozoravanje (prevention and early warning),
- detekcija (detection),
- reakcija (reaction) i
- upravljanje krizama (crisis management).

U područje kritične infrastrukture, koju je na nacionalnom nivou potrebno štiti, ne ulazi samo statička infrastruktura, već i usluge, kao i fizički i elektronski tok informacija. Upravo u tom smislu i sajber prostor predstavlja kritičnu infrastrukturu, dok su istovremeno koncepti zaštite kritične infrastrukture i sajber prostora usko povezani. Potrebno je napomenuti da je problematika sajber odbrane dodatno izražena i unutar pojedinih spomenutih sektora kritične infrastrukture. Različiti infrastrukturni objekti u tim sektorima najčešće su povezani određenim komunikacijskim vezama putem sajber prostora, odnosno samo upravljanje pojedinim resursima realizuje se putem ugrađenih procesnih kompjuterskih sistema (Supervisory Control and Data Acquisition Systems – SCADA Systems).

Prilikom zaštite kritične infrastrukture, državni sektor tj. vlade ne mogu da deluju samostalno, već je neophodna saradnja s predstavnicima poslovnog sektora, nevladinim organizacijama i stručnjacima za pojedina područja. Takva je saradnja posebno važna s obzirom na činjenicu da su vlasništvo, upravljanje kritičnim sistemima najvećim delom u, kada su u pitanju razvijene zemlje, nadležnosti pravnih osoba u privatnom vlasništvu. Zbog toga privatni sektor mora značajno da bude angažovan na zaštiti kritične infrastrukture, zbog čega se i model javno-privatnog partnerstva smatra važnim stubom politike kritične infrastrukture.

Kako bi se uspostavili efikacni mehanizmi ranog upozoravanja na pretnje, osnivaju se različiti oblici CERT organizacija, odnosno tačaka za razmenu i analizu informacija o pretnjama iz sajber prostora (ISAC – Information Sharing and Analysis Centers, WARP – Warning, Alerting and Reporting Points i sl.). Razmena informacija se vrši ne samo vezano za problematiku pretnji iz sajber prostora, već i za svaki pojedini sektor kritične infrastrukture.

### **3. ISKUSTVA EU U POGLEDU KOORDINACIJE SAJBER BEZBEDNOSTI U SLUČAJU ZNAČAJNIJIH INCIDENATA**

Analiza strategija sajber bezbednosti mnogih zemalja EU, ukazuje da su se, za sada, izdvojili sledeći mandati država u sajber prostoru: *sajber upravljanje* – koordinacija aktivnosti na državnom nivou; *zaštita kritične infrastrukture i upravljanje kriznim situacijama* – podrazumeva i koncept javno-privatnog partnerstva; *suzbijanje visokotehnološkog kriminala* – u nadležnosti policijskih organa; *obaveštajne i kontraobaveštajne aktivnosti* – težišno u nadležnosti službi za signalni

obaveštajni rad (SIGINT); i *vojne aktivnosti* – koje se kreću od zaštite specifičnih informaciono-komunikacionih sistema pa do osposobljavanja za izvođenje napadnih operacija.

U institucionalnom smislu, *krizni menadžment* u sajber odbrani podrazumeva angažovanje kapaciteta državne uprave, ministarstva saobraćaja, ministarstva odbrane, ministarstva spoljnih poslova, ministarstva finansija, ministarstva unutrašnjih poslova i obaveštajno bezbednosne zajednice.

Evidentno je da je, za razliku od mnogih drugih oblasti nacionalne bezbednosti, sajber bezbednost u nadležnosti većeg broja državnih institucija. Zbog toga je potrebno da se obezbediti funkcija unutar državnog aparata koja koordinira ovom aktivnošću i obezbeđuje „*nacionalni i državni prisut*“ celokupne vlade na svim nivoima (strategijski, operativni i taktički) tokom čitavom ciklusa upravljanja incidentima u sajber prostoru, odnosno tokom faza: 1) predhodne akcije, 2) prevencije, 3) pripreme, 3) odgovora, 4) oporavka - konsolidacije 5) istrage, analize i drugih aktivnosti nakon incidenta[4].

Funkcija međuresorne koordinacije sajber bezbednosti se, zbog gore navednog, naziva i „*nacionalnim upravljanjem u oblasti sajber bezbednosti*“.

Imajući u vidu navedeno, odgovornost za poslove koordinacije često se dodeljuje telu koje ima mandat da daje zadatke ministarstvima i nacionalnim agencijama, koje je odgovorno za više koordinacionih aktivnosti između različitih resora i agencija (npr., Kao što su Kancelarija pri kabinetu predsednika vlade ili slično), zbog čega bi trebalo da ovo telo bude relativno visoko pozicionirano u državnom aparatu.

*Koordinaciona funkcija* u oblasti sajber bezbednosti ima nekoliko centralnih uloga, među kojima su najvažnije: koordinacija tokom izrade procene rizika iz sajber prostora na nacionalnom nivou (obično se izrađuje za potrebe donošenja Nacionalne strategije sajber bezbednosti), kordinacija tokom izrade Nacionalne strategije, koordinacija tokom uspostavljanja i rada nacionalnog (javno-privatnog) Saveta za sajber bezbednost i koordinacija tokom upravljanja kriznim situacijama i bilo kakvim inostranim bezbednosnim incidentima koji uključuju sajber prostor.

Nakon usvajanja Nacionalne strategija sajber bezbednosti, pored dodele odgovornosti za kreiranje Akcionog plana, Strategija bi trebala da imenuje telo nadležno za sprovođenje predloženih aktivnosti, ili telo koje će da obezbedi koordinaciju i nadgledanje njihovih implementacija, ako se zadatak raspoređuje između nekoliko državnih institucija. Koordinaciono telo trebalo da, na osnovu Strategije, postavi smernice svim resorima državne uprave, javnom i privatnom sektoru, kao i akademskim institucijama, koje bi potom trebalo da razviju svoje politike, strategije i zakonski okvir za vlastiti resor, koje će biti podređene nacionalnoj politici i

strategiji, i u skladu sa nacionalnim i međunarodnim zakonodavstvom.

Na strategijskom i političkom nivou, predsednici Vlada najčešće vode celokupnu politiku sajber bezbednosti, kao elemenat nacionalne bezbednosti, i uspostavljaju pravila vezana za sprovođenje bezbednosti nacionalnih informacionih sistema.

Premijeru, u izvršavanju ovih obaveza, često pomaže telo koje je deo njegovog Kabineta, na primer Kancelarija za sajber bezbednost, koja je odgovorna za međuvladinu koordinaciju i strateško rukovođenje u vezi sa sajber bezbednošću, što je na primer slučaj u Velikoj Britaniji. Druga najzastupljenija varijanta koordinacije na strategijskom nivou je formiranje Saveta za sajber bezbednost, čije se formiranje predviđa Strategijom a osniva se odlukom Vlade. Radom Savera rukovodi Nacionalni koordinator za sajber bezbednost koji je direktno potčinjen premijeru.

Savet za sajber bezbednost uspostavljen od strane Vlade ili Ministarstva nadležnog za sajber bezbednost, i često je podređen Savetu za nacionalnu bezbednost. Savet za sajber bezbednost je u radu administrativno i tehnički podržan od strane sopstvenog sekretarijata, kao i od strane nadležnih javnih tela koja su dobila zadatak da pomažu Savetu u izvršavanju njegovih nadležnosti, što se precizira Odlukom Vlade o radu Saveta.

*Savet za sajber bezbednost* – ili Kancelarija za sajber bezbednost, predstavlja najviše državno telo za međuresornu koordinaciju u ovoj oblasti. U okviru ovog tela funkcionišu više međuresornih radnih grupa, koje se bave različitim pitanjima, kao što su pitanja nacionalne sajber bezbednosti, kriznih situacija, međunarodna pitanja, pitanja javno-privatnog partnerstva, pitanja obrazovanja, obuka i vežbi, istraživanja i razvoja, kao i drugim pitanjima. U radu ovih grupa učestvuju vladini službenici, kompanijski i akademski eksperti iz ove oblasti, i ove grupe predstavljaju sjajan primer kako se može uključiti privatni sektor u donošenje odluka Vlade. Putem ovih radnih grupa, nedržavni sektor može postati aktivan partner sa državom tokom donošenja novih zakonskih akata iz ove oblasti, imajući u vidu da domaće i međunarodne kompanije poseduju veliko znanje i iskustvo u oblasti sajber bezbednosti. Savet ima zadatak da prati uspeh realizacije Strategije i ciljeva iz Akcionog plana tako što podnosi godišnje izvještaje o napretku Vladi.

*Na operativnom i taktičkom nivou*, obaveštajno-bezbednosne službe, Ministarstvo unutrašnjih poslova ili Ministarstvo odbrane, najčešće su zaduženi za sajber bezbednost od značaja za nacionalnu bezbednost, često pod odgovornošću resornog ministra, Vladinog koordinatora za sajber bezbednost ili Glavnog vladinog službenika za informacionu i sajber bezbednost (Chief Information Security Officer - CISO). U slučaju velikog i intezivnog sajber incidenta koji zahteva koordinisani odgovor više ministarstava, Savet za sajber bezbednost može da aktivira *Međuministarsku jedinicu za krizne situacije* (Komitet za specijalne situacije), koja nadgleda

koordinaciju odgovora, a Centar za sajber bezbednost, Vladini tehnički Tim za sajber incidente i intervencije (Vladin CERT) ili nadleža Agencija (Ministarstvo), koji imaju nadležnost da upravljaju kriminalnim incidentima i kriznim situacijama povezanim sa incidentima iz sajber prostora“, odgovorni su za mere tehničkog odgovora.

Međuministarska jedinica za krizne situacije u sajber prostoru saraduje sa NATO, Evropskom unijom, OEBS, OUN i drugim međunarodnim organizacijama kao kontakt tačka tokom međunarodnih kriznih situacija. Za uspešno praćenje i odgovore na incidente tokom sajber kriznih situacija, Međuministarska jedinica za krizne situacije, kojom rukovodi Nacionalni koordinator, zaseda u *Situacionom centru*, koji je uspostavljen ili u okviru nadležnog Ministarstva ili Agencije za operativni odgovor na sajber incidente, ili u okviru Kancelarije Kabineta premijera.

Posebna, veoma specifična, organizaciona funkcija u domenu sajber bezbednosti je sposobnost nezavisnog pregleda (inspekcije) glavnih incidenata u sajber prostoru na nacionalnom nivou. Dodavanjem odgovarajućeg nivoa sajber ekspertize, ova funkcija može biti dodeljena npr. Nacionalnom nadzornom odboru za informacionu bezbednost, koga čine eksperti iz ove oblasti.

#### **4. IZAZOVI NA PLANU PREVENCIJE I OPERATIVNOG REAGOVANJA U SLUČAJU SAJBER INCIDENATA U R SRBIJI**

U Republici Srbiji nije definisana kritična informaciona infrastruktura koja bi trebala prioritarno da se brani od pretnji iz sajber prostora, niti su opredeljene snage za njihovu odbranu. Što se tiče ugroženosti savremenih informaciono-komunikacionih sistema, za razliku od proteklih godina, kada su napadi na mobilne uređaje i android platforme su bili u granicama laboratorijskog eksperimenta, poslednje vreme su napadi na mobilne telefone i softverske platforme, na kojima ti uređaji rade, postali najmasovniji rastući oblik sajber kriminala [5]. Nesporno je da otvoren i nezaštićen sajber prostor stvara skoro neograničene mogućnosti za ugrožavanje nacionalnih interesa. Proliferacija informatičke tehnologije, uz sve moguće benefite, povećali su ranjivost informacionih sistema u zemlji.

U Republici Srbiji, prema odredbama Zakona o informacionoj bezbednosti, u cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji informacione bezbednosti, kao i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti, Vlada je obrazovala Telo za koordinaciju poslova informacione bezbednosti.

Organ državne uprave nadležan za bezbednost IKT sistema, prema odredbama Zakona o informacionoj bezbednosti, je Ministarstvo trgovine, turizma i telekomunikacija, odnosno ovo ministarstvo je predviđeno na bude Nadležni organ – tj. nacionalni autoritet za mrežnu i informacionu bezbednost (NIS) [6].

Za poslove Nacionalnog CERT-a, prema odredbama pomenutog Zakona, nadležna je Regulatorska agencija za elektronske komunikacije i poštanske usluge. Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi sa tim obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji. Planirano je da i svaka važna institucija, pravno lice, i grupa pravnih lica formira Poseban centar za CERT koji će ostvarivati saradnju sa Nacionalnim CERT-om. Takođe, za zaštitu IKT sistema Računarske mreže republičkih organa biće formiran Centar za bezbednost IKT sistemima u republičkih organa, čije poslove obavlja novoformirana Kancelarija za IT i e-uprvu Vlade R Srbije.

U smislu preventivnog delovanja, odnosno uspostavljanja efikasnog okvira sajber bezbednosti pre nastupanja incidenta u sajber prostoru zemlje, jedan od ključnih uočenih izazova je *pitanje procene i upravljanja rizikom*. Naime, upravljanje rizikom je načelo predviđeno Zakonom o informacionoj bezbednosti i predviđa da se svaki organ, prilikom izbora mera zaštite, vodi rezultatima prethodno sprovedene analize rizika. [7]

Dodatni izazov uspostavljanju sveobuhvatnog sistema upravljanja rizikom je činjenica da ne postoji obaveza da se rezultati sprovedenih analiza rizika dele sa bilo kim. Tačnije, analiza rizika je interni dokument u operatorima IKT sistema, na osnovu kojeg se definiše Akt o bezbednosti i uvode mere zaštite.

Zbog brzine kojom se mogućnosti i rizici razvijaju u sajber svetu, potreba za analizom rizika u realnom vremenu, posebno u slučaju nastupanja incidenta, postaje neophodna. Međutim, upitno je da li je tako nešto moguće ukoliko se ne uspostavi radno telo za ove potrebe. Čak i tada, pitanje kapaciteta Nacionalnog CERTa da isprati sve informacije predstavlja još jedan od uočenih rizika. Ključno pitanje vezano za procenu rizika u slučaju izbijanja incidenta je kako se koordinišu i gde se sabiraju relevantne informacije koje bi služile kao osnova za određivanje stepena ozbiljnosti jednog ovakvog događaja i njegovog potencijalnog daljeg razvoja.

*Operativni izazovi* se odnose na izazove koji proizlaze iz primene postojećih politika i procedura u praksi, odnosno, u slučaju incidenta. Odnose se na procedure komunikacije među ključnim akterima, njihove kapacitete za delovanje, kao i na operativne izazove prouzrokovane trenutnim zakonskim rešenjima. Svi ovi izazovi se međusobno preklapaju.

*Krizna komunikacija* odnosi se na razmenu informacija u realnom vremenu među ključnim akterima u slučaju nacionalnog sajber incidenta. Pokazalo se da, iako delom uređene Zakonom i pratećim podzakonskim aktima, procedure komunikacije među ključnim institucijama i dalje nisu potpuno jasno definisane.

Zakonsko rešenje koje je bilo iznuđeno situacijom (nepostojanjem n-CERTa u trenutku usvajanja Zakona o informacionoj bezbednosti) po kome se incidenti prijavljuju Ministarstvu trgovine, turizma i telekomunikacija, umesto n-CERTu biće uskoro rešeno posebnim protokolom o saradnji između te dve institucije.

Jedino mesto koje se trenutno prepoznaje kao forum za razmenu informacija u kriznim situacijama jeste Telo za koordinaciju poslova informacione bezbednosti. Pretpostavlja se da će predstavnici institucija u ovom Telu informisati svoje matične institucije. *Generalno, komunikacija među državnim organima i infrastrukturom u vlasništvu države odvija se neformalnim kanalima i zasniva se na ličnim poznavanjima.* Sa jedne strane, ovo omogućava brži protok informacija. Međutim, osim toga što ovakav mehanizam ne može biti trajno rešenje, potencijalni odlazak kadrova ujedno znači i urušavanje postojećih, neformalnih kanala komunikacije među institucijama.

Kapaciteti ključnih aktera, u smislu tehničkih mogućnosti kao i operativnih (ljudstvo), predstavljaju jedan od glavnih problema i prepreka uspostavljanju efikasnog i sveobuhvatnog sistema krizne komunikacije u slučaju sajber incidenata na nacionalnom nivou. Najpre, iako je jasno da je Nacionalni CERT institucija u formiranju, njegovi postojeći kapaciteti ocenjeni su kao nedovoljni za hitno reagovanje. Opšti utisak je da n-CERT koordiniše isključivo informacije koje su na tehničkom nivou. Generalno, uloga n-CERTa kao nacionalne kontakt tačke za kriznu komunikaciju ocenjena je kao nedovoljno jasna i izražena.

Telekomunikacioni operateri i internet provajderi, kao kritična informaciona infrastruktura, odnosno, operatori IKT sistema od posebnog značaja, trenutno imaju razvijene interne procedure u slučaju incidenta, u skladu sa zakonski predviđenim Aktom o bezbednosti. U slučaju incidenta, dakle, oni uspostavljaju međusobnu komunikaciju, formalnu i neformalnu preko definisanih kontakt osoba. Međutim, postavlja se pitanje horizontalne komunikacije velikih provajdera sa malim provajderima i obrnuto – u kojoj meri formalno postoji, koliko je ažurna i koliko efikasna. Imajući u vidu da trenutno ne postoji CERT operatera, istaknuti izazovi odnose se na pitanje mogućnosti hitne reakcije na incident i efikasnost kojim bi se informacije prenele manjim operaterima koji, za razliku od većih, nisu u bazi kontakata Nacionalnog CERT-a, već se očekuje da će veliki provajderi (kao nadprovajderi) ovu poruku poslati dalje svojim kanalima komunikacije.

## ZAKLJUČAK

Stanje bezbednosti Srbije u sajber prostoru sa aspekta mogućih pretnji, posledica i šteta približno jednaka stanju u svetu i okruženju. Internet je svetski fenomen, jedinstven je i važi za sve, za male i velike, za siromašne i bogate, za moćne i one koji to nisu. Republika Srbija je u

fazi uspostavljanja sistema odbrane od pretnji u informacionom i sajber prostoru.

Ključni problemi i izazovi koji su identifikovani u slučaju pojave incidenata na nacionalnom nivou su : 1) nejasnoće postojećih procedura za komunikaciju u kriznim situacijama, 2) nejasne zakonske odrednice: definicije i klasifikacije incidenata, 3) nejasan okvir u u kojem Telo za koordinaciju poslova informacione bezbednosti funkcioniše, ovlašćenja i operativni kapaciteti, 4) nedostatak centralnog operativnog tela za reagovanje i koordinaciju svih drugih aktera u slučaju nacionalnog sajber incidenta, 5) nedostatak jasnih odrednica i procedura za komunikaciju nadležnih organa sa javnošću, 6) nedefinisana ovlašćenja, operativno funkcionisanje i procedure reagovanja nacionalnih kontakt tačaka za međunarodnu saradnju kroz okvire Ujedinjenih nacija i OEBSa.

Imajući u vidu zahteve i iskustva EU u organizovanju koncepta sajber bezbednosti i odbrane, ključne mere koje R Srbija treba da sprovede u ovoj oblasti: 1) definisanje koncepta privatno-javnog partnerstva; 2) donošenje Strategije sajber bezbednosti i odbrane 3) formiranje Nacionalnog Saveta i ministarstva (ministra bez portfelja) nadležnog za sajber bezbednost; 5) uspostavljanje efikasnije interesorne koordinacije u slučaju incidenata od nacionalnog značaja; 6) uspostavljanje sistema edukacije u oblasti sajber bezbednosti i 6) standardizacija u oblasti obuke, tehnologije, opremanja i sertifikacije IKT sistema.

## LITERATURA

[1] Cybersecurity Strategy of the European Union: A Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final [http://eeas.europa.eu/policies/eu-cyber-security/cybsec\\_comm\\_en.pdf](http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf).

<sup>ii</sup> [2] Lewis G., Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006, p. 4.

[3] Suter M., A Generic National Framework for Critical Information Infrastructure Protection, Center for Security Studies, ETH Zurich, 2007.

[4] National Cyber Security Strategy Guidelines, NATO CCD COE, Tallinn 2013., at <http://www.ccdcoe.org>.

[5] Živković Z.: "Stanje informacione bezbednosti u Srbiji i svetu", Informaciona bezbednost 2013 – naučno stručni skup, PKS, Beograd, 2013. <http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.29.0.html:437424-A-larmatno-stanje-informacione-bezbednosti-u-Srbiji>

[6] Закон о информационој безбедности Републике Србије, ("Сл. Гласник Р. Србије, бр. 6/2016 и 94/2017)

[7] Podaci su iz Izveštaja koji je sastavila Misija OEBS-a u Srbiji i Diplo Fondacija uz angažovanje domaćih i stranih stručnjaka, na osnovu rezultata Simulacione sajber vežbe "Srbija 2017", održane od 28. do 30. novembra 2017. godine u Istraživačkoj stanici Petnica.



# PREPARING FOR SOA GOVERNANCE IN DSO “EPS DISTRIBUCIJA”

## PRIPREME ZA SOA UPRAVLJANJE U ODS “EPS DISTRIBUCIJA”

Miloš Kostić<sup>1</sup>, Dejana Stefanović-Kostić<sup>2</sup>, Aleksandra Tomić<sup>3</sup>  
*EPS Distribucija*<sup>1,2</sup>, *Fakultet za menadžment Sremski Karlovci*<sup>3</sup>

**Sadržaj** – U ovom radu je predstavljeno SOA upravljanje, kao i detalji implementacije SOA politika. Predstavljene su aktivnosti na uvođenju SOA upravljanja u ODS “EPS Distribucija”. Data je strategija uvođenja koja je primenljiva na preduzeća u javnom sektoru.

**Abstract** – In this paper we present SOA governance, and the details of SOA policies. We also present activities for introduction of SOA governance in DSO “EPS Distribucija”. The strategy that is described is applicable throughout the public sector.

### 1. INTRODUCTION

In the last two decades, business software evolved from simple programs that ran on few servers to very complex, distributed applications. In the same time, business that was automated by those applications started to change even more, partially because applications enabled it. Enterprise – wide changing events, like acquisitions and mergers became normal, and even frequent. In public sector, regulating agencies started to demand more of public enterprises year after year, inducing previously unimaginable, and often illogical changes to business practices. The frequency of those changes demanded more agile applications. After many partial solutions, industry came up with Service – Oriented Architecture (SOA), as a set of practices that enabled creation of agile business applications. SOA brings many potential benefits to an enterprise and increases its business value [1]. However, many organizations that try to implement SOA fail to meet the expectations [2]. This can be prevented with embracing the best practices in SOA adoption, one of which is effective SOA governance [3]

### 2. WHAT IS SOA GOVERNANCE

Even before SOA emerged as preferred design practice, the complexity of distributed software solutions demanded some form of governance over application architecture and business requirements. With introduction of SOA, governance over various aspects of business application solutions became more important, because interoperability between loosely coupled services relies on strict adherence to design policies. The existing forms of IT governance, like ITIL, COBIT or ISO/IEC 38500 need to be merged with corporate governance, in order to form SOA governance.

Authors endorse the following definition of SOA governance: Activities for implementation and ongoing execution of an SOA stakeholder decision model and accountability framework that ensures an organization is pursuing an appropriate SOA strategy aligned with business goals, and is executing that strategy in accordance with guidelines and constraints defined by a body of SOA principles and policies. SOA policies are enforced via a policy enforcement model, which is realized in the form of various policy enforcement mechanisms such as governance boards and committees; governance processes, checkpoints, and reviews; and governance enabling technology and tools [4].

In order to be effective, SOA governance has to ensure the following [5]:

- Define the SOA related policies
- Apply these policies during service design time
- Monitor and enforce the policies during runtime

Applying and monitoring policies are activities that require mature SOA governance process. However, one can start defining SOA policies early in the process of SOA adoption.

### 3. SOA POLICIES

Policies can be guidelines or rules. Guidelines describe desired attributes of certain parts of SOA architecture, whereas rules state mandatory requirements.

In EPS Distribucija, we have established a form for documenting policies, which has following fields:

- Policy name
- Area – identifies principal stakeholder
- Type – guideline or rule
- Service provider responsibilities
- Service consumer responsibilities
- Infrastructure responsibilities

Industry standards like TOGAF recommend that SOA policies reflect agreed-upon reference architecture. This introduces the need for sophisticated reference architecture which is either absent, or inadequate in early stages of SOA adoption. Therefore we propose creating SOA policies before establishing reference architecture. Of course, such policies can't be very specific, but we assert that

establishing some high level policies early in the process of SOA adoption helps creating the governance process itself. At this stage, it is very important to identify shortcomings of the governance process, like decision making, or documentation of the policies. After few iterations of ironing out identified deficiencies, the SOA governance should be prepared for challenges that will inevitably come.

#### 4. ORGANIZING FOR SOA GOVERNANCE

Arguably the most important factor for success of SOA governance is the selection of the right people that will conduct the governance process. The selection process depends on organizational position of governance body. Literature even suggests creating a special department for SOA governance exclusively [6, p. 131]. Having assessed current business trends, we decided against enlarging organizational structure of EPS Distribucija, and opted for creation of special SOA governance commission without hiring additional people instead. This commission has a mandate for creating SOA governing policies.

The majority of people selected for SOA governance commission are senior employees, just below manager level, with at least five years of work experience in company. However, we decided to include two manager level members, because of their insight in ongoing regulatory changes that are impacting EPS Distribucija profoundly.

Also in the team is one employee from quality assurance division. Having been certified for numerous ISO standards, EPS Distribucija has extensive documentation regarding business practices. This documentation has to be synchronized with SOA governing policies.

#### 5. CONCLUSION

Having established that SOA governance is the pillar of successful SOA adoption, we decided to start introducing this process in EPS Distribucija. Our strategy is to create a group that will start with simple governing policies, in order to perfect the SOA governing process itself. This governing process will enable smooth adoption of SOA in EPS Distribucija.

#### LITERATURE

- [1] B. Mueller, G. Viering, C. Legner and G. Riempp, "Understanding the Economic Potential of Service-Oriented Architecture," *Journal of Management Information Systems*, vol. 26, no. 4, pp. 145-180, 2010.
- [2] X. Li and S. Madnick, "Understanding Organizational Traps in Implementing Net-Centric Systems," Composite Information Systems Laboratory (CISL), MIT, 2012.
- [3] D. Vukomanović and D. Kalpić, "Key Practices for SOA Adoption," *Recent Researches in Applied Information Science*, pp. 20-26, 2012.

- [4] E. A. Marks, *Service-Oriented Architecture Governance for the Services Driven Enterprise*, John Wiley & Sons, Inc. Editions, 2008.
- [5] J. Dirksen, *SOA Governance in Action*, Manning, 2013.
- [6] T. Erl, *SOA Governance - Governing Shared Services On-Premise and in the Cloud*, Prentice Hall, 2011.

# Uporedna analiza GraphQL i RESTful načina implementacije veb servisa

## Comparative analysis of GraphQL and RESTful web service implementations

Miloš Zlatković

Fakultet organizacionih nauka

**Sadržaj** – Od kada je Facebook objavio svoj GraphQL okvir za implementaciju veb API-ja, ova tehnologija postaje sve popularnija i daje alternativu najčešće korišćenom RESTful arhitekturnom stilu. Cilj ovog rada je uporedna analiza ova dva načina implementacije veb API-ja. U prvom delu daće se kratak prikaz koncepata RESTful arhitekturnog stila. Nakon toga, biće ukratko opisan GraphQL. Na kraju će biti prikazane razlike GraphQL okvira u odnosu na RESTful.

**Abstract** – Since Facebook has released its GraphQL framework for the implementation of the Web API, this technology is becoming more and more popular and provides an alternative to the most frequently used RESTful architectural style. The goal of this paper is a comparative analysis of these two ways of implementing the Web API. The first part will give a brief overview of the RESTful architectural style concepts. After that, GraphQL will be briefly described. Finally, the differences between the GraphQL framework and the RESTful will be displayed.

### 1. UVOD

Sa razvojem tehnologije, dolazi i do promene arhitektura aplikacija, odnosno načina njihovih implementacija. Sve veća potreba za podacima, razvoj interneta, razvoj mobilnih i pametnih uređaja i napredak tehnologija za razvoj aplikacija su neki od faktora koji utiču na odabir odgovarajuće arhitekture aplikacije.

Iz toga proizilazi potreba za korišćenjem veb servisa. Bilo da se koriste interno, u okviru aplikacije, ili postaju javno dostupni, veb servise je potrebno izložiti. U tu svrhu se kreira aplikacioni programski interfejs (API), koji omogućava pristup veb servisima.

Postoji više načina za implementaciju API-ja, od kojih je najčešće korišćen RESTful (REpresentational State Transfer) stil. Ovaj stil, koji je razvijen kao deo doktorske disertacije Roja Fieldinga (eng. Roy Fielding) 2000. godine [1] uvodi resurs kao apstrakciju i podrazumeva da je svaki resurs jedinstveno identifikovan. Resurs može biti stranica, podatak, slika itd. Takođe, iako nije zavisn od HTTP protokola, REST koristi neke od svojstava HTTP protokola. Pored toga, ovaj stil podrazumeva primenu dodatnih ograničenja o kojima će biti više reči kasnije.

Jedna od alternativa RESTful stilu je i GraphQL okvir, koji je razvijen od strane kompanije Facebook 2012. godine, a zvanično objavljen kao specifikacija 2015. nakon 3 godine internog korišćenja. Uz specifikaciju, Facebook je objavio i referentnu implementaciju. Od trenutka objavljivanja, broj korisnika je u konstantnom porastu, od kojih su neki svetski poznati brendovi kao što su Coursera, GitHub, Shopify i Twitter [2]. Među glavnim karakteristikama

GraphQL-a izdvajaju se način dobijanja podataka i stroga tipiziranost koja smanjuje mogućnost grešaka. O ovim i ostalim karakteristikama biće više reči kasnije.

Osnovna razlika između ova dva načina implementacije je pristup podacima. Kod RESTful stila svaki resurs ima svoj jedinstveni identifikator u vidu URL-a, dok GraphQL ima jedinstveni URL kao ulaznu tačku (eng. endpoint) za više resursa, a gde se kroz upit specificira zahtevani skup podataka.

### 2. REST

REST (REpresentational State Transfer) označava principe, pravila i ograničenja koje je potrebno zadovoljiti da bi API bio u skladu sa RESTful arhitekturnim stilom. Ovakav API treba da izloži resurse i definiše operacije nad njima. Operacije su u skladu sa CRUD operacijama (Create, Read, Update, Delete) [6]. Iako po definiciji nije zavisn od HTTP protokola, REST se oslanja na ovaj protokol, i pomoću HTTP metoda određuje se koja operacija se zahteva, dok je resurs nad kojim treba da se izvrši zahtevana operacija identifikovan pomoću URL-a. Implementacija REST API-ja ne zavisi od konkretnog programskog jezika, već može biti urađena u svakom programskom jeziku koji podržava HTTP metode. Kao ni za GraphQL, način skladištenja podataka ne utiče na arhitekturu REST-a, tj. moguće je implementirati bilo koji način skladištenja.

RESTful arhitekturni stil daje neka ograničenja prema kojima API treba da se upravlja: [1]

1. **Klijent – Server** (eng. Client - Server) – Ovo ograničenje podrazumeva upotrebu klijent – server arhitekture, odnosno podelu aplikacije na klijentski i serverski deo, gde je svaki od njih nezavisn i može se posebno razvijati. Takođe, osnovni princip ove arhitekture je da klijent šalje zahtev, a server šalje odgovor, bez izuzetaka.
2. **Bez čuvanja stanja** (eng. Stateless) – Ovo ograničenje zahteva da između zahteva koje upućuje klijent server nigde ne čuva stanje aplikacije. Iz ovoga proizilazi da svaki zahtev mora sadržati sve potrebne informacije kako bi server znao da obradi taj zahtev, a kao odgovor server mora da pošalje sve zatražene informacije klijentu.
3. **Keširanje** (eng. Cache) – Potrebno je omogućiti keširanje odgovora eksplicitnim ili implicitnim obeležavanjem koji odgovori mogu biti keširani, tako da sloj/komponenta zadužena za keširanje može na pravi način odgovoriti klijentskim zahtevima.
4. **Interfejs/Jednoobrazni ugovor** (eng. Interface/Uniform contract) – Po ovom ograničenju interfejs koji se izlaže mora biti kao

ugovor između dve strane, gde se izlažu funkcionalnosti servera kroz URL, metode i tipove sadržaja. Način izlaganja svih funkcionalnosti je standardizovan. Takođe, standard se primenjuje na više klijenata, odnosno ne bi trebalo da bude prilagođavan svakom klijentu. Ovo ograničenje takođe podrazumeva da server u odgovoru šalje relevantne linkove ka drugim resursima ili drugim operacijama nad istim resursom. Na ovaj način moguće je dinamičko otkrivanje API-ja, tj. klijent ne mora znati unapred sve moguće opcije koje API pruža.

5. **Višeslojevni sistem** (eng. Layered system) – Da bi aplikacija bila u skladu sa ovim ograničenjem, aplikacija treba da se podeli na slojeve koji su nezavisni i koji komuniciraju samo sa „sledećim slojem do sebe“. Što znači da sloj ne zna za postojanje nijednog drugog sloja osim onog koji treba da pozove. Slojevi se mogu menjati, dodavati i uklanjati nezavisno jedan od drugog. Pridržavajući se ovog ograničenja, razvoj jednog sloja neće uticati na ostale.
6. **Kod na zahtev** (Code-on-demand) – Ovo ograničenje je opciono, i ono podrazumeva da se logika na klijentu ažurira nezavisno od serverske. Najčešće se oslanja na veb tehnologije koje se mogu izvršavati na klijentu, kao što je JavaScript (i okviri zasnovani na ovom programskom jeziku). Ovaj princip se može prenositi na slojeve, pa tako neki sloj koji je iz jednog aspekta server, iz drugog postaje klijent, i za njega važi isti princip.

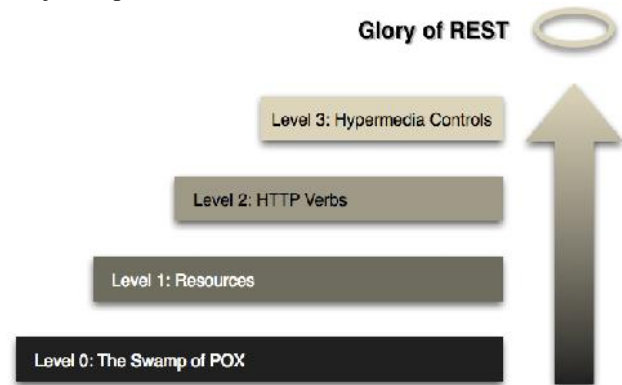
Ova pravila predstavljaju 6 osnovnih ograničenja RESTful arhitekturnog stila. Ipak, neke aplikacije se ne pridržavaju svih 6 ograničenja. Zbog toga je Lenard Ričardson (eng. Leonard Richardson) uveo model zrelosti REST API-ja, koji klasifikuje REST API na 4 osnovna nivoa. [7]

1. **Nivo 0:** ceo interfejs je izložen kroz jednu ulaznu tačku, ne koristi se nijedno svojstvo HTTP protokola (metode, zaglavlja). Svi podaci smešteni su u telu zahteva koje je najčešće u XML ili JSON formatu. Ovakav API otežava dokumentovanje, nije indikativan i težak je za dalju nadogradnju i održavanje.
2. **Nivo 1:** uvodi se koncept resursa i jedinstvenog identifikovanja resursa preko URL-a. Svaki resurs ima svoju ulaznu tačku preko koje je identifikovan, dok se ostale informacije prenose u telu zahteva kao i na nivou 0. I dalje se koristi samo jedna HTTP metoda, tj. semantika metode nije od značaja.
3. **Nivo 2:** uvode se funkcionalnosti HTTP protokola. Koriste se HTTP metode, gde svaka metoda ima različitu semantiku, uz klijentske zahteve šalju se zaglavlja koja pružaju dodatne informacije o podacima koji se šalju (npr. tip/format podataka, veličina podataka...). Pri formiranju odgovora, server koristi odgovarajuće HTTP statusne kodove, i u slučaju uspešno izvršenih operacija, i u slučaju grešaka prilikom

obrade zahteva. Bitna je razlika između GET i ostalih metoda, gde je GET metoda „sigurna“, tj. nema nikakve sporedne efekte, dok ostale metode mogu proizvesti izmenu resursa.

4. **Nivo 3:** na ovom nivou uvodi se HATEOAS (Hypermedia As The Engine Of Application State). HATEOAS podrazumeva da server prilikom odgovora šalje i moguće akcije koje klijent može da preduzme a koje su povezane sa trenutnom akcijom. Na taj način, olakšava klijentu „kretanje“ kroz API. Zbog ovakvog pristupa, moguće je lako predstaviti aplikaciju preko dijagrama promene stanja, gde klijentski zahtev dovodi aplikaciju u neko stanje, a akcije koje se šalju kao odgovor predstavljaju tranzicije koje prevode aplikaciju u neko drugo stanje.

Grafički prikaz nivoa dat je na slici 2, gde se vidi prikaz svojstava po nivou.



Slika 1. Ričardsonov model zrelosti

Iako se termin REST koristi za aplikacije koje su na različitim nivoima zrelosti, Roj Filding kao kreator REST-a kaže da je tek nivo 3 preduslov da bi aplikacija bila u skladu sa RESTful arhitekturnim stilom. [1]

Postoji dosta okvira i alata koji se baziraju na REST-u kao što su OpenAPI specifikacija [8], RAML [9] i mnogi drugi, koji olakšavaju rad i uvode dodatna ograničenja u cilju što bolje implementacije i dokumentacije API-ja.

### 3. GRAPHQL

GraphQL okvir je objavljen kao specifikacija, te nije zavisen ni od jedne konkretne tehnologije. On predstavlja sloj za pristup podacima, gde se definiše model dostupnih podataka i operacija koje se mogu izvršavati. Osnovna komponenta ovog okvira je upitni jezik koji se koristi za izražavanje zahteva za podacima. [3] Implementacija ovakvog API-ja nije ograničena na konkretan programski jezik. Takođe, GraphQL se ne oslanja na HTTP protokol i ne zavisi od HTTP metoda, iako je upravo HTTP protokol najčešće korišćen pri pozivanju API-ja koji implementiraju GraphQL.

Način funkcionisanja GraphQL-a se znatno razlikuje od RESTful API-ja. Osnovna razlika je u pristupu podacima. Za razliku od RESTful sistema gde se svaki resurs

jedinstveno identifikuje pomoću URL-a (ulazne tačke), GraphQL ima samo jednu ulaznu tačku za ceo skup entiteta. Prilikom slanja zahteva API klijent šalje i upit koji sadrži informacije o tome koje podatke on želi da pročita ili upiše, u skladu sa upitnim jezikom. Ovaj upit se šalje u formatu koji je sličan JSON formatu. Server obrađuje taj upit i sakuplja odgovarajuće tražene podatke, koje šalje kao odgovor u istom formatu i istog oblika kao i upit na koji odgovara. Za pronalaženje odgovarajućih podataka pozivaju se specijalne funkcije koje se nazivaju rezolverima (eng. resolvers). Za svako polje svakog entiteta moguće je napisati rezolver koji je zadužen za pronalaženje vrednosti za dato polje. Upit koji se šalje mora biti u skladu sa šemom koja definiše model.

GraphQL okvir zahteva strogu tipizaciju entiteta nad kojima se kreira API. U tu svrhu kreira se šema entiteta, gde su iskazane definicije tipova, veze između njih, definicije ulaznih argumenta i operacija. Za definiciju šeme koristi se jezik za definisanje šeme (eng. Schema Definition Language). Stroga tipizacija omogućava lakšu detekciju grešaka i osnovni je preduslov za rad GraphQL upitnog jezika koji korisniku API-ja omogućava da odabere polja koja su mu potrebna.

Tipovi koji se definišu sadrže svoj naziv i skup polja. Svako polje ima svoj tip, koji može biti prost ili složen. Prosti tipovi nemaju složenu strukturu već pri odgovoru na upit polja koja su prostog tipa sadrže literalne vrednosti. Prosti tipovi mogu biti korisnički definisani ili predefinisani. GraphQL implementira 5 predefinisanih tipova i to [4]:

- Int
- Float
- String
- Boolean
- ID

Prost tip se definiše ključnom rečju „*scalar*“, dok se za definiciju složenog tipa koristi ključna reč „*type*“. Takođe, pri definiciji tipa može se naznačiti da neko polje mora imati povratnu vrednost ako je zatraženo, tj. da njegova vrednost ne sme biti „*null*“. Ovo se postiže stavljanjem uzvičnika (!) pored tipa polja u definiciji tipa. Osim toga, polje može biti i kolekcija, što se naznačava srednjim zagradama ( [ ] ) koje se stavljaju oko tipa polja.

Operacije nad podacima se definišu kao upiti (eng. Query) i mutacije (eng. Mutation). Upit je operacija koja se koristi za čitanje podataka. Svaki upit ima povratnu vrednost koja mora biti određenog tipa. Prilikom slanja zahteva od strane klijenta, klijent može zahtevati samo određena polja povratne vrednosti, i na taj način može prilagoditi upit svojim potrebama. Kao što je već napomenuto, GraphQL server će poslati odgovor koji po strukturi potpuno odgovara zahtevanim podacima. Ova pogodnost daje veliku fleksibilnost GraphQL-u i smatra se jednom od njegovih najvećih prednosti u odnosu na konkurente.

Pomoću mutacija se definišu operacije koje podrazumevaju neku manipulaciju podacima. Tu spada dodavanje novih podataka, menjanje postojećih i brisanje

podataka. Prilikom slanja zahteva, klijent prosleđuje podatke u formatu sličnom JSON-u, koje odgovarajući rezolver za tu mutaciju prihvata i vrši njihovu obradu. Svaka mutacija, kao i upit, ima odgovarajuću povratnu vrednost. Ovo svojstvo omogućava da klijent može da formira odgovarajući skup podataka koji želi da dobije kao rezultat mutacije.

U GraphQL šemi se mogu definisati i tipovi koji predstavljaju ulazne argumente za upite i mutacije. Ovakvi tipovi se nazivaju ulazni tipovi, i definišu se isto kao i regularni, sa tom razlikom da polja ulaznog tipa mogu biti ili prostog tipa ili drugog ulaznog tipa. Drugim rečima, nije dozvoljeno kombinovanje ulaznih i regularnih tipova. Za definisanje ulaznog tipa koristi se ključna reč „*input*“. Razlog za specijalizaciju tipova na regularne i ulazne je potencijalni problem prilikom kružnih referenci kod ulaznih argumenata, ili referenci na interfejs ili uniju. Ulazni tipovi ne mogu implementirati interfejs ili biti deo unije. [5] Primer šeme može se videti na slici 1, gde su dati tipovi Student i Smer, ulazni tip StudentInput kao i dva upita, za pretragu studenta po ID-u, i za pretragu smeru, gde ID nije obavezno polje pa se može i izostaviti. Dat je i primer mutacije za unos studenta gde se ulazni tip StudentInput koristi kao ulazni argument, a povratna vrednost mutacije je instanca tipa Student.

```

type Student {
  id: ID!
  ime: String!
  prezime: String!
  brojIndeksa: String!
  smer: Smer!
  godinaStudija: int!
}

input StudentInput {
  id: ID
  ime: String!
  prezime: String!
  brojIndeksa: String!
  smer: ID!
  godinaStudija: int!
}

type Smer {
  id: ID!
  naziv: String!
  studenti: [Student!]!
}

type Query {
  vratiStudenta(id: ID!): Student!
  vratiSmer(id: ID): Smer!
}

type Mutation {
  unesiStudenta(student: StudentInput): Student!
}

```

Slika 2. Primer GraphQL šeme

Često se dešava da više tipova imaju zajedničke osobine, ali se u nekim delovima razlikuju (npr. student, zaposleni). U tim situacijama, moguće je kreirati novi tip, koji bi predstavljao nadtip pomenutim tipovima. U GraphQL-u je to moguće uraditi preko koncepta interfejsa. Definiše se interfejs sa odgovarajućim poljima koje sadrže svi podtipovi. Da bi podtip implementirao interfejs, potrebno je imati sva ona polja koja sam interfejs ima. Tako kreirani

interfejs se može koristiti kao tip polja ili kao povratna vrednost upita ili mutacije. Takođe, postoji koncept unije, gde više različitih tipova mogu činiti uniju. Ovaj koncept se najčešće koristi kada rezultat nekog upita ili mutacije ne mora biti jednog tipa, već je moguće vratiti konačno mnogo različitih tipova. Tada ti tipovi kreiraju uniju koja se, kao i u slučaju interfejsa, može upotrebiti kao tip polja ili povratna vrednost upita ili mutacije.

#### 4. UPOREDNA ANALIZA

Opisani načini implementacije API-ja imaju neke sličnosti i dosta razlika. Ističe se razlika koja se odnosi na način zahtevanja podataka. Kao što je rečeno, REST svaki resurs i svaku operaciju nad istim posebno identifikuje kombinacijom URL-a i HTTP metoda i tipa sadržaja zahteva, dok GraphQL ima jedinstvenu pristupnu tačku za ceo skup podataka, dok se zahtevani podaci ili operacije nad njima specificiraju kroz upite ili mutacije. Dostupni resursi su strogo tipizirani kroz šemu, tako da se za svaki zahtev zna kakvog oblika će biti odgovor. Jedna od stvari koje izdvajaju GraphQL je mogućnost odabira polja zahtevanog tipa od strane klijenta. Prednosti ovakvog načina implementacije u odnosu na REST su:

- **Nema dobijanja nepotrebnih podataka:** u slučaju da klijent zahteva samo mali određen deo polja nekog entiteta, on će dobiti samo ono što je tražio. U slučaju REST-a, šalje se ceo skup podataka za traženi resurs. Ovo se može sprečiti otvaranjem nove ulazne tačke za taj određeni skup podataka, ali ako se taj skup podataka menja, mora se menjati i API, dok kod GraphQL-a to nije slučaj. Dodavanjem novih ulaznih tačaka za svaku moguću kombinaciju, taj API postaje praktično neodrživ. Ova pogodnost GraphQL-a posebno se oslikava kod mobilnih aplikacija gde treba uzeti u obzir tehnologiju preko koje klijent komunicira sa serverom (3G, 4G). Zbog toga, jako je bitno da saobraćaj preko mreže bude što manji, kako bi aplikacija dobila na performansama. Aplikacije koje su rađene po RESTful arhitekturnom stilu često imaju posebne verzije API-ja za veb i mobilne aplikacije iz ovog razloga, dok fleksibilnost koju pruža GraphQL omogućava razvoj jednog API-ja koji jednako dobro opslužuje i mobilne i veb aplikacije.
- **Nema nedostatka informacija po zahtevu:** u slučaju kada klijent želi da pročita više različitih resursa, on može pozvati više upita u istom zahtevu i na taj način može dobiti sve potrebne podatke odjednom. Kod REST-a ovo nije slučaj, već se mora slati zahtev po resursu. Na ovaj način GraphQL znatno dobija na performansama kada je vreme putovanja zahteva od klijenta do servera veliko, a broj resursa koji je potrebno pročitati relativno je veliki.

Ovi faktori utiču na vreme odziva API-ja. Eksperimentima [10] je utvrđeno da je za skupljanje podataka koji su iste strukture (isti resurs) i manjeg obima potrebno manje vremena sa REST API-em. Ipak, u slučaju kada je potrebno

preuzeti više podataka koji nisu nužno povezani, tada će API implementiran u GraphQL-u imati bolje performanse.

Ukoliko usled održavanja, unapređenja ili evoluiranjem aplikacije dođe do promene API-ja, postavlja se pitanje kako ova dva načina implementacije reaguju na ovu promenu. U slučaju REST-a, dolazi do takozvanog verzionisanja, gde se pravi nova verzija API-ja. Problem je što svi klijenti koji komuniciraju sa API-em treba da odreaguju na tu promenu, što u praksi nije tako lako izvodljivo. Zbog toga, najčešće se određeni vremenski period koriste dve verzije, što podrazumeva održavanje koje se udvostručuje. Kod GraphQL-a, fleksibilnost koju nudi kreiranje upita dozvoljava serveru da evoluiru bez verzionisanja, već da se menja u skladu sa potrebama. Pri tome, klijenti samo treba da prilagode svoje upite svojim potrebama, ako su se one promenile.

GraphQL koristi HTTP samo kao protokol za prenos informacija preko veba, ali ne koristi svojstva HTTP-a za dodavanje semantike na zahtev, već svu semantiku daje kroz specificiranje upita ili mutacije. Sa druge strane, REST se, kao što je već rečeno, oslanja na HTTP u velikoj meri. Zbog ovoga, aplikacije rađene po RESTful arhitekturnom stilu mogu iskoristiti sve prednosti HTTP-a. Jedna od funkcionalnosti je keširanje zahteva, gde se lako može dodati sloj koji bi keširao upite po jedinstvenom identifikatoru, što u slučaju REST-a predstavlja URL zajedno sa HTTP metodom. Prilikom čitanja podataka, tj. prilikom pozivanja operacije sigurnom metodom GET, sloj za keširanje može odmah odgovoriti na taj zahtev ukoliko je on već ranije izvršen (a u međuvremenu nije došlo do izmene podataka) i smanjiti vreme obrade zahteva. Pri velikoj opterećenosti servera, keširanje može značajno da utiče na performanse sistema, posebno kod aplikacija gde je mnogo češći scenario da klijent čita podatke nego da ih upisuje. Zbog toga što je svaki resurs globalno jedinstveno identifikovan URL-om, lako se može implementirati sloj za keširanje. GraphQL nema jedinstveni identifikator za resurs, i to znatno otežava uvođenje keširanja između više zahteva. Jedan od načina da se to prevaziđe je da svaki entitet ima identifikator koji je jedinstven na nivou sistema, pa se po njemu može implementirati i sloj za keširanje. [11] Takođe, mogu se keširati podaci po strukturi upita, ali ova metoda nije tako efikasna zbog fleksibilnosti strukture upita nad istim entitetom.

Broj API-ja koji su implementirani po REST-u i GraphQL-u još uvek nije uporedan. REST kao zreli arhitekturni stil ima mnogo veću primenu za sada, ali trend se značajno menja u korist GraphQL-a. Iz ugla odabira između ova dva načina implementacije, često se postavlja pitanje podrške zajednice i dostupnih alata koji ubrzavaju i olakšavaju implementaciju. REST i dalje ima veću podršku zajednice, ali se razlika sve više i više smanjuje. GraphQL dobija sve više biblioteka koji olakšavaju rad. Takođe, raste broj programskih jezika u kojima je data referentna implementacija, pa se vreme učenja smanjuje što značajno utiče na broj korisnika. Ono što posebno treba istaći su biblioteke koje su namenjene integraciji GraphQL-a sa klijentskom stranom aplikacije. Tu se izdvajaju Relay [12] i Apollo client [13], dve biblioteke koje integrišu klijentski



deo sa GraphQL-om. Relay biblioteka integriše React [14] aplikaciju sa GraphQL-om. Relay olakšava razvoj klijentske strane tako što posao prikupljanja podataka sa serverske strane preuzima na sebe za svaku React komponentu. Takođe, ima integrisan sistem za keširanje i mnoge druge optimizacije, pa se performanse poboljšavaju. Apollo client je biblioteka slična Relay biblioteci. Razlika je u tome što nije usko vezana za React, već podržava veći broj okvira za razvoj klijentskog dela aplikacije. Sa druge strane, i REST ima alate i okvire koji olakšavaju i ubrzavaju razvoj, i dodatnim ograničenjima dopunjuju mogućnosti i definiciju REST API-ja. Najznačajniji okvir za specifikaciju REST API-ja je OpenAPI specifikacija. Ova specifikacija daje format i ograničenja po kome se opisuje API, gde se uključuju ulazne tačke, dozvoljen skup metoda na tim tačkama, ulazni parametri za svaku operaciju i rezultati tih operacija, način autentikacije i drugi relevantni podaci. Ova specifikacija se piše u YAML ili JSON formatu, pa je lako mogu čitati i ljudi, a pogodna je i za računarsku obradu. Za rad sa OpenAPI specifikacijom najčešće se koristi Swagger [15], okvir koji sadrži skup alata koji olakšavaju i ubrzavaju implementaciju API-ja. Swagger pruža podršku prilikom definisanja specifikacije jer ima svoj editor koji je prilagođen pisanju specifikacije. Takođe, na osnovu specifikacije moguće je izgenerisati kod kako za serverski, tako i integracioni deo za klijentski deo aplikacije. Ovo omogućava Swagger codegen, alat koji na osnovu specifikacije može generisati aplikaciju u više različitih popularnih tehnologija i tako značajno ubrzati razvoj aplikacije. Swagger takođe može na osnovu date specifikacije omogućiti direktno korišćenje kroz Swagger UI, alat kome se pristupa iz veb pretraživača i koji daje priliku klijentima da pročitaju podatke iako nemaju aplikacionu logiku klijenta kod sebe. Što se testiranja tiče, Swagger inspector je alat koji testira API, proverava da li su odgovori servera korektni u skladu sa onim što po specifikaciji server treba da vrati i beleži istoriju testiranja. Ono što je interesantno je da se ovaj alat može prilagoditi i GraphQL i SOAP veb servisima i testirati i njih uspešno.

Uspešnost API-ja pored dobrih performansi zavisi i od toga koliko je lako korisnicima toga API-ja da ga koriste. Zbog toga, veoma bitna stavka u ovoj analizi je i dokumentacija API-ja. Kod REST API-ja, svaki URL u kombinaciji sa HTTP metodom predstavlja neku ulaznu tačku, gde je potrebno dokumentovati šta ta tačka predstavlja, njene parametre, povratnu vrednost, način autentikacije i dr. Uz pomoć dostupnih alata, ovaj posao postaje znatno lakši, posebno koristeći Swagger ili RAML, kod kojih je moguće definisati specifikaciju API-ja i na osnovu koje onda alat daje kompletnu dokumentaciju API-ja. Još jedna stvar koju treba imati u vidu je HATEOAS, preduslov za REST koji dinamički „otkriva“ moguće akcije nakon trenutnog zahteva. Zbog toga je nekad moguće i koristiti API koji nije dobro dokumentovan, ako je HATEOAS implementiran na odgovarajući način. Sa druge strane, GraphQL ima jednu ulaznu tačku, ali je potrebno dokumentovati sve moguće upite i mutacije, kao i moguće tipove. U tu svrhu, koristi se sistem introspekcije, mogućnosti postavljanja upita o osnovnim podacima u šemi. Svaka GraphQL šema metapodatke, gde spadaju predefinisani introspektivni

tipovi i mogući upiti, pomoću kojih se mogu saznati podaci o samoj šemi, tipovima, upitima i mutacijama. Postoje razne biblioteke koje se oslanjaju na introspekciju i kreiraju potpunu dokumentaciju GraphQL API-ja, koja se može izložiti i omogućiti korisnicima API-ja lakše korišćenje.

## 5. ZAKLJUČAK

U vremenima kada se količina podataka koja se prenosi preko mreže između različitih uređaja svakodnevno povećava, pri projektovanju aplikacija potrebno je naći odgovarajući način za izlaganje resursa. To se najčešće obezbeđuje kreiranjem veb servisa koji se izlažu pomoću API-ja. U ovom radu dat je prikaz osnovnih karakteristika dva najpopularnija načina implementacije veb API-ja. REST, kao arhitekturni stil daje smernice i ograničenja prema kojima se razvoj API-ja upravlja. Sa druge strane, GraphQL predstavlja okvir koji obuhvata specifikaciju i upitni jezik pomoću kojih se implementira API i omogućava interakcija sa njim. Takođe, data je uporedna analiza nekih osnovnih karakteristika, gde su iznete prednosti i mane u cilju boljeg razumevanja ova dva načina implementacije.

Dalji pravci istraživanja na ovu temu bili bi mogućnost kombinovanja ova dva pristupa, tj. kako da se izvuku dobre osobine iz oba a da se premoste loše. Takođe, ukoliko se API implementira na jedan način, promena načina implementacije nije jednostavna, tj. zahteva mnogo resursa, što odabir načina implementacije API-ja čini bitnom odlukom. Rad na transformaciji jednog u drugi način bi relativizovao ovu odluku. Prevedljivo transformacija iz REST-a u GraphQL zbog veće broja API-ja koji su rađeni u REST-u, a kasnije i inverzna transformacija.

## LITERATURA

- [1] R. T. Fielding, „Architectural Styles and the Design of Network-based Software Architectures,“ University of California, Irvine, 2000.
- [2] „GraphQL users,“ [Na mreži]. Available: <http://graphql.org/users/>. [Poslednji pristup 2 January 2018].
- [3] O. Hartig i J. Pérez, „An Initial Analysis of Facebook’s GraphQL Language,“ u *11. AMW 2017*, Montevideo, 2017.
- [4] Facebook, „GraphQL scalar types,“ [Na mreži]. Available: <http://graphql.org/learn/schema/#scalar-types>. [Poslednji pristup 2 January 2018].
- [5] Facebook, „GraphQL specification,“ October 2016. [Na mreži]. Available: <http://facebook.github.io/graphql/October2016/>. [Poslednji pristup 2 January 2018].
- [6] F. Belqasmi, J. Singh i S. Y. B. Melhem, „SOAP-Based vs. RESTful Web Services: A Case Study for Multimedia Conferencing,“ *IEEE Internet Computing*, t. 16, br. 4, pp. 54 - 63, 2012.

- [7] M. Fowler, „Richardson Maturity Model,“ 18 March 2010. [Na mreži]. Available: <https://martinfowler.com/articles/richardsonMaturityModel.html>. [Poslednji pristup 2 January 2018].
- [8] Swagger, „OpenAPI specification,“ [Na mreži]. Available: <https://swagger.io/specification/>. [Poslednji pristup 2 January 2018].
- [9] RAML, „RAML,“ [Na mreži]. Available: <https://raml.org/>. [Poslednji pristup 2 January 2018].
- [10] A. F. Helgason, „Performance analysis of Web Services: Comparison between RESTful & GraphQL web services,“ University of Skövde, Skövde, 2017.
- [11] Facebook, „GraphQL caching,“ [Na mreži]. Available: <http://graphql.org/learn/caching/>. [Poslednji pristup 2 January 2018].
- [12] Facebook, „Relay,“ [Na mreži]. Available: <https://facebook.github.io/relay/>. [Poslednji pristup 2 January 2018].
- [13] Apollo, „Apollo client,“ [Na mreži]. Available: <https://www.apollographql.com/client>. [Poslednji pristup 2 January 2018].
- [14] Facebook, „React,“ [Na mreži]. Available: <https://reactjs.org/>. [Poslednji pristup 2 January 2018].
- [15] Swagger, „Swagger,“ [Na mreži]. Available: <https://swagger.io/>. [Poslednji pristup 2 January 2018].

# TEHNIKE ZAŠTITE ANDROID APLIKACIJA I KODA OD OBRNUTOG INŽENJERINGA

## ANDROID APPLICATION AND REVERSE ENGINEERING PROTECTION TECHNIQUES

Petar Ljubić<sup>1</sup>, Bratislav Predić<sup>1</sup>, Miloš Roganović<sup>3</sup>

*Elektronski fakultet u Nišu<sup>1</sup>  
Fakultet zaštite na radu Niš<sup>2</sup>*

**Sadržaj** - U ovom radu biće opisani postojeći alati za zaštitu Android bajt koda, kao i alati za dekompajliranje izvršnih fajlova i biblioteka, koji za cilj imaju prikaz izvornog koda i resursa neke aplikacije. Cilj ovog rada jeste da se kroz primere trenutnih alata ukaže na njihove mogućnosti, funkcionalnosti, ali i nedostatke, prikažu slabe tačke i predlože izmene i dopune.

**Abstract** - This document will describe existing tools for Android byte code protection, as well as the tools for decompiling executables and libraries whose main purpose is to show the source code and resources of an application. The aim of this paper is to show existing tools' strengths through examples, but also to point out flaws and weak spots, as well as to suggest improvements.

### 1. UVOD

Svedoci smo postojanja trenda promene tehnologija i brzih prelaska sa jednih računarskih platformi na druge. Poslednjih godina ovaj trend obeležava prelazak sa desktop računara na mobilne uređaje. U globalnoj slici dostupnih platformi, Android platforma se ističe kao trenutno najpopularnija i najzastupljenija platforma na mobilnim uređajima, i njena popularnost ne prestaje da raste. Samim tim, ova platforma biva eksploatisana od strane programera koji pišu *malware* programe ili koriste *software* koji je dobijen nezakonitim putem uz pomoć obrnutog inženjeringa (*reverse engineering*).

Obrnuti inženjering se u Android operativnom sistemu najčešće izvodi nad izvršnim fajlom (*Android Application Package - APK*) koji služi za distribuciju i instaliranje mobilnih aplikacija. *APK* fajl je tip arhiviranog fajla, i vrlo lako se može otvoriti uz pomoć različitih programa za dearhiviranje (npr. *7zip*). Jednostavnim korišćenjem programa za čitanje arhiviranih fajla ili promenom ekstenzije *.apk* u *.zip* moguće je utvrditi da se sam *APK* fajl sastoji od niza foldera i drugih fajlova koji u sebi sadrže kriptovane i ne kriptovane fajlove kreirane od strane programera. Među dostupnim fajlovima u *APK*-u nalazi se i *classes.dex* fajl. Ovaj fajl je razumljiv *Dalvik* i drugim virtualnim mašinama i sadrži bajt kod koji te virtualne mašine izvršavaju. Samim tim, *classes.dex* fajl je od

izuzetnog značaja za temu koja će biti obrađena u ovom radu.

Upotrebom nekog od alata za analizu bajt koda koji su kao *open source* rešenja dostupni na internetu (npr. *Dex2jar*, *Dexdump* i dr.) moguće je ovaj fajl konvertovati u *.jar* fajl koji predstavlja biblioteku *Java* koda. Sadržaj ovog fajla je nerazumljiv za običnog korisnika, a razlog tome je taj što sadržaj fajla čini kompajliran kod. Ipak, na internetu se može naći nekoliko *open source* rešenja koja uspešno vrše dokompajliranje ovakvih fajlova. Jedno od tih rešenja jeste *JD-GUI*.

Praćenjem opisanih koraka raspakivanja i dekompajliranja *APK* i *.dex* fajla, respektivno, potencijalnom napadaču je dostupan niz *java* fajlova koje je programer napisao ili koristio u sklopu njemu dostupnih biblioteka. Ovi fajlovi u sebi nose izvorni kod koji se od originalnog razlikuje u zavisnosti od tehnike kompajliranja istog. Ukoliko programer nije koristio neki od postojećih alata za maskiranje (*obfuscation*), dekompajlirani kod će biti jako sličan originalnom kodu.

U svrhu zaštite među koda za različite platforme, klasa programerskih tehnika poznata pod nazivom *code obfuscation* pokušava da preventivno deluje i zaštititi intelektualnu svojinu propuštajući kod aplikacije kroz set metoda kako bi izlazni kod bio optimizovaniji, i što je bitnije, nerazumljiv potencijalnim napadačima. Ovaj proces se obavlja prilikom kompajliranja koda i kao rezultat ima neuporedivo veliku razliku između originalnog koda programera, i koda dostupnog tehnikom dekompajliranja koja je opisana u tekstu.

U ovom radu biće predstavljeni postojeći alati za zaštitu koda od obrnutog inženjerstva (poglavlje 2), zatim će kroz niz primera biti prikazane mane i nedostaci istih. U trećem poglavlju biće prikazan predlog novog alata za zaštitu koda sa adekvatnim primerima koji ilustruju njegov uticaj na kompajliran kod koji je potencijalno vidljiv napadaču. Četvrto poglavlje ovog rada baviće se performansama predloženog alata, dok će peto poglavlje sadržati opšti zaključak i buduće pravce i korake u zaštiti Android aplikacija i koda.

## 2. ZAŠTITA ANDROID BAJT KODA

U razvoju softvera, *obfuscation* je namerni čin stvaranja izvornog ili mašinskog koda koji čovek teško može da razume. Ovakav proces zaštite korišćen je i u svrhu zaštite poruka, kada su reči ili slova poruke menjana tako da se bez posedovanja rečnika teško može razumeti smisao teksta. Programeri mogu namerno promeniti kod kako bi sakrili njegovu svrhu, njegovu logiku ili implicitne vrednosti ugrađene u njega, a pre svega, kako bi se sprečilo neovlašćeno obrnuto inženjerstvo. Ovo se može uraditi ručno ili uz pomoć automatizovanog alata.

Među najpoznatijim alatima za maskiranje koda može se naći nekoliko tehnika koje su prisutne u svim alatima, i to su:

- Uklanjanje belina (*whitespace*), koja predstavlja trivijalan način maskiranja i zasniva se na uklanjanju svih nepotrebnih razmaka i praznih linija iz fajla u kome se nalazi izvorni kod.
- Zamena imena promenljivih predstavlja jednu od najučinkovitijih tehnika maskiranja koda, a najčešći način maskiranja se zasniva na jednostavnoj zameni imena promenljivih kratkim i nerazumljivim imenima, tako da je bez odgovarajuće dokumentacije (rečnika) praktično nemoguće otkriti algoritam ne trivijalnih programa.
- Zamena toka rada programa omogućava promene toka algoritma na nekim mestima na kojima je ta mogućnost pogodna. Neki alati za maskiranje, kao što je *Allatori*, menjaju standardne *Java* konstrukcije kao što su petlje, uslovi i instrukcije grananja, i u slučajevima gde je to moguće, serije komandi. Time se postiže da se nakon dekompajliranja kod učini gotovo nečitljivim.

Obfuskacija kao tehnika zaštite se u Android aplikacijama primenjuje na nivou izvornog koda ili nivoa bajt koda. Postoji nekoliko alata koji se široko koriste u svrhu zaštite, među kojima su najpoznatiji i najpopularniji analizirani u nastavku.

*ProGuard* je najpopularniji *optimizer java* bajt koda. Osnovna uloga ovog *optimizer-a* jeste smanjivanje veličine izvršnog fajla aplikacije i njena optimizacija u smislu ubrzanja rada. Prema podacima koji su dostupni na oficijalnom sajtu ovog *optimizer-a* [1], *ProGuard* čini izvršni fajl do 90 % manjim, odnosno čini da program radi do 20 % brže.

Prema autorima rada [2] *ProGuard* vrši proveru i verifikaciju bajt koda kada se učitaju *.classes* fajlovi, da bi se potvrdilo da programski kod ne može naškoditi radu same virtuelne mašine koja kod treba da izvrši. Kako navode autori, ovaj proces pridodaje informacije o verifikaciji *.class* fajlovima, čime proces verifikacije

fajla čini jednostavnijim, omogućavajući *.class* fajlovima brže i efikasnije učitavanje.

*Allatori* je komercijalni produkt koji je razvila kompanija Smardec. Pored tehnike maskiranja koda koju implementira *ProGuard*, *Allatori* poseduje funkcije za modifikovanje programskog koda. Konstrukcije petlje su isečene na takav način da alati za obrnuto inženjerstvo ne mogu da ih prepoznaju. Ovim pristupima algoritmi bivaju manje čitljivi i dobijaju na dužini inače kompaktni fragmenti kodova. Pored toga, stringovi su maskirani i dekodirani tokom izvršavanja. Maskiranje uključuje poruke i imena koja su obično čitljiva za čoveka i dala bi dobre predloge ljudima koji pokušavaju da razumeju smisao koda.

Metode maskiranja koje se koriste u *Allatori-u* su superset *ProGuard-a*, što omogućava bolju zaštitu koda u odnosu na izvorni *ProGuard* alat. Kako navode autori u [3], ovaj alat pored osnovne zaštite koju poseduje *ProGuard*, vrši redukciju *.dex* fajla, poboljšanje brzine rada *APK* fajla, smanjenje zauzete memorije, otklanjanje viška koda, kao i enkripciju stringova i njihovu dekripciju u realnom vremenu.

Kompanija koja je razvila za sada najpopularniji alat za maskiranje koda, *ProGuard*, 2014. godine razvila je unapređenu verziju *DexGuard*, koja se zasniva na ranijoj verziji ovog alata, i koja, za razliku od *ProGuard-a*, nije besplatna. Kako navode autori u [4], ovaj alat, pored osnovne zaštite koju nudi *ProGuard*, omogućava i enkripciju stringova, assets fajlova i biblioteka, kao i enkripciju klasa. Prema ovim autorima, najznačajnija razlika između dve verzije alata za zaštitu koje kompanija *Eric Lafortune* nudi jeste kombinacija enkripcije stringova sa automatskom refleksijom.

Na slici 1. prikazan je primer *Java* koda koji predstavlja implementaciju funkcije koja će se pozivati na određenu akciju klika. Ova funkcija poziva funkciju *exit*, klase *System*, prosleđujući kao argument vrednost 0.

```
public void onClick(DialogInterface arg2, int arg3) {
    System.exit(0);
}
```

Slika 1. Originalni kod

Nakon što *DexGuard* izvrši proces automatske refleksije nad prikazanim kodom, kod će izgledati kao na slici 2.

```

public void onClick(DialogInterface arg2, int arg3) {
    try {
        Class.forName
        ("java.lang.System")
        .getMethod("exit", Integer.TYPE)
        .invoke(null, Integer.valueOf(0));
    } catch (Throwable throwable) {
        throw throwable.getCause();
    }
}

```

Slika 2. Izvorni kod nakon automatske refleksije

Prateći predložene korake autora [4] i uvodeći dodatnu, opcionu, zaštitu enkripcije stringova, kod će u izvršnom fajlu biti upisan kao na slici 3.

```

public void onClick(DialogInterface arg2, int arg3) {
    try {
        Class.forName
        (COn.`{-COn.`[0xC],COn.`[0x12],COn.`[0x10])
        .getMethod(COn.`(11, 12, 12 | 6), Integer.TYPE)
        .invoke(null, Integer.valueOf(0));
    } catch (Throwable throwable) {
        throw throwable.getCause();
    }
}

```

Slika 3. Izvorni kod nakon enkripcije stringova

Kako se navodi u radu [5] nijedan alat za maskiranje koda nije savršen. I pored očigledno velike zaštite koju pruža komercijalna verzija alata *DexGuard*, u radu [5] se navodi da postoje 3 osnovna koraka koja omogućavaju obrnuti inženjering nad zaštićenim kodom, i to su:

- „DexGuard decryption python script.“ [6],
- Logovanje [7],
- Preimenovanje stringova [8].

I pored opisanih koraka, postojeća rešenja ne nude adekvatnu zaštitu povodom sakrivanja argumenata koji se prosleđuju funkciji prilikom izvršavanja. Primera radi, bez obzira koji alat za maskiranje koristili, u dekompileiranom kodu uvek možemo lako videti koliko argumenata ima pozvana funkcija, lako možemo razaznati povratnu vrednost funkcije, i na posletku, ukoliko argumenti nisu tekstualnog tipa, uočiti njihove vrednosti.

### 3. PREDLOG DODATNOG NIVOA ZAŠTITE - MASCOT

MASCOT (*Master Android Security Code Obfuscation Technique*) predstavlja novi predlog zaštite koda od obrnutog inženjeringa.

MASCOT predstavlja nadogradnju trenutno najpopularnijeg alata za maskiranje koda, *ProGuard* i taj sistem zaštite koristiti kao komponentu. Dodatni sistem zaštite omogućen je korišćenjem karakteristike Java programskog jezika da se na osnovu imena funkcija i promenljivih njima može pristupiti korišćenjem refleksije.

Osnovne funkcionalnosti prezentovanog alata jesu:

- Detektovanje sekvenci koda koje treba zaštititi novim alatom.
- Prepoznavanje vrednosti ugrađenih u izvorni kod (hard-coded) stringova unutar koda, proveranje mogućnosti zaštite istog i zaštita tih vrednosti.
- Lociranje svih poziva funkcija u sekvencama koda koje treba zaštititi.
- Čuvanje neophodnih podataka u kriptovanom fajlu i zamena poziva funkcije novom funkcijom koju implementira MASCOT.

U svrhu poboljšanja performansi samog sistema, a takođe i želje da se programeru omogući veća kontrola nad radom alata, uvedena su pravila koja bi kontrolisala uticaj alata na kod. Naime, uvođenjem komentara predefinisano formata, koji bi označavali početak i kraj neke sekcije, MASCOT zna koji deo koda treba da obradi, a koji ne.

Postupak obrade String vrednosti koje imaju hard-code vrednost kroz izvorni kod počinje proverom :

- Vrednost ne sme biti globalno inicijalizovana
- Vrednost ne sme biti final

Promenom gore navedenih slučajeva narušio bi se koncept Java koda i pre kreiranja APK fajla korisnik bi dobio određene greške u konzoli. Nakon izdvajanja slučajeva koji se mogu refaktorirati, vrednosti stringova se zamenjuju pozivom funkcije MASCOT alata koja će iz novog, kriptovanog fajla, na osnovu prosledene linije fajla, pročitati i dekriptovati vrednost stringa i proslediti je nazad kao povratnu vrednost funkcije. Primer uticaja MASCOT alata na izgled koda prikazan je na slici 4.

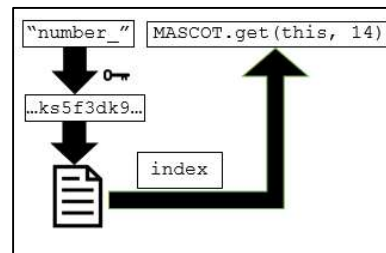
```

/*Originalni kod*/
String a = "number_" + b;
/*Kod zasticen novim alatom*/
String a = MASCOT.get(this, 14) + b;

```

Slika 4. Uticaj alata na stringove u kodu

Tok maskiranja *hard-coded* vrednosti dat je na slici 5.



Slika 5. Tok zaštite Stringa

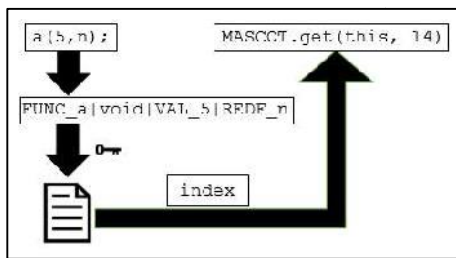
Kada se u sekvencama koda koji treba zaštititi nađe poziv neke funkcije, novi alat za maskiranje koda uzima ime funkcije, povratnu vrednost funkcije, i argumente koji su prosledjeni funkciji. Ti podaci se

čuvaju u jednoj liniji kriptovanog fajla. Na mestu poziva funkcije koja se obrađuje upisuje se poziv funkcije alata za maskiranje, kome se prosleđuje linija u kriptovanom fajlu u kojoj su upisane sve potrebne informacije. Primer koda pre i posle upotrebe alata dat je na slici 6.

```
/*Originalni kod*/
result = randomMultiple(number, randomNuber);
/*Kod zasticen novim alatom*/
result = MASCOT.get(this,6);
```

Slika 6. Uticaj alata na pozive funkcija

Posmatrajući slike 4 i 6, možemo uočiti da je poziv funkcije koja vraća string i poziv MASCOT funkcije koja zamenjuje funkciju iz originalnog koda identičan. Potencijalnom napadaču nakon dekriptovanja koda neće biti jasno da li je prosleđena vrednost nastala izvršenjem neke funkcije ili jednostavnim čitanjem string vrednosti iz fajla. Takođe, uočljiva je razlika u implementaciji MASCOT alata i *DexGuard* alata. Naime, broj argumenata funkcije i same vrednosti istih nisu vidljivi u kodu što u mnogome može otežati posao potencijalnom napadaču i kada on bude znao da se radi o izvršenju neke funkcije. Tok rada alata za maskiranje funkcija u kodu dat je na slici 7.



Slika 7. Tok zaštite poziva funkcija

Sam fajl koji nosi neophodne informacije poštuje specifična pravila upisa podataka kako bi se prilikom čitanja fajla znalo da li se radi o pozivu funkcije, da li su argumenti realne vrednosti ili reference na neku vrednost, da li je sam argument funkcije poziv neke nove funkcije i sl. Jedna linija u fajlu predstavlja ulazno-izlazni podatak za poziv funkcije *get* MASCOT alata. Ako određena linija u fajlu nosi vrednost nekog Stringa, onda je struktura te linije koda:

STR\_<vrednost>

Pri čemu je vrednost ono što se prosleđuje kao povratna vrednost funkcije.

Ako linija fajla nosi informaciju o pozivu funkcije, ta linija je zapisana u sledećem obliku:

FUNC\_<ime\_funkcije><povratna\_vrednost>[argumenti ...]

Pri čemu su argumenti opcioni, jer neke funkcije nemaju argumente. Sami argumenti ispred sebe mogu imati prefiks *VAL*, *REF* ili *FUNC* što opisuje da li je u

fajlu upisana realna vrednost, ime atributa ili se radi o ponovnom pozivu neke funkcije.

Fajl je lociran u *assets* folderu projekta i u taj folder je upisan prilikom kompajliranja i kreiranja APK fajla. Sadržaj ovog fajla kriptovan je AES kriptom algoritmom. U zavisnosti od prirode same aplikacije, šifra za kriptovanje i dekriptovanje se može nalaziti na dve lokacije:

- U .so fajlu unutar APK-a
- Na serveru, zajedno sa kriptovanim fajlovima

Lokacija šifre koja vrši enkripciju i dekripciju podataka može zavisiti od same prirode aplikacije koja se štiti MASCOT alatom od obrnutog inženjerstva. Naime, ukoliko aplikacija iziskuje konstantnu konekciju sa nekim serverom, na tom istom serveru mogu se naći kriptovani fajlovi i šifre neophodne za rad same aplikacije. Korišćenjem *https* protokola uz osnovnu zaštitu samih podataka na serverskoj strani, moguće je ostvariti dodatnu zaštitu samih podataka. Alati poput *ApkTool*-a mogu dekodirati resurse u gotovo originalan oblik i obnoviti ih nakon što izvrše određene modifikacije. Na taj način čuvanje podataka od značaja u *resource* fajlovima unutar projekta postaje besmisleno. Stoga je osnovna zaštita koju nude mrežni protokoli poput *https*-a znatno bolja.

Ukoliko aplikacija ne iziskuje konstantnu konekciju sa nekim serverom, ili je aplikacija u potpunosti u *offline* modu, šifra za enkripciju i dekripciju podataka se čuva u .so fajlu unutar APK-a. Ovaj fajl predstavlja izvršni fajl koda koji je pisan u C ili C++ programskom jeziku i koji se uz pomoć *Android Native Develop Kit*-a (NDK) izvršava na *Dalvik* virtualnoj mašini. Ono što ovaj fajl izdvaja u odnosu na ostale fajlove koji se mogu naći u projektu jeste otpornost na pokušaje dekripcije. Pre kompajliranja koda i kreiranja APK fajla, MASCOT alat kreira fajl sa ekstenzijom *.cpp* i u njega upisuje kod prikazan na slici 8.

```
Java_com_example_getKey( JNIEnv* env, jobject this )
{
    return (*env)->NewStringUTF( env, "myKey". );
}
```

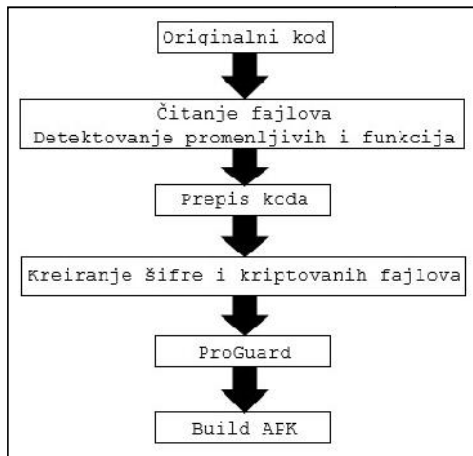
Slika 8. Kod iz koga nastaje .so fajl

Pri tome se sama vrednost ključa generiše i upisuje u fajl u trenutku njegovog kreiranja, i pri svakom kompajliranju i kreiranju novog APK fajla se menja.

MASCOT alat je zamišljen kao dopuna sistema zaštite koji poseduje *ProGuard* alata. Razlog izbora *ProGuard* alata u odnosu na ostale alate jeste njegova pristupačnost (*ProGuard* je osnovni nivo zaštite u najpopularnijem i oficijalnom razvojnom okruženju Android aplikacija) i njegova cena (alat je u potpunosti besplatan). Obzirom da *ProGuard* alat nije *open source*, njegova implementacija unutar MASCOT alata zasniva se na jednostavnom pozivanju *ProGuard* nad



kodom koji je prethodno obrađen uz pomoć MASCOT-a. Tok rada MASCOT alata prilikom kompajliranja koda i kreiranja APK fajla dat je na slici 9.



Slika 9. Tok rada MASCOT alata

#### 4. ANALIZA PERFORMANSI

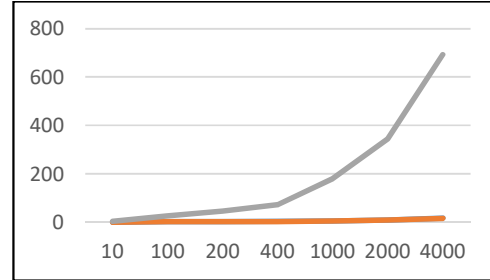
Refleksija kao osobina Java programskog jezika je uticala na razvoj velikog broja popularnih alata i biblioteka koje se koriste u programiranju Android aplikacija. Veliku primenu Java refleksije možemo naći kod biblioteka i alata koje služe za konverziju *json* i *xml* fajlova u modele klasa. Jedni od najpopularnijih alata tog tipa svakako jesu *Gson* i *Jackson* koji uz pomoć kroz parsere detektuju određena imena atributa unutar *json* i *xml* fajlova, i u prosleđenim klasama pronalaze i inicijalizuju promenljive tog imena.

Ipak, proces pronalaženja odgovarajućeg atributa neke klase, i proces njegove inicijalizacije, gledano kroz prizmu performansi sistema, predstavljaju najveću manu refleksije u Java programskom jeziku. Cena univerzalnosti parsera i funkcionalnosti Refleksije plaćena je kroz veliko vreme izvršavanja osnovnih funkcionalnosti.

Na slici 10 prikazan je graf koji prikazuje uticaj refleksije na performanse MASCOT alata opisanog u ovom radu. Naime, uz pomoć logovanja vremena izvršen je test performansi aplikacije koja ne sadrži nikakvu zaštitu, koja sadrži *ProGuard* zaštitu, i koja sadrži MASCOT sistem. Vrednosti x ose na grafu predstavljaju broj uzastopnih poziva neke metode iz koda. Broj uzastopnih poziva kreće se od 10 do 4000. Po y osi prikazanog grafa nalazi se vreme u mili sekundama (ms) potrebno za izvršenje metode. Narandžastom bojom prikazana je kriva koja predstavlja performanse aplikacije zaštićene *ProGuard* alatom, dok su sivom bojom prikazane performanse aplikacije zaštićene MASCOT alatom.

Iz datog grafa može se zaključiti da bi izvršenje velikog broja funkcija uz pomoć refleksije moglo da uspori aplikaciju na čak nekoliko sekundi. Ovakav scenario je izuzetno moguće ukoliko se u kodu nađe *for*

petlja koja će određenu metodu pozivati veliki broj puta.



Slika 10. Uticaj refleksije na performanse sistema

Na slici 11 dat je tabelarni prikaz vremena izvršenja određenog broja iteracija u zavisnosti od primenjene zaštite.

Broj iteracija	Bez zaštite (ms)	ProGuard (ms)	MASCOT (ms)
10	0.1	0.1	4
100	2.3	1.6	26
200	2.6	2.2	46
400	3.4	2.3	72
1000	5	4.6	180
2000	9	8.1	344
4000	17	16	693

Slika 11. Prikaz vremena izvršenja

Iz datog grafa i tabele se može zaključiti da li MASCOT alat treba upotrebiti u određenoj aplikaciji. Naime, upotrebnost ovog alata zavisi od samih aplikacija u kojima bi alat trebalo primeniti. Ukoliko posmatramo sam rad aplikacije i izračunamo prosečan broj poziva metoda koje bi se izvršavale uz pomoć ovog alata, možemo izvući zaključak da li je ovaj alat primenljiv u aplikaciji ili ne. Proučavajući gore opisan graf možemo zaključiti sledeće: Ako aplikacija po sesiji (interakciji korisnika) ima kao prosečan broj izvršenja metoda vrednost do 100 poziva, možemo izvesti zaključak da je alat primenljiv u toj aplikaciji jer kašnjenje od 100 ms po sesiji neće frustrirati uticati na samog korisnika. Ipak, ukoliko je taj broj veći od 100 poziva, postoji rizik od izazivanja nezadovoljstva kod korisnika aplikacije. Sa druge strane, i pored loših performansi sistema, korišćenje ovog alata je opravdano ukoliko je od izuzetne važnosti sačuvati kod od napada obrnutim inženjeringom. Aplikacije koje bi morale razmotriti upotrebu ovog alata su aplikacije koje rade sa platnim računima, kreditnim karticama i sl.

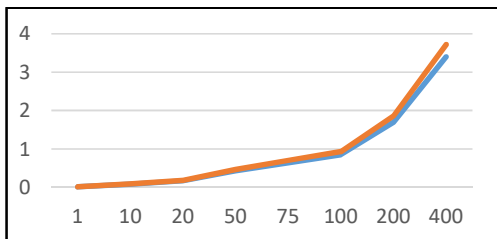
U svrhu smanjenja vremena koje je aplikaciji potrebno kako bi izvršila kod koji je zaštićen opisanim alatom, programer bi trebao pratiti primere dobrih praksi prilikom pisanja koda koji će sadržati MASCOT zaštitu. Prva i najvažnija praksa koju bi programer trebao da sledi jeste korišćenje sekcija za kontrolisanje

rada alata. Naime, ukoliko programer proceni da određeni segmenti koda ne iziskuju zaštitu MASCOT alatom, već je sama zaštita koju pruža *ProGuard* alat zadovoljavajuća, treba iskoristiti sekcije za kontrolu MASCOT alata kako bi taj segment koda isključio iz sistema napredne zaštite. Time bi se vreme izvršenja programa značajno ubrzalo jer se ne bi štitilo nepotreban kod. Ukoliko bi se neki kod koji pak treba da bude zaštićen našao unutar neke petlje, potencijalno je moguće da će se kod izvršavati duže nego što je očekivano, i iz tog razloga, dobra praksa bi bila da se kod petlje stavi u posebnu funkciju koja bi se pozivala kao zaštićen kod. Primer takvog koda dat je na slici 12.

<pre> /*Loša praksa*/ for(;;){     if(someFunc())         break; }  /*Rezultat loše prakse*/ for(;;){     if(MASCOT.get(this,5))         break; } </pre>	<pre> /*Dobra praksa*/ private void tmpFunc(){     for(;;){         if(someFunc())             break;     } } /*Dobra praksa*/ MASCOT.get(this,5); </pre>
--	---

Slika 12. Prikaz loše i dobre prakse.

Poštovanjem dobre prakse i predloženog načina pisanja koda, mogu se postići velika poboljšanja u performansama. Graf koji prikazuje performanse sistema koji poštuje predloge dobre prakse dat je na slici 13.



Slika 13. Prikaz performansi sistema koji prati dobru praksu pri pisanju koda.

## 5. ZAKLJUČAK

U ovom radu obrađene su tehnike zaštite Android koda od obrnutog inženjerstva. Prikazani su postojeći sistemi zaštite i predstavljene njihove karakteristike. Ovaj rad sadrži primere korišćenja postojećih alata, kao i ocenu stepena zaštite koju pružaju. Kao odgovor na nedostatke postojećih rešenja, u ovom radu je predstavljen alat koji bi u mnogome mogao da reši postojeće mane i unapredi zaštitu koda u celosti. Pored osnovnih funkcionalnosti predloženih izmena, u ovom radu su prikazane performanse ponuđenog rešenja, kao i metode poboljšanja istih.

U svetu programiranja idealna zaštita ne postoji, i sa pravom se može reći da nikada neće postojati u

potpunosti bezbedan sistem. Prema tome, predloženi alat, kao i svi ostali, nije idealan, i pogodan je za dalja unapređenja koja bi se mogla kretati u smeru poboljšanja sistema refleksije i eventualne zamene iste. Takođe, alat bi mogao biti dopunjen jačom zaštitom samih fajlova koji su kriptovani, i moguće je unaprediti alat sistemom zaštite podataka koji se čuvaju u memoriji u toku rada programa, koji predstavljaju potencijalnu metu prilikom *real time* napada.

## LITERATURA

- [1] Lafortune, E. P. (n.d.). ProGuard. (GuardSquare, Leuven, Belgium) Retrieved from <https://www.guardsquare.com/en/proguard>
- [2] Harrison, R. (2015). Investigating the effectiveness of obfuscation against Android application reverse engineering. Royal Holloway University of London, Tech. Rep. RHUL-MA-2015-7.
- [3] Faruki, P., Fereidooni, H., Laxmi, V., Conti, M., & Gaur, M. (2016). Android Code Protection via Obfuscation Techniques: Past, Present and Future Directions. arXiv preprint arXiv:1611.10231.
- [4] Strazzere, T., & Sawyer, J. (2014). Android hacker protection level 0. DEF CON, 22..
- [5] Apvrille, A., & Nigam, R. (2014). Obfuscation in android malware, and how to fight back. Virus Bulletin, 1-10.
- [6] Fallière, N. (2013, April 2). A look inside DexGuard. Retrieved from PNF software: <https://www.pnfsoftware.com/blog/a-look-inside-dexguard/>
- [7] Gruver, B. (n.d.). GitHub – JesusFreke baksmali. Retrieved from <https://github.com/JesusFreke/smali>
- [8] Apvrille, A. (2013). Playing hide and seek with Dalvik executables. Hacktivity, Budapest, Hungary.
- [10] Suzumura, T., Takase, T., & Tatsubori, M. (2005, July). Optimizing web services performance by differential deserialization. In Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on (pp. 185-192). IEEE.
- [11] Chiba, S. (2000, June). Load-time structural reflection in Java. In European Conference on Object-Oriented Programming (pp. 313-336). Springer, Berlin, Heidelberg.
- [12] "How to store the Credentials securely in Android," 17 June 2016. [Online]. Available: <https://www.darwinrecruitment.com/blog/2016/06/store-credentials-securely-in-android>. [Accessed 15 January 2018].



# ИМПЛЕМЕНТАЦИОНИ ДЕТАЉИ АЛГОРИТМА ШИФРОВАЊА CRYPTO1

## IMPLEMENTATION DETAILS OF THE STREAM CIPHER CRYPTO1

Марко Мићовић<sup>1</sup>, Урош Раденковић<sup>1</sup>, Владимир Јоцовић<sup>1</sup>,  
Тамара Шекуларац<sup>1</sup>, Филип Хаџић<sup>1</sup>, Живојин Шуштран<sup>1</sup>, Дражен Драшковић<sup>1</sup>

*Електротехнички факултет Универзитета у Београду<sup>1</sup>*

**Садржај** – Сигурност *Mifare Classic* паметне картице заснива се на тајности коришћеног сигурносног протокола. Истраживачки тимови из Холандије и Немачке су помоћу реверзног инжењеринга открили детаље криптографског алгорита који користи *Mifare Classic* паметна картица. Након објављивања детаља алгорита шифровања CRYPTO1, предложени су бројни напади на *Mifare Classic* паметну картицу. Овај рад садржи имплементационе детаље алгорита шифровања CRYPTO1, указује његове највеће сигурносне пропусте и даје кратак преглед неких од најопаснијих напада.

**Abstract** – The Mifare Classic smart card security mechanisms are based on the secrecy of the security protocol. The proprietary cryptographic algorithm used by the Mifare Classic has been reverse engineered by research groups from Netherlands and Germany. Both groups made their results public. Following the disclosure of proprietary stream cipher CRYPTO1, numerous attacks on the Mifare Classic have been proposed. This paper includes the implementation details of the CRYPTO1, highlights biggest weaknesses of the security mechanisms and gives an overview of the most serious attacks.

### 1. УВОД

Одређивање шта се може свести под појам паметне картице није једноставан задатак, посебно имајући у виду често поистовећивање са појмом *RFID* (енгл. *Radio Frequency Identification*). *RFID* представља једноставан ентитет који комуницира и може да се идентификује путем радио таласа. *RFID* може бити активан тј. има властити извор напајања или може бити пасиван тј. користи енергију електромагнетног поља које генерише читач. Паметна картица садржи интегрисано коло уз помоћ којег пружа шири спектар могућности у односу на *RFID*. Паметне картице се грубо могу поделити на оне које пружају: 1) само идентификацију; 2) складиштење података без икаквих сигурносних протокола; 3) складиштење података уз њихову заштиту помоћу криптографских алгоритама и 4) обраду складиштених података. Други тип поделе паметних картица јесте на контактне и бесконтактне.

*Mifare Classic* је бесконтактна паметна картица пројектована да омогући складиштење података уз њихову заштиту помоћу криптографских алгоритама. Услед лошег дизајна читавог сигурносног протокола, *Mifare Classic* паметна картица не пружа прописану заштиту података. Ово не чини *Mifare Classic* паметну картицу неупотребљивом, јер се она може користити у оквиру система који захтевају паметну картицу која пружа могућност складиштења података без икаквих сигурносних протокола.

### 2. MIFARE CLASSIC

Компанија *NXP Semiconductors* представила је 1995. године фамилију производа *Mifare* којој припада и *Mifare Classic* бесконтактна картица. *Mifare Classic* бесконтактна картица је компатибилна са прва три дела стандарда *ISO/IEC-14443*. Четврти део стандарда дефинише протокол комуникације вишег нивоа. У наредној секцији описани су појединачни делови стандарда.

#### 2.1. Комуникациони слој

Комуникациони слој *Mifare Classic* паметне картице заснива се на *ISO/IEC-14443* стандарду. Овај стандард дефинише на који начин се одвија комуникација између бесконтактних картица и читача. Први део стандарда описује физичке карактеристике картице и услове под којима може да функционише. Други део стандарда дефинише како се преносе подаци између картице и читача. Подаци могу бити кодовани и модулирани на два начина које стандард реферише као *Type A* и *Type B*. *Mifare Classic* картица за пренос података користи начин *Type A*. Трећи део стандарда описује иницијализацију и антиколизиони протокол. Антиколизиони протокол се користи за одабир тачно једне картице када је у електромагнетном пољу читача присутно више картица. Након успешне антиколизије, одабрана картица се налази у активном стању и спремна је да прихвати команду протокола вишег нивоа. Четврти део стандарда дефинише на који начин се шаљу команде протокола вишег нивоа. *Mifare Classic* картица није компатибилна са овим делом стандарда, већ користи властити протокол чији детаљи нису у потпуности познати. Документација *Mifare Classic* картице набраја доступне команде и

наводи да се пре било какве размене података мора извршити аутентикација, након чега се шифрују сви подаци који се размењују између картице и читача.

## 2.2. Логичка структура

*Mifare Classic* картица поседује интерну меморију капацитета 1KB, која је организована у блокове величине 16 бајтова. Блокови се групишу у секторе. Меморија је подељена на 16 сектора, при чему се сваки сектор састоји из тачно 4 блока. Последњи блок сваког сектора назива се крај сектора. Блок 0 унутар сектора 0 назива се блок произвођача и он садржи идентификатор картице, контролну суму и податке произвођача. Блок произвођача је попуњен и закључан приликом производње картице како његов садржај не би било могуће касније променити. Пре било које меморијске операције над неким блоком, читач мора да буде аутентикован за приступ сектору у којем се жељени блок налази. Крај сектора садржи тајни кључ А, права приступа блоковима датог сектора и тајни кључ Б (опционо).

Сваки блок осим блока произвођача и краја сектора може бити одређен за складиштење произвољног податка величине 16 бајтова или може бити дефинисан као вредносни блок у оквиру којег се чува вредност величине 4 бајта. Формат вредносног блока је дизајниран тако да је могуће препознати грешку, уклонити грешку и извршити опоравак. Зарад интегритета вредности унутар вредносног блока и њене сигурности, дата вредност величине 4 бајта записана је три пута за редом у првих 12 бајтова вредносног блока. Преостала 4 бајта вредносног блока садрже једнобајтну адресу блока која је записана четири пута.

## 2.3. Скуп меморијских команди

Скуп команди вишег протокола *Mifare Classic* паметне картице је релативно мали. Меморијске команде се користе за манипулацију блокова са подацима. Читач мора бити аутентикован за приступ одговарајућем сектору пре слања команде. Права приступа датом блоку се проверавају сваки пут када се команда извршава. Постоје команде за упис податка у блок и читање податка из блока, који може бити или блок са подацима или вредносни блок. За манипулацију вредносних блокова на располагању су и команде за инкрементирање и декрементирање

вредности која се чува у њему, као и команде за премештање вредности из одређеног вредносног блока у меморијски регистар и обрнуто.

## 3. CRYPTO1

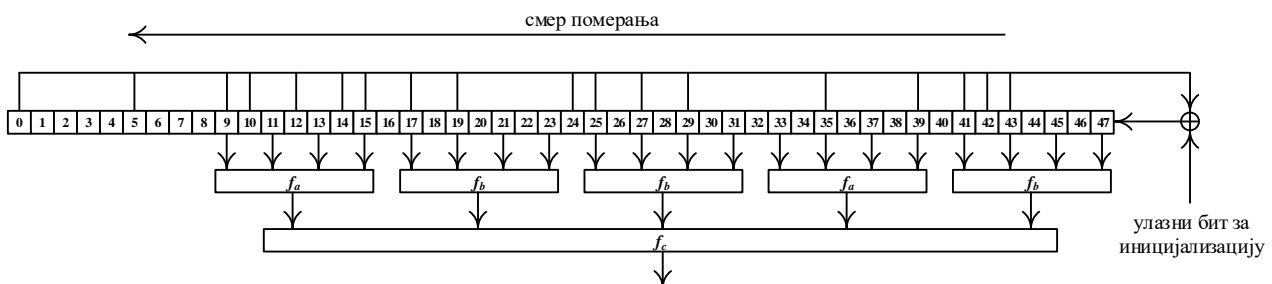
*CRYPTO1* је симетрични алгоритам шифровања развијен од стране компаније *NXP Semiconductors*. Алгоритам је имплементиран директно у хардверу *Mifare Classic* паметне картице како би се постигла већа брзина шифровања. Сигурност коју овај алгоритам шифровања пружа заснива се на тајности тј. непознавању детаља самог алгоритма. Упркос томе, детаљи алгоритма су откривени посматрањем *Mifare Classic* картице под микроскопом [1] и анализом порука које размењују читач и картица у току протокола аутентикације [2]. У овој секцији биће описан алгоритам шифровања *CRYPTO1*.

### 3.1. Генерисање тока битова за шифровање

*CRYPTO1* је проточни алгоритам шифровања [3]. Најбитнији део овог алгоритма, генератор псеудо случајних битова, састоји се из 48-битног померачког регистра са линеарном повратном спрегом (енгл. *Linear Feedback Shift Register*) и нелинеарног филтер генератора у два нивоа. Слика 1 приказује поменути померачки регистар са линеарном повратном спрегом и нелинеарни филтер генератор у два нивоа који се састоји од функција  $f_a$ ,  $f_b$  и  $f_c$ .

Нелинеарни филтер генератор узима 20 битова из померачког регистра са линеарном повратном спрегом и на основу њих генерише један псеудо случајни бит који се користи за шифровање проточним алгоритмом шифровања. Вредност померачког регистра се затим помера за једну позицију улево, одбацујући први бит с лева (нулти бит) и убацујући нови бит који је генерисан користећи линеарну функцију повратне спреге, на први бит с десна (четрдесетседми бит). Ако користимо  $x_i$  да означимо вредност бита на позицији  $i$  и ако користимо  $\oplus$  да означимо логичку функцију ексклузивно ИЛИ, линеарна функција повратне спреге се дефинише као:

$$LF_{cipher}(x_0x_1 \dots x_{47}) = x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$



Слика 1. Померачки регистар са линеарном повратном спрегом

Нелинеарни филтер генератор, којим се генерише један бит тока који се користи за шифровање, може да се дефинише као комбинација три логичке функције  $f_a$ ,  $f_b$  и  $f_c$ . Користећи исту  $x_i$  нотацију као и за померачки регистар и увођењем оператора  $\vee$  за логичку функцију ИЛИ и оператора  $\wedge$  за логичку функцију И, нелинеарни филтер генератор и три логичке функције  $f_a$ ,  $f_b$  и  $f_c$  дефинишу се на следећи начин:

$$f(x_0x_1 \dots x_{47}) = f_c(f_a(x_9, x_{11}, x_{13}, x_{15}), \\ f_b(x_{17}, x_{19}, x_{21}, x_{23}), f_b(x_{25}, x_{27}, x_{29}, x_{31}), \\ f_a(x_{33}, x_{35}, x_{37}, x_{39}), f_b(x_{41}, x_{43}, x_{45}, x_{47})) \\ f_a(a, b, c, d) = ((a \vee b) \oplus (a \wedge d)) \\ \oplus (c \wedge ((a \oplus b) \vee d)) \\ f_b(a, b, c, d) = ((a \wedge b) \vee c) \\ \oplus ((a \oplus b) \wedge (c \vee d)) \\ f_c(a, b, c, d, e) = (a \vee ((b \vee e) \wedge (d \oplus e))) \\ \oplus ((a \oplus (b \wedge d)) \wedge ((c \oplus d) \vee (b \wedge e)))$$

### 3.2. Аутентикациони протокол

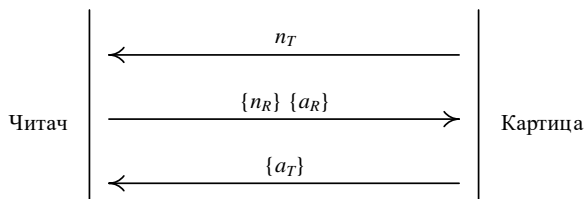
Аутентикациони протокол који користи *Mifare Classic* картица заснива се на аутентикацији путем изазова (енгл. *challenge*) и одговора (енгл. *response*). Читач започиње аутентикацију за одређени сектор меморије слањем захтева за аутентикацију. Након слања захтева, међусобна аутентикација читача и картице постиже се кроз следећа три корака:

1) Картица прво шаље свој 32-битни изазов ( $n_T$ ) који је псеудо случајан број;

2) Од другог корака комуникација је шифрована. Читач шаље картици свој 32-битни изазов ( $n_R$ ) који је псеудо случајан број и шаље 32-битни одговор ( $a_R$ ) на изазов који је картица послала у првом кораку;

3) У случају да је примљени одговор читача исправан, картица ће послати 32-битни одговор ( $a_T$ ) на изазов који је читач послао у другом кораку. Ако је примљени одговор читача погрешан, картица неће ништа послати.

Размена података у оквиру аутентикационог протокола приказана је на слици 2. Витичастим заградама  $\{ \}$  представљене су шифроване вредности.



Слика 2. Аутентикациони протокол

Међусобна аутентикација је постигнута након успешног проласка кроз ова три корака протокола

аутентикације. Након што је читач аутентикован, дозвољено је извршавање меморијских операција над блоковима унутар сектора за који је захтевана аутентикација.

### 3.2.1. Генерисање случајног броја за изазов

Изазов представља 32-битну вредност добијену од генератора псеудо случајних бројева који је реализован помоћу 16-битног померачког регистра са линеарном повратном спрегом. Генератор псеудо случајних бројева за изазов је у потпуности независан од генератора псеудо случајних бита за шифровање. Стога, *Mifare Classic* картица поседује два независна померачка регистра (48-битни и 16-битни).

На сваку ивицу сигнала такта, вредност 16-битног померачког регистра помера се за једну позицију улево, одбацујући при томе први бит с лева и убацујући нови бит који је генерисан користећи линеарну функцију повратне спреге, на први бит с десна. Ако користимо  $x_i$  да означимо вредност бита на позицији  $i$  и ако користимо  $\oplus$  да означимо логичку функцију ексклузивног ИЛИ, линеарна функција повратне спреге се дефинише као:

$$LF_{nonce}(x_0x_1 \dots x_{15}) = x_0 \oplus x_2 \oplus x_3 \oplus x_5$$

### 3.2.2. Израчунавање одговора на дати изазов

Представимо изазов 32-битном секвенцом  $x_0x_1 \dots x_{31}$  генерисаном помоћу 16-битног померачког регистра. Одговор на дати изазов може се добити помоћу функције следбеника која се рачуна на следећи начин:

$$suc_{nonce}(x_0x_1 \dots x_{31}) = x_1x_2 \dots x_{31}LF_{nonce}(x_{16}x_{17} \dots x_{31}) \\ suc_{nonce}^n(x_0x_1 \dots x_{31}) = suc_{nonce}^{n-1}(suc_{nonce}(x_0x_1 \dots x_{31}))$$

На основу вредности коју картица шаље као свој изазов ( $n_T$ ) израчунавају се и одговор читача ( $a_R$ ) и одговор картице ( $a_T$ ) користећи следеће релације:

$$a_R = suc_{nonce}^{64}(n_T) \\ a_T = suc_{nonce}^{96}(n_T)$$

### 3.3. Иницијализација алгоритма шифровања

Алгоритам шифровања *CRYPTO1* је неопходно иницијализовати пре него што се започне шифровање и дешифровање. Иницијализација се извршава на идентичан начин на страни читача и на страни картице. Алгоритам се иницијализује у оквиру протокола аутентикације.

Параметри који се користе за иницијализацију алгоритма су 48-битни тајни кључ сектора ( $K$ ), изазов картице ( $n_T$ ), идентификатор картице ( $id$ ) и изазов читача ( $n_R$ ). Иницијализација алгоритма започиње паралелним уписом 48-битног кључа сектора ( $K$ ) у померачки регистар са линеарном повратном спрегом који се користи за генерисање тока псеудо случајних бита за шифровање. Затим се у померачки регистар уписује бит по бит добијен применом логичке функције ексклузивно ИЛИ на бит повратне спреге и

одговарајући бит вредности  $n_T \oplus id$ . На крају се у померачки регистар уписује бит по бит добијен применом логичке функције ексклузивно ИЛИ на бит повратне спреге и одговарајући бит вредности  $n_R$ .

Процес иницијализације алгоритма може се формално представити на следећи начин. Ако су дати 48-битни тајни кључ сектора ( $K$ ), изазов картице ( $n_T$ ), идентификатор картице ( $id$ ) и изазов читача ( $n_R$ ):

$$\begin{aligned} K &= k_0 k_1 \dots k_{47} \\ n_T &= n_{T,0} n_{T,1} \dots n_{T,31} \\ id &= id_0 id_1 \dots id_{31} \\ n_R &= n_{R,0} n_{R,1} \dots n_{R,31} \end{aligned}$$

онда се унутрашње стање алгоритма  $state_i$  у тренутку  $i$  дефинише као:

$$state_i = s_i s_{i+1} \dots s_{i+47}$$

а  $s_i$  се дефинише следећим релацијама:

$$\begin{aligned} s_i &= k_i & \forall i \in [0,47] \\ s_{i+48} &= LF_{cipher}(s_i s_{i+1} \dots s_{i+47}) \oplus n_{T,i} \oplus id_i & \forall i \in [0,31] \\ s_{i+80} &= LF_{cipher}(s_{i+32} s_{i+33} \dots s_{i+79}) \oplus n_{R,i} & \forall i \in [0,31] \\ s_{i+112} &= LF_{cipher}(s_{i+64} s_{i+65} \dots s_{i+111}) & \forall i \in \mathbb{N} \end{aligned}$$

Након успешно завршене аутентикације, читач и картица имају идентично стање алгоритма.

### 3.4. Шифровање бита податка

Један бит податка шифрује се применом логичке функције ексклузивно ИЛИ на дати бит податка и бит добијен на излазу генератора псеудо случајних битова за шифровање. Вредност бита на излазу генератора псеудо случајних битова за шифровање дефинише се на следећи начин:

$$b_i = f(s_i s_{i+1} \dots s_{i+47}) \quad \forall i \in \mathbb{N}$$

Изазов читача ( $n_R$ ), одговор читача ( $a_R$ ) и одговор картице ( $a_T$ ) шифрују се према следећим правилима:

$$\begin{aligned} \{n_R\} &= n_{R,i} \oplus b_{i+32} & \forall i \in [0,31] \\ \{a_R\} &= a_{R,i} \oplus b_{i+64} & \forall i \in [0,31] \\ \{a_T\} &= a_{T,i} \oplus b_{i+96} & \forall i \in [0,31] \end{aligned}$$

Наведена нотација користи витичасте заграде  $\{ \}$  да означи шифровану вредност.

Треба приметити да се за шифровање не користи првих 32 битова које генератор псеудо случајних битова генерише одмах након уписа 48-битног тајног кључа сектора у померачки регистар.

Када се врши шифровање или дешифровање података проточним алгоритмом шифровања *CRYPTO1* мора се водити рачуна којим редоследом *Mifare Classic* картица шаље битове појединачних бајтова. Наиме, *Mifare Classic* картица прво шаље бит најмање тежине, у складу са стандардом *ISO/IEC-14443-A*.

### 3.5. Шифровање бита парности

Стандард *ISO/IEC-14443-A* специфицира да након сваког послатог бајта података мора да следи бит парности. Бит парности се користи као метод детекције грешака у преносу. Вредност бита парности се израчунава тако да број битова чија је вредност једнака јединици у скупу битова који чине битови датог бајта и сам бит парности буде или паран или непаран у завиности од стандарда. Стандард *ISO/IEC-14443-A* дефинише непарну парност, тако да број јединица у скупу који чине битови датог бајта и сам бит парности мора да буде строго непаран.

*Mifare Classic* картица рачуна вредност бита парности над оригиналним бајтом, уместо над шифрованим бајтом који ће послати. Додатно, *Mifare Classic* картица шифрује и бит парности. Бит парности се шифрује битом из тока псеудо случајних битова за шифровање који се затим користи и за шифровање првог следећег бита података. То значи да се померачки регистар са линеарном повратном спрегом не помера улево за једну позицију након шифровања бита парности.

## 4. СЛАБОСТИ MIFARE CLASSIC КАРТИЦЕ И АЛГОРИТМА CRYPTO1

Анализирајући имплементационе детаље алгоритма *CRYPTO1*, у овом истраживању смо описали његове највеће слабости.

### 4.1. Ниска ентропија генератора случајних бројева за изазове

Највећа слабост алгоритма *CRYPTO1* јесте премали број битова померачког регистра са линеарном повратном спрегом који се користи за генерисање псеудо случајних бројева за изазов. Померачки регистар има ширину од само 16 битова. Потребно је свега 0,6 секунди да се генерише свих  $2^{16}$  могућих бројева, након чега се започиње поновно генерисање истих псеудо случајних бројева за изазов. Позната је иницијална вредност померачког регистра са линеарном повратном спрегом, па је вредност изазова могуће унапред одредити на основу протеклог времена од тренутка када *Mifare Classic* картица добије нападање до тренутка када се започне аутентикација.

#### 4.1.1. Филтер генератор не зависи од првог бита с лева померачког регистра

Нелинеарни филтер генератор генерише ток битова за шифровање користећи 20 битова померачког регистра са линеарном повратном спрегом. Први бит с лева померачког регистра не учествује у генерисању тока битова за шифровање. Ово омогућава одређивање реверзне функције нелинеарног филтер генератора и реконструкцију стања померачког регистра бит по бит. Реконструкцијом стања померачког регистра може се добити његово иницијално стање које представља тајни кључ.

#### 4.1.2. Вишеструка употреба једног бита за шифровање

Ова слабост је последица комуникационог протокола дефинисаног стандардом *ISO/IEC-14443-A* који налаже слање бита парности након сваког послатог бајта. *Mifare Classic* картица израчунава вредност бита парности над оригиналном бајтом, уместо над шифрованим бајтом који се шаље. Слабост се огледа у чињеници да се израчунати бит парности и први бит наредног бајта шифрују истим битом из тока битова за шифровање.

### 5. НАПАДИ НА АЛГОРИТАМ CRYPTO1

Први напад има за циљ реконструкцију коришћеног тока битова за шифровање у оквиру комуникације између валидног читача и валидне картице [4]. Напад експлоатише слабост генератора случајних бројева за изазове, јер управо изазов картице и изазов читача одређују у потпуности ток битова за шифровање. За потребе напада потребна је потпуна контрола над читачем, док је мета напада картица. Реконструкцијом коришћеног тока битова за шифровање може се читати садржај картице и без познавања тајног кључа.

Други напад има за циљ реконструкцију тајног кључа, што омогућава прављење копије (енгл. *cloning*) картице [5]. Напад експлоатише слабост нелинеарног филтер генератора тј. чињеницу да се први бит с лева померачког регистра не користи за генерисање тока битова за шифровање. Мета напада је валидни читач. Реконструкцијом стања померачког регистра са линеарном повратном спрегом може се добити тајни кључ за мање од једне секунде.

### 6. ЗАКЉУЧАК

Имајући у виду да је могуће направити копију валидне картице за свега неколико секунди, јасно је да *Mifare Classic* картица не пружа никакву заштиту података. Овим је употребна вредност *Mifare Classic* картице сведена само на системе који не захтевају заштиту података. Постоје предлози техника којима се могу ублажити наведени сигурносни пропусти или барем омогућити детекција напада [6].

Познавање имплементационих детаља алгорита *CRYPTO1* може бити од користи код система који на располагању имају читач који није компатибилан са *Mifare Classic* картицом. У овом случају неопходно је имплементирати алгорита *CRYPTO1* у софтверу.

### ЗАХВАЛНИЦА

Овај рад је написан у оквиру пројеката ТР-32047 код Министарства просвете, науке и технолошког развоја Републике Србије.

### ЛИТЕРАТУРА

[1] K. Nohl, D. Evans, S. Ploetz and H. Ploetz, "Reverse-Engineering a Cryptographic RFID Tag," USENIX security symposium, vol. 28, Jul. 2008.

[2] F. D. Garcia, G. K. Gans, R. Muijers, P. Rossum, R. Verdult, R.W. Schreur and B. Jacobs, "Dismantling MIFARE Classic," in European Symposium on Research in Computer Security, Malaga, ES, 2008, pp. 97-114.

[3] W. H. Tan, "Practical Attacks on the MIFARE Classic," M.S. thesis, Dept. Comp., Imperial College London, London, UK, 2009.

[4] G. K. Gans, J. H. Hoepman and F. D. Garcia, "A practical attack on the MIFARE Classic," in International Conference on Smart Card Research and Advanced Applications, London, UK, 2008, pp. 267-282.

[5] F. D. Garcia, P. Rossum, R. Verdult and R. W. Schreur, "Wirelessly Pickpocketing a Mifare Classic Card," in IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2009, pp. 3-15.

[6] W. Teepe. (2008, Oct.). Making the Best of Mifare Classic. Radboud University Nijmegen. Netherlands. [Online]. Available: <http://www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf>

[7] K. E. Mayes and C. Cid, "The MIFARE Classic story," Information Security Technical Report, vol. 15, issue 1, pp. 8-12, Feb. 2010.

[8] R. W. Schreur, P. Rossum, F.D. Garcia, W. Teepe, J. H. Hoepman, B. Jacobs, G. K. Gans, R. Verdult, R. Muijers, R. Kali and V. Kali. (2008, Mar.). Security Flaw in MIFARE Classic. Radboud University Nijmegen. Netherlands. [Online]. Available: <http://www.sos.cs.ru.nl/applications/rfid/pressrelease.en.html>

[9] H. Dimitrov and K. Erkelens. (2014, Feb.). Evaluation of the feasible attacks against RFID tags for access control systems. University of Amsterdam. Netherlands. [Online]. Available: [https://www.os3.nl/media/2013-2014/courses/rp1/p60\\_report.pdf](https://www.os3.nl/media/2013-2014/courses/rp1/p60_report.pdf)

[10] K. Nohl. (2008, Oct.). Cryptanalysis of Crypto-1. University of Virginia. Virginia. [Online]. Available: <http://proxmark.nl/files/Documents/13.56%20MHz%20-%20MIFARE%20Classic/Cryptanalysis.of.Crypto-1.pdf>



# PRIMENA WEB APLIKACIJE ZA OBRADU PODATAKA SA DRUŠTVENE MREŽE TWITTER ZA ANALIZU TURISTIČKIH POTENCIJALA – STUDIJA SLUČAJA SMEDEREVSKA I GOLUBAČKA TVRĐAVA USING OF WEB APPLICATION FOR DATA PROCESSING FROM TWITTER SOCIAL NETWORK FOR ANALYZE OF TOURIST POTENTIAL – CASE STUDY: SMEDEREVO AND GOLUBAC FORTRESS

Nikola Džaković<sup>1</sup>, Nikola Dinkić<sup>1</sup>, Jugoslav Joković<sup>1</sup>, Leonid Stoimenov<sup>1</sup>, Aleksandra Djukić<sup>2</sup>

*Univerzitet u Nišu - Elektronski fakultet*<sup>1</sup>

*Univerzitet u Beogradu - Arhitektonski fakultet*<sup>2</sup>

**Sadržaj** - Predmet istraživanja u ovom radu je analiza mogućnosti primene podataka sa društvene mreže Twitter, za analizu turističkih potencijala kulturno istorijskih objekata i njihove umreženosti sa urbanim sredinama. Za potrebe obrade podataka i odgovarajuće analize kreirana je Web aplikacija koja koristi Twitter REST API kao sredstvo komunikacije sa tom društvenom mrežom. Prikupljeni podaci za lokacije Smederevske i Golubačke tvrđave, filtrirani su i klasifikovani prema zadatim kriterijumima koji se odnose na prostornu i vremensku raspodelu, kao i semantičku i analizu sadržaja za potrebe istraživanja atraktivnosti razmatranih objekata odnosno otvorenih prostora.

**Abstract** - Purpose of this paper is analysis of the ability to use data from the social network Twitter for determining tourist potential of cultural and historical locations and their networking with urban areas. For needs of this analyzes a Web application was created, which uses Twitter REST API as a medium for communication with this social network. Data gather for fortresses of Smederevo and Golubac was filtered and classified based on time and space criteria, but also based on semantic and content analysis in order to determine attractiveness of the considered locations or open spaces.

## 1. UVOD

U današnjem savremenom informatičkom dobu, društvene mreže značajno utiču na svaki aspekt života i društva uopšte. Nastale su kao nusprodukt interneta, a transformisale su svet u ono što se može nazvati informaciono društvo, sa visoko-tehnološkom komunikacijom koja prožima gotovo svaki aspekt ljudskog života. Društvene mreže su se pojavile kao inovacija u tehnologiji i dovele su do ubrzanog razvoja u politici, ekonomiji, biznisu i posebno turizmu. Njihovom pojavom znatno je povećana komunikacija između ljudi širom sveta, pošto one predstavljaju jedan od glavnih izvora informacija, koje su javno dostupne na bilo kom mestu i bilo kom trenutku, bilo preko računara ili pametnih telefona. One predstavljaju društvenu strukturu koju čine pojedinci ili organizacije koje se nazivaju čvorovi (eng. *nodes*). Čvorovi su međusobno povezani jednom ili više međuzavisnosti kao što su prijateljstvo, srodstvo, zajednički interes, finansijska razmena, neprilagođenost, polna pripadnost ili vera [1]. Za Kaplan-a [2] termin socijalne mreže predstavljaju grupu web aplikacija koje se zasnivaju na ideološkim i tehnološkim

temeljima Web 2.0 i omogućavaju generisanje i deljenje sadržaja koje je kreirao sam korisnik.

Danas se koristi više od 60 različitih društvenih mreža, od kojih su među najpopularnijim Twitter i Facebook. One podstiču svoje korisnike da izraze svoja mišljenja, osećanja ili detalje iz svog privatnog života, ali i pružaju mogućnost da promovišu svoje poslovanje. Sadržaj tvitova i statusa varira od veoma važnih do potpuno nebitnih informacija. Većina tih poruka nosi veoma malo korisnih informacija, ali agregacijom milion poruka može se doći do veoma važnih i korisnih informacija. U tom kontekstu, Twitter društvena mreža predstavlja interesantan izazov. Kratki tekstovi (tvitovi), široko korišćenje nestandardne gramatike, pisanja i znakova interpunkcije, zatim korišćenje slenga, skraćenica i neologizma dosta otežavaju semantičku analizu. Analiziranje ovakvog sadržaja može dovesti do korsnih informacija na poljima kao što je personalizovani marketing ili društveno profiliranje. Nekoliko studija društvene mreže Twitter potvrdilo je činjenicu da se na osnovu ogromnog broja tvitova može dobiti dragoceni uvid stanja u društvu. *Barbosa* i *Feng* [3] su izvršili klasifikaciju tvitova po osećanjima (eng. *sentiment*), prvi korak ka merenju stava javnog mnjenja, kao što je politička opredeljenost, za šta se pokazalo da prati javno političko mišljenje i predviđa izbore [4]. *Ajnštajn et al.* je proučavao varijacije u rečniku kod tvitova za određena geografska područja. Drugi su pratili širenje vesti [5], detektovali su prvo spominjanje vesti o nekom događaju, i pratili su kada su se dešavali zemljotresi [7].

Glavni cilj ovog rade jeste da se ilustruju mogućnosti metodologije koje, na osnovu odgovarajućih analiza zasnovanim na korisničkim podacima deljenim na društvenoj mreži Twitter, mogu unaprediti posećenost i atraktivnost istorijskog kulturnog nasleđa i njegovog šireg okruženja. Istraživanje je izvršeno za dve srednjovekovne tvrđave, Golubačku i Smederevsku koje se nalaze u Istočnoj Srbiji na desnoj strani reke Dunav. Ove tvrđave sagrađene u XIV i XV veku predstavljaju kulturne spomenike od izuzetnog značaja, pa su zato veoma interesantne, kako za domaće, tako i za inostrane turiste. Istovremeno, one su značajan pokretač razvoja okolnih gradova i regiona, kao i osnov za jačanje kulturnog turizma.

Metodologija korišćena prilikom analiza je mapiranje korisnika na društvene mape (pomoću društvenih mreža), bazirana na aplikaciji „Twitter search engine“ (TSE) [8]. Praćenjem i merenjem intenziteta korisnika na teritorijama od značaja, mogu se testirati obrasci u

ponašanju, ali i pronalaci tzv „pozitivne rute“. Dobijeni rezultati pomažu u kreiranju celokupne slike o odabranim istorijskim spomenicima kulture sa aspeta njihovih korisnika i lokalnog stanovništva. Analizom tvitova, kao i grupe ljudi koja ih posećuje, ta slika se može rekonstruisati u željenu kako bi se iskoristio njihov pun potencijal.

U nastavku, objašnjene su metode za analizu teksta kao i opis novih mogućnosti TSE web aplikacije koje se odnose na semantičku analizu tekstova na srpskom jeziku. U cilju ilustracije mogućnosti aplikacije, dat je statistički pregled i analiza rezultata na bazi prikupljenih podataka, na osnovu koji su izvedeni zaključci i pravac budućeg rada.

## 2. APLIKACIJA TSE I OBRADA PRIRODNIH JEZIKA

Obrada prirodnih jezika (Natural Language Processing, NLP) u daljem tekstu NLP, predstavlja oblast informatike, veštačke inteligencije i kompjuterske lingvistike, koja se bavi interakcijom između računara i ljudskih (prirodnih) jezika. Atribut „prirodni“ treba da ukaže da se radi o jeziku kojim ljudi komuniciraju u uobičajenom smislu, a ne o formalnim jezicima, kakvi su jezici matematičkih izraza ili kakvi su programski jezici. NLP je područje istraživanja i primene koje se bavi temom kako računari mogu biti upotrebljeni za razumevanje i manipulaciju teksta ili govora prirodnog jezika. Istraživači NLP-a teže da saznaju kako ljudska bića razumeju i koriste jezik, kako bi se razvili odgovarajući alati i tehnike koje bi kompjuterski sistemi razumeli i omogućili im manipulisane prirodnim jezikom u svrhu obavljanja željenih zadataka. Sentimentalna analiza, odnosno obrada mišljenja, jeste posebna sfera u oblasti NLP-a koja analizira mišljenja ljudi ali i osećanja, ocenjivanje i procenu stavova i emocija prema nekim entitetima kao što su: različiti proizvodi, usluge, organizacije, individue, pitanja, događaji, teme, i to prema njihovim atributima. Ova oblast obuhvata ogroman problemski prostor. Termin sentimentalna analiza češće je upotrebljavan u akademskim krugovima, u praksi se terminii sentimentalna analiza i obrada mišljenja koriste podjednako često. Sentimentalna analiza i obrada mišljenja se uglavnom fokusiraju na osećanja, koja izražavaju ili impliciraju pozitivan ili negativan stav. Aplikacija TSE omogućava prikupljanje, obradu i smeštanje georeferenciranih podataka koje generiše društvena mreža Twitter. Ovaj rad opisuje najnovije funkcionalnosti aplikacije TSE koje se odnose na sentimentálnu analizu i mogućnosti da procesira i analizira podatke sa ove društvene mreže.

Glavni indikatori nečijeg stava su sentimentálne reči, koje se takođe nazivaju i mišljenja. Ove reči se često koriste kako bi se izrazila pozitivna ili negativna osećanja. Na primer, dobro, predivno i zapanjujuće su pozitivne sentimentálne reči, dok loše, očajno i strašno su negativne. Sentimentálne reči i fraze su iz očiglednih razloga ključne za sentimentálnu analizu. Skup takvih reči i fraza se naziva sentimentální rečnik. Iako su ovakve reči i fraze bitne za sentimentálnu analizu, samo obična upotreba ovih reči nije dovoljna. Ovaj problem je mnogo kompleksniji. Drugim rečima možemo reći da je

sentimentální rečnik potreban ali ne i dovoljan za sentimentálnu analizu kompleksnog teksta. Kako su tvitovi generalno kratki i informativnog karaktera, a takođe sadrže i dosta Internet slengova i smajlija, oni su lakši za analizu zbog ograničenja u dužini slova a i zato što su autori tvitova uglavnom direktni u izražavanju svojih mišljenja. Za sentimentálnu analizu, ovaj rad koristi algoritam baziran na rečniku, kako bi odredio orijentaciju tvitova. Nakon jezičke selekcije tvitova, po prvi put izvršena je analiza tvitova koji su napisani na srpskom jeziku uz pomoć svih reči koje su zastupljene u tvitovima. Rečnik je kreiran na osnovu najzastupljenijih reči u okviru twitova. Izdvojenim rečima je ručno dodeljena pozitivna ili negativna orjentacija, uz pomoć čega će se na kraju zaključiti konačna impresija tvita. Svaka reč ima svoju vrednost koja može biti pozitivna ili negativna i u zavisnosti od toga šalje pozitivnu ili negativnu poruku. Ukoliko tvit ne sadrži nijednu pozitivnu ili negativnu reč onda se on smatra neutralnim, ukoliko sadrži samo pozitivne reči onda je on pozitivno orijentisan, ukoliko sadrži samo negativne reči onda je on negativno orijentisan u suprotnom je spada u grupu kompleksnih koja podrazumeva kombinaciju ove dve grupe reči i zahteva detaljniju analizu.

## 3. ANALIZA PRIKUPLJENIH PODATAKA

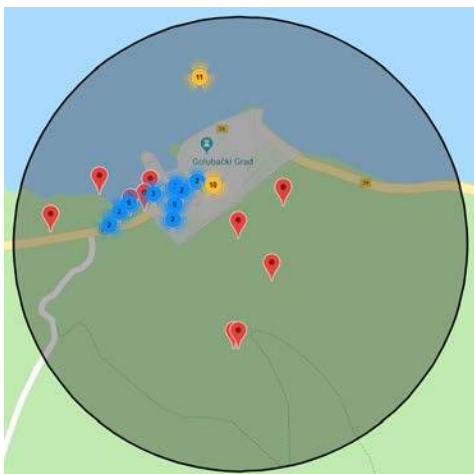
Prikupljeni podaci za područja Golubačke i Smederevske tvrđave obrađeni su uz pomoć TSE web aplikacije, kojoj su pridodate nove funkcionalnosti. Oblasti za koje su prikupljeni tvitovi, određene su geografskom širinom (*latitude*), geografskom dužinom (*longitude*), kao i radijusom (300m). U Tabeli 1 prikazani su kumulativni podaci u periodu od 7 godina (2011 – 2017).

Tip analize	Golubačka tvrđava	Smederevska Tvrđava	Ukupno
Ukupan broj tweetova	61	218	279
Broj korisnika	44	85	127
Broj aplikacija	5	4	6
Broj jezika	8	10	15
Broj like-ova	36	158	194
Broj retweet-a	2	12	14
Broj pratilaca	85253	670005	755258
Broj prijatelja	50872	290792	341664

Tabela 1. Kumulativni podaci za Golubačku i Smederevsku tvrđavu

Na osnovu broja tvitova i broja različitih korisnika, lako se može zaključiti da su korisnici bili znatno aktivniji u Smederevske tvrđavi. Takođe, podaci pokazuju da su neke pozicije unutar ovih prostora daleko zanimljivije korisnicima od drugih. Tako se, na primer, za Golubačku tvrđavu mogu izdvojiti dve lokacije koje su daleko popularnije od ostalih i one se mogu videti na Slici 1., dok se u Smederevske tvrđavi raspodela malo ravnomernija i može se videti na Slici 2. Povećana aktivnost korisnika u Smederevske tvrđavi, može se objasniti činjenicom da je

ona deo grada Smedereva i u samoj blizini tvrđave nalaze lokali koji imaju besplatnu internet konekciju što turistima omogućava da postavljaju sliku ili željeni sadržaj. Iz kumulativnih podataka korisnika koji su omogućili geografsko pozicioniranje može se uočiti, na primer, da se zbir različitih korisnika koji su posetili obe tvrđave ne poklapa sa ukupnim brojem različitih korisnika, što govori da postoje korisnici koji su u ovom vremenskom intervalu postavili tweetove u obe tvrđave.

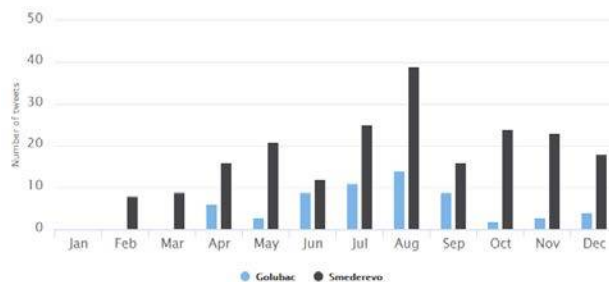


Slika 1. Raspodela georeferenciranih tweetova na prostoru Golubačke tvrđave

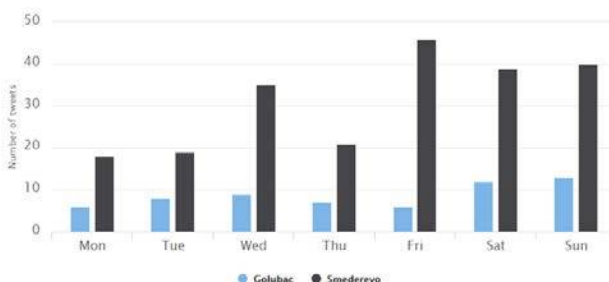


Slika 2. Raspodela georeferenciranih tweetova na prostoru Smederevske tvrđave

Pored prostornog mapiranja korisnika, TSE takođe omogućava vremensku raspodelu tweetova po godinama, mesecima, danima pa čak i dobu dana. Slika 3. daje raspodelu tweetova po mesecima za svaku od tvrđava od interesa, dok Slika 4. prikazuje vremensku raspodelu tweetova po danima u nedelji. Može se videti da su korisnici u zimskom periodu znatno manje aktivni, pa se tako može izdvojiti januar, gde nije postavljen nijedan tweet, dok sa druge strane tokom avgusta su korisnici bili najaktivniji u obe tvrđave. Može se takođe primetiti da su korisnici u proseku dosta aktivniji preko vikenda u odnosu na radne dane i to u poslepodnevnim časovima.

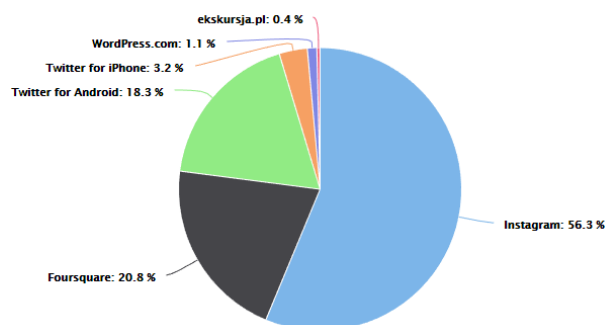


Slika 3. Vremenska raspodela tweetova po mesecima

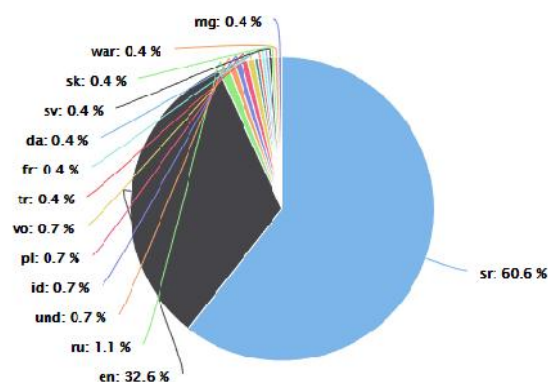


Slika 4. Vremenska raspodela tweetova po danima u nedelji

Ukupno gledano za obe tvrđave najatraktivnija aplikacija je Instagram sa koje je postavljeno više od polovine ukupnog sadržaja, što nam govori da je većina tweetova pored teksta sadrži sliku (Slika 5). Detekcija jezika koja je vršena uz pomoć Language detection API-ja [9] pokazuje da je tekst tweetova najčešće na srpskom jeziku (Slika 6), što otvara potrebu da se i semantička analiza vrši na ovom jeziku.



Slika 5. Raspodela tweetova po aplikacijama



Slika 6. Raspodela tweetova po detektovanim jezicima



Pošto je analiza teksta na engleskom jeziku relativno razvijena oblast informatičke lingvistike gde postoje različite metode i alati koji na pružaju osnovne vidove klasifikacije teksta, analiza na srpskom predstavljala je pravi izazov pre svega zbog veoma specifičnih gramatičkih pravila. Za samu analizu je iskorišćena analiza teksta koja se zasniva na rečniku reči koje šalju pozitivnu ili negativnu poruku. Pošto čak ni ovi rečnici ne postoje na srpskom jeziku za potrebe ove analize kreirane su grupe reči na osnovu teksta tvitova. Najzastupljenijim rečima dodeljena je pozitivna odnosno negativna orijentacija u zavisnosti od značenja. Ovim putem kreiran je zatvoren skup reči, odnosno rečnik koji neophodan za samu analizu tvitova. Primenom opisanog algoritma i rečnika dobijeni su sledeći rezultati (Tabela 2). Pod pretpostavkom da su neutralni tvitovi informativnog karaktera i ne iskazuju mišljenje i osećanja korisnika prema lokacijama od značaja, može se zaključiti da je pozitivno orijentisanih 71.62% tvitova.

#	Golubac	Smederevo	Ukupno
Pozitivni	7	46	53
Negativni	3	16	19
Kompleksni	0	2	2
Neutralni	51	154	205
Ukupno	61	218	279

Tabela 2. Rezultati sentimentalne analize tvitova

#### 4. ZAKLJUČAK

Aplikacija čije su mogućnosti ilustrovane u radu razmatra uticaj društvene mreže Twitter na život ljudi u savremenom informatičkom društvu, kao i njihova direktna korelacija i potencijal u cilju poboljšanja posećenosti i atraktivnosti kulturnih spomenika. Pošto se radi o veoma popularnoj temi današnjice, fokus ovog rada na prikazivanju novih mogućnosti i unapređenja TSE web aplikacije, baziranih na obradi prirodnih jezika i semantičkoj analizi teksta na srpskom jeziku. Na osnovu kumulativnih podataka za Smederevsku i Golubačku tvrđavu i dobijenih statistika izvedeni su zaključci, koji mogu biti iskorišćeni u svrhu unapređenja posećenosti, a samim tim atraktivnosti kulturnih spomenika. S obzirom da je većina sadržaja postavljena putem društvenih mreža multimedijalnog tipa tekstualna analiza sama po sebi nije u potpunosti dovoljna, pa će fokus u budućem radu, pored proširenja analize prema poslanim simbolima (npr. smajliji – pozitivni i negativni), takođe biti i na obradi slika gde će akcent biti na detekciji objekata kao raspoloženja ljudi na slikama.

#### ZAHVALNICA

Istraživanja izložena u ovom radu su delimično finansirana od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, u okviru projekata III-44009, III-47003 i INTERREG projekta „DANURB - DANUBE URBAN BRAND - a regional network building through tourism and education to strengthen the “Danube” cultural identity and solidarity“.

#### LITERATURA

- [1] Nwabueze, C. and Chizoba, V. “Traditional Media and Sustainable Rural Development“, A Synergic Approach in 1<sup>st</sup> Bevezer Sola Conference on Communication, 2007.
- [2] Kaplan, A.M. and Haenlein, M. “Users of the world, unite! The challenges and opportunities of Social Media“, Business Horizons, Vol. 53, No. 1, pp 59-68, 2010.
- [3] Barbosa, L., and Feng, J., “Robust sentiment detection on twitter from biased and noisy data“, COLING '10 Proceedings of the 23rd International Conference on Computational Linguistics, pp 36-44, Peking, Kina, 2010.
- [4] Andranik, T., Timm, O. S., Philipp, G. S., Isabell, M. W., “Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment“, Social Science Computer Review, Vol. 29, pp 402-418, 2011.
- [5] Lerman, K., and Ghosh, R., “Information contagion: an empirical study of the spread of news on digg and twitter social networks“, Proceedings of 4th International Conference on Weblogs and Social Media, 2010.
- [6] Petrović, S., Osborne, M., i Lavrenko, V. “Streaming first story detection with application to twitter“, Proceeding Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, pp 181-189, Los Angeles, California, 2010.
- [7] Sakaki, T., Okazaki, M. and Matsuo, Y., “Earthquake shakes Twitter users: real-time event detection by social sensors“, Proceedings of the 19th international conference on World wide web, pp 851-860, Raleigh, North Carolina 2010.
- [8] Džaković, N., Dinkić, N., Joković, J., Stoimenov, L., “Web aplikacija za prikupljanje, skladištenje, obradu i geo-analizu podataka sa društvene mreže Twitter“, Zbornik radova, YUINFO, str 145-148, Kopaonik, 2016.
- [9] Language detection API – <https://detectlanguage.com>, last visited 20.01.2018.

# C2C MODELI ELEKTRONSKOG POSLOVANJA: PRIMER PORTALA ZA PRONALAZENJE PASA

## C2C E-BUSINESS MODELS: CASE OF A PORTAL FOR FINDING DOGS

Katarina Đorđević<sup>1</sup>, Tamara Naumović<sup>1</sup>, Lazar Živojinović<sup>1</sup>, Marijana Despotović-Zrakić<sup>1</sup>  
*Fakultet organizacionih nauka, Univerzitet u Beogradu<sup>1</sup>*

**Sadržaj** – Područje istraživanja ovog rada su C2C modeli elektronskog poslovanja. Fokus rada je na razvoju i implementaciji portala za pronalaženje pasa. Ključna prednost ovog portala u odnosu na ostale je algoritam za pretragu i povezivanje oglasa sa sličnim osobinama. U radu je prikazana i realizacija Internet marketing plana preko društvenih mreža Facebook i Instagram, kao i dodatnih servisa. Definisana je i model prihoda portala.

**Abstract** – The subject of this paper is oriented towards C2C e-business models. Focus of the paper is on development and implementation of the portal for finding the lost pets. Key advantage that differentiates this portal from its competitors is an algorithm for matching the ads with similar descriptions. The paper also presents realization of Internet marketing plan using social networks Facebook and Instagram as well as additional services. Further, business model of the portal was defined, too.

### 1. UVOD

Danas na Internetu postoji veliki broj sajtova koji korisnicima nude različite informacije, interesantne linkove i sadržaje, mogućnost dobijanja korisničkog prozora, personalizaciju sadržaja i slično.

Korišćen model poslovanja u realizaciji portala je C2C (customer to customer). Ovaj poslovni model podrazumeva direktnu razmenu proizvoda i usluga između potrošača, odnosno krajnjih korisnika [6][7]. Ukoliko se ovaj oblik poslovanja realizuje putem Interneta, uobičajeno je da postoji posrednik, koji omogućava infrastrukturu za realizaciju različitih tipova transakcija [8]. U ovom radu će biti prikazan veb portal, koji predstavlja posrednika između vlasnika i pronalazača izgubljenih pasa.

Portal predstavlja jedinstvenu tačku pristupa različitim izvorima podataka [9]. Portali objedinjuju različite informacije iz većeg broja izvora, pružajući tako dosledne podatke i pristup brojnim aplikacijama, koje bi u suprotnom predstavljale zasebne jedinice.

Kao prednosti portala uglavnom nabrajaju se:

- inteligentna integracija i pristup sadržajima, aplikacijama i raznim informacijama
- poboljšana komunikacija i saradnja korisnika i saradnika
- objedinjen, trenutni pristup informacijama iz različitih izvora
- brza, jednostavna izmena i održavanje sadržaja

Cilj rada je kreirati portal koji će biti koristan krajnjim korisnicima u pronalaženju pasa. Portal pronadjipsa.rs biće korišćen za promociju aktivnosti koje pojedinci sprovode u domenu društvene odgovornosti i brige o životinjama.

### 2. ANALIZA POSTOJEĆIH REŠENJA

Halo oglasi (<https://www.halooglasi.com>) je jedan od najpopularnijih oglasnika u Srbiji. Veliki broj korisnika na njihovom sajtu koristi usluge pretrage oglasa za izgubljene i nađene pse, ali kao i u slučaju ostalih oglasnika, njegova namena nije za direktno pronalaženje oglasa o psima. Na ovom sajtu se nalaze oglasi različitih kategorija, a oglasi o psima su kategorija koju možete pronaći ulaskom na sajt, odabirom kategorije Kućni ljubimci, pa zatim podkategorije u zavisnosti od tipa. To može biti i jedan od razloga smanjenog broja oglasa, jer korisnici ne vole da preterano traže željeni sadržaj, već da im sadržaj bude „na dohvata ruke“ – kao što je u slučaju sa pronadjipsa.rs. Glavna prednost Halo oglasa je popularnost i veliki broj registrovanih korisnika, samim tim i veliki broj oglasa različitih kategorija. Međutim jedan od glavnih nedostataka je da ne postoje oglasi čija je namena oglašavanje pasa za udomljavanje. Broj oglasa na ovom sajtu za podkategoriju Izgubljenih i nađenih pasa iznosi tek 120.

Mali oglasi (<http://malioglasi.co.rs>) je još jedan od sajtova na kojem se mogu pronaći oglase o psima i u odnosu na Halo oglase sadrži povećani broj oglasa. Jedini nedostatak je što su svi oglasi stavljeni pod kategoriju Kućni ljubimci i ne postoji filter za pretragu prema tipu oglasa, pa su oglasi poređani prema datumu postavljanja i jedina mogućnost pretrage je unos pojma po kojem se vrši pretraga, a kao i Halo oglasi nisu fokusirani na oglase za pse već je to jedna od kategorija.

Životinje (<http://www.zivotinje.rs>) je portal koji nudi različite vrste informacija i zanimljivih sadržaja na temu životinja. Kao poseban deo sajta je deo sa oglasima koji možemo naći u glavnom meniju. Nakon toga postoji mogućnost za pretragu oglasa prema različitim kategorijama, od kojih postoje oglasi za izgubljene i nađene životinje, poklanjanje, prodaja, kupovinu životinja i slično. Jedan od glavnih nedostataka koji je primećen jeste da administratori ne proveravaju postavljanje oglasa tako da se u delu za izgubljene/nađene životinje mogu naći oglasi za pozajmice, kredite, koji zapravo nemaju puno dodirnih tačaka sa nazivom kategorije i na taj način odvlače korisnike. Još jedan nedostatak, kao i kod ostalih

sajtova je što ovo nije prvenstveno portal za oglašavanje pasa.

Na Facebook-u postoji veliki broj grupa u kojima ljudi mogu postavljati oglase izgubljenih, nađenih, pasa za udomljavanje i slično. Jedna od njih je Izgubljeni nađeni psi u Beogradu. Glavna pretpostavka je da korisnik poseduje Facebook nalog, a to nije slučaj sa svim korisnicima. Osnovni problem u ovim grupama je njihova zatvorenost i neupućenost ljudi na njihovo postojanje i njihov veliki broj, pa samim tim zbog velikog broja korisnika po grupi, mnogi oglasi mogu postati teški za pretragu i brzo zagubljeni među ostalima. Takođe, udomljavanje na pomenutoj grupi je zabranjeno.

### 3. RAZVOJ C2C PORTALA ZA PRONALAZENJE PASA

Potrebno je realizovati portal za pronalazjenje pasa koji će omogućiti upravljanje korisnicima i njihovim oglasima. Glavni cilj portala je brzi pronalazak željenog oglasa i jednostavnost kreiranja novih oglasa, ali sa mogućnošću pružanja različitih karakteristika oglasa neophodnih za bolju povezanost sličnih oglasa i primenu algoritma podudaranja. Portal treba da obezbedi osnovne funkcije pri radu sa navedenim entitetima, kao što su: unos, izmena, brisanje i pretraživanje [4][10].

SWOT analiza korišćena je kao konceptualni okvir za sistemsku analizu koja olakšava poređenje spoljnih pretnji i šansi sa unutrašnjim slabostima i snagama organizacije. U Tabeli 1 prikazana je SWOT analiza na primeru portala pronadjipsa.rs.

Snage	Slabosti
<ul style="list-style-type: none"> <li>- Pristupačne cene oglašavanja</li> <li>- Atraktivna ponuda</li> <li>- Veliki popusti</li> <li>- Saradnja sa različitim kompanijama i organizacijama</li> </ul>	<ul style="list-style-type: none"> <li>- Nedovoljno angažovanje i promocija</li> <li>- Nemogućnost plaćanja preko Interneta (npr. PayPal)</li> </ul>
Šanse	Pretnje
<ul style="list-style-type: none"> <li>- Širenje na tržištu (potencijalno sklapanje partnerstava i otvaranje novih poslovnica)</li> <li>- Još veća podrška korisnika</li> <li>- Horizontalno povezivanje sa preduzećima</li> </ul>	<ul style="list-style-type: none"> <li>- Ekonomska kriza</li> <li>- Konkurentno tržište</li> <li>- Smanjivanje obima poslovanja</li> </ul>

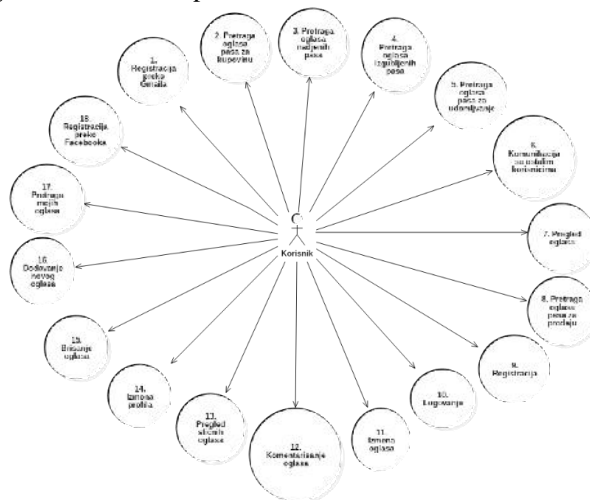
Tabela 1 SWOT analiza portala pronadjipsa.rs

Portal treba da se sastoji iz dva glavna dela:

- Rad sa oglasima
- Rad sa korisnicima.

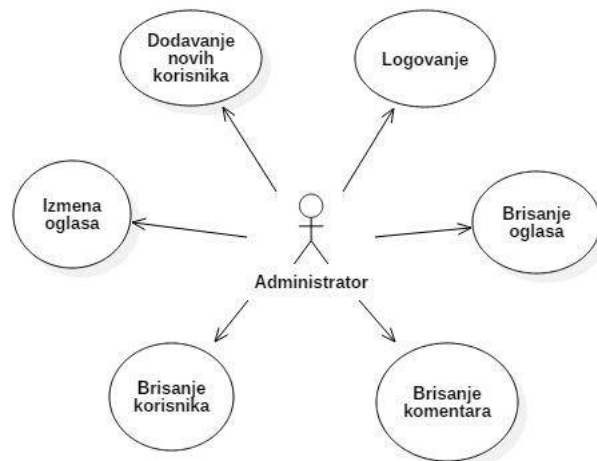
U delu za rad sa korisnicima, potrebno je omogućiti pregled, pretragu oglasa koje je kreirao konkretni korisnik. Isto tako je potrebno omogućiti da korisnik pre

nego što krene sa korišćenjem sistema ima mogućnost registracije i logovanja. U delu za rad sa oglasima potrebno je omogućiti pregled svih oglasa po različitim kategorijama. Identifikovani slučajevi korišćenja u kojima je akter - korisnik prikazani su na slici 1.



Slika 1 Dijagram slučajeva korišćenja aktera korisnik

Identifikovani slučajevi korišćenja u kojima je akter administrator prikazani su na slici 2.



Slika 2 Dijagram slučajeva korišćenja aktera administratora

Korišćenje tehnologije za razvoj portala: SQL Server, ASP .NET, ASP.NET MVC, HTML, CSS, jQuery, Java script, Bootstrap, Entity Framework [4].

Na slici 3 je prikazana početna stranica portala.



Slika 3 Početna strana portala

Sledi objašnjenje realizovanog algoritma za pronalaženje sličnih oglasa. Za svaki korisnikovog oglas koji nije tipa „Udomljavanje“ uraditi sledeće korake:

- a. Vratiti sve oglase istog pola i iste rase (to su isključujući parametri) u odnosu na trenutni oglas
- b. Filtrirati pronađene oglase na osnovu tipa oglasa:
  - i. Ako je trenutni oglas Izgubljen, filtrirati tako da pronađeni oglasi budu tipa Pronađen
  - ii. Ako je trenutni oglas Pronađen, filtrirati tako da pronađeni oglasi budu tipa Izgubljen
  - iii. Ako je trenutni oglas Kupujem, filtrirati tako da pronađeni oglasi budu tipa Prodajem
  - iv. Ako je trenutni oglas Prodajem, filtrirati tako da pronađeni oglasi budu tipa Kupujem
- c. Za svaki element tako filtrirane liste, uraditi sledeće korake:
  - i. Postavi brojač parametara slaganja na 2.
  - ii. Za svaki sledeći parametar slaganja između trenutnog oglasa povećati broj parametara slaganja za 1.
  - iii. Ukoliko je broj parametara slaganja veći od 3, izračunati procenat slaganja i dodati u rezultat (listu sličnih oglasa)
 
$$[100 * \text{brojač parametara slaganja} / \text{ukupan broj parametara slaganja}]$$
  - iv. Resetovati brojač parametara slaganja

Na slici 4. prikazan je izgled stranice nakon podudaranja dva slična oglasa.



Slika 4 Prikaz stranice sličnih oglasa

#### 4. IMPLEMENTACIJA INTERNET MARKETING PLANA

Onlajn promocija omogućava reklamiranje korišćenjem Interneta, dok se offline promocija odnosi na reklamiranje bez korišćenja Interneta [1][2][3]. Prednost onlajn promocije je pre svega smanjenje troškova. Načini ostvarivanja onlajn promocije su [1]:

- Facebook stranica (ažuriranje novosti, komunikacija preko Inboxa, nagradne igre)
- Instagram profil
- Google+ profil
- Postavljanje oglasa na sajtovima
- Plaćeno pozicioniranje na pretraživačima

Na društvenoj mreži Facebook definisana je ciljna grupa čiji korisnici imaju:

- interval od 15 do 65+ godina

- žive na teritoriji Srbije
- govore srpskim jezikom
- interesovanja su im psi i životinje

Na društvenoj mreži Instagram kreiran je poslovni profil koji daje mogućnost unošenja informacija o kontaktu, adresi i omogućava naznaku ostalim korisnicima da se radi o poslovnom profile i ubrzava povezivanje i komunikaciju. Da bi profil bio poslovni, prilikom registracije potrebno je povezati se sa kreiranom Facebook stranicom koja bi isto trebalo da bude povezana sa Instagram nalogom. To omogućava korisnicima da sav sadržaj na Instagram-u lakše i brže istovremeno podele na Facebook stranici. Novi poslovni profili na Instagramu pored već pomenutih funkcija poseduju nekoliko korisnih alata. Među njima se nalaze i Impresije koje predstavljaju koliko puta je objavljen post pregledan.

Za potrebu realizacije banera koji će se implementirati potrebno je definisati ciljnu grupu portala, a to su:

- Veterinarske ambulante
- Pet-shopovi
- Uzgajivačnice
- Novine koje pišu o psima i životinjama
- Stolarske radionice koje prave kućice za pse

U slučaju portala pronadjipsa.rs, baneri se nalaze na stranicama kupovina i prodaja pasa. Realizujuju se po rotaciji. Rotacija podrazumeva da se baner smenjuje sa još banera na toj poziciji. Baneri se rotiraju po principu slučajnosti (random), ali tako da prikazivanje rotacionih banera na istoj poziciji bude ravnomerno. Na portalu se nalaze baneri sledećih dimenzija: 300x800, 1300x150, 500x500, 728x90, 728x300. Baner veličine 728x90 je tip roll-down i primenjuje se na poziciji 728x90 piksela a prelaskom miša širi se na 728x300 piksela. Omogućava da na se na većoj površini predstavi ponuda. Prikazuje se na svim stranicama sajta. Realizuje se po principu rotacije.



Slika 5 Primer banera tipa roll down

#### 5. ZAKLJUČAK

S obzirom na rast i sveprisutnost društvenih mreža, važno je napomenuti da prisustvo na istim doprinosi imidžu i stvaranju brenda, a ujedno pomaže u razumevanju korisnikovih potreba i omogućava bolju analizu za dalji rad [1]. Uslovi na tržištu su takvi da potrebno stalno održavati i poboljšavati poziciju primenom savremenih rešenja, alata i tehnika da bi se pobedila konkurencija i pružilo drugačije iskustvo korisnicima. Upravo je ovo jedan od glavnih ciljeva za budući rad i istraživanje. Prilikom definisanja funkcionalnosti portala pronadjipsa.rs naglašena i detaljno objašnjena njegova glavna funkcionalnost, a to je korišćenje algoritma za

prepoznavanje sličnih oglasa. U daljem razvoju istraživače se i raditi na poboljšavanju samog algoritma korišćenjem neuronskih mreža i mapiranja. Planirano je poboljšanje izgleda oglasa, pa će svaki korisnik pored grada, u slučaju oglasa izgubljenih i nađenih pasa, unositi tačnu adresu na kojoj je pas poslednji put viđen i unaprediti dizajn oglasa i njegovu preglednost. Ova promena će doprineti promeni pretrage, pa će korisnici pored liste, moći uz pomoć mape da pretražuju oglase. Ovakvo rešenje će omogućiti vlasnicima oglasa praćenje kretanja psa, prikazom njegove putanje na mapi, koja će doprineti prikupljanju više informacija koje bi mu bile važne za dalju pretragu i pronalaženje psa. Još jedna od funkcionalnosti koja je planirana je integracija sa SMS servisom, da prilikom ubacivanja sličnog oglasa, vlasniku stigne poruka o tome. Takođe će se koristiti neuronske mreže kao oblik implementacije sistema veštačke inteligencije, koji će omogućiti provere da li se slični oglasi odnose na konkretnog psa. Na sajtu će biti dodata anketa koju će popunjavati korisnici, a njeni rezultati će doprineti daljem napretku i korigovanju postojećeg stanja, a u planu je i izrada mobilne aplikacije.

## LITERATURA

- [1] Kannan, P. and Li, H. "Digital marketing: A framework, review and research agenda", *International Journal of Research in Marketing*, Vol. 34, No. 1, pp 22-45, 2017.
- [2] Pinheiro, M., Tiago, M. and Veríssimo, J. "Digital marketing and social media: Why bother?", *Business Horizons*, Vol. 57, No. 6, pp 703-708, 2014.
- [3] Leeflang, P., Verhoef, P., Dahlström, P., and Freundt, T. "Challenges and solutions for marketing in a digital era", *European Management Journal*, Vol. 32, No. 1, pp 1-12, 2014.
- [4] Radenković B., Despotović-Zrakić, M, Bogdanović. Z., Barać, D. i Labus, A., *Elektronsko poslovanje*, Fakultet organizacionih nauka, 2015.
- [5] Lazarević, S., Juranović, J., Končarević, R. i Đorđević, K., *Projektovanje softvera*, Fakultet organizacionih nauka, 2016.
- [6] Yoo, J., Arnold, T. and Frankwick, G. "Effects of positive customer-to-customer service interaction", *Journal of Business Research*, Vol. 65, No. 9, pp 1313-1320, 2012
- [7] Gruen, T., Osmonbekov, T. and Czaplewski, A. "eWOM: The impact of customer-to-customer online know-how exchange on customer value and loyalty", *Journal of Business Research*, Vol. 59, No 4., pp 449-456, 2016.
- [8] Stein, A. and Ramaseshan, B. "Towards the identification of customer experience touch point elements", *Journal of Retailing and Consumer Services*, Vol. 30, pp 8-19, 2016.
- [9] Munk, M, Vrabelová, M. and Kapusta, J. "Probability modeling of accesses to the web parts of portal", *Procedia Computer Science*, Vol. 3, pp 677-683, 2011.
- [10] Nam, J, "Understanding the motivation to use web portals", *Computers in Human Behavior*, Vol. 36, pp. 263-273, 2014.

# UNAPREĐENJE RADA APOTEKE PRIMENOM B2C I G2B FORMI E-POSLOVANJA

## IMPROVE THE WORK OF THE PHARMACY BY USING B2B AND G2B FORMS OF E-BUSINESS

Aleksandar Barbul, Doc.dr Tatjana Stojadinovic, Prof.dr Miodrag Brzaković  
*Fakultet za menadžment, ekonomiju i finansije, Beograd*

**Sadržaj** – U ovom radu je pored značaja razvoja e-poslovanja u zdravstvu i farmaciji, prikazana i metodologija razvoja e-poslovanja u farmaceutskim ustanovama. Naveden je primer koji se odnosi na primenu ove metodologije u apotekama Džavić. Primena savremene elektronske forme G2B poslovanja omogućava unapredjenje poslovanja apoteka interaktivnim radom sa Agencijom za lekove i medicinska sredstva Srbije.

*Ključne reči:* e-poslovanje, farmacija, lekovi

**Abstract** - U ovom radu je pored značaja razvoja e-poslovanja u zdravstvu i farmaciji, prikazana i metodologija razvoja e-poslovanja u farmaceutskim ustanovama. Naveden je primer koji se odnosi na primenu ove metodologije u apotekama Džavić. Primena savremene elektronske forme G2B poslovanja omogućava unapredjenje poslovanja apoteka interaktivnim radom sa Agencijom za lekove i medicinska sredstva Srbije.

*Key word:* e-business, pharmacy, medicines

### 1. UVOD

Današnjica, živimo u 21. veku za koji kažu da je vek brzog života. Uz taj tempo života nam doprinosi tehnologija koja se razvija još brže koju je jednostavno teško pratiti, kako bi dostigli taj tempo, treba biti jedan korak ispred i razmišljati unapred, konstantno gledati u budućnost.

Brzi razvoj informaciono komunikacionih tehnologija dovodi do sve veće primene e-poslovanja u farmaciji i zdravstvu.

E-poslovanje u farmaciji i zdravstvu, a posebno u apotekama doprinosi efikasnijem poslovanju apoteke, boljem informisanju pacijenata o registrovanim lekovima i medicinskim sredstvima, o uputstvima za lek i medicinsko sredstvo, o neželjenim reakcijama na lek, a sve u cilju bolje zdravstvene zaštite pacijenata.

### 2. E-POSLOVANJE U FARMACIJI I APOTECI

Nova istraživanja u oblasti farmacije, zdravstva i regulative lekova, sinteza farmakoloških informacija, primena Informacionih tehnologija, omogućava šira saznanja o lekovima, definisanja novih pristupa u lečenju, unapređenje koncepta rasuđivanja i edukacija o lekovima i o lečenju pacijenata.

Ključni elementi za uvođenje jedinstvenih, standardnih, jednoznačnih identifikatora za farmaciju su jedinstvena numeracija i indetifikacija proizvoda, jedinstven jezik poslovnog komuniciranja, šire i čvršće povezivanje proizvođača lekova, farmaceutskih organizacija i zdravstvenih institucija kroz efikasnije inforisanje i bolju saradnju, povećanje proizvodnje i racionalnost poslovanja i zaštita korisnika farmaceutskih proizvoda i bolja farmaceutska zdravstvena zaštita uz prihvatanje međunarodnih standarda, planiranje potrebnih vrsta i količina lekova i ostalih sredstava, smanjenje zaliha i racionilazacija i efikasnije usmeravanje sredstava i elektronska razmena recepta i obezbeđenje sigurnog transfera informacija, obezbeđenje podata o rokovima, upotrebe i način čuvanja lekova.

U farmaciji, zdravstvu i regulativi lekova se najčešće koriste sledeći alati informacionih tehnologija.

- Elektronski zdravstveni zapis
- Baza podataka
- Internet
- Umrežavanje i telemedika
- Elektronske zdravstvene kartice
- Elektronski dnevnici za pacijente

Ovaj rad prikazuje primenu elektronskog poslovanja u zdravstvenoj ustanovi apoteka "Džavić", koja je osnovana 1993. godine kao deo porodične firme sa ciljem da se u ovoj delatnosti dokaže sa visokim nivoom usluge i prihvatljivim cenama.

U poslovanju apoteka Džavić primenjuje se B2C (Business to Customer) forma elektronskog poslovanja koja omogućava poslovanje između apoteke i građana, kada je u pitanju prodaja lekova, medicinskih sredstava, preparata i slično, ali i primenu G2B (Government to Business) forme e-poslovanja kada je u pitanju unapredjenje poslovanja apoteka interaktivnim radom sa Agencijom za lekove i medicinska sredstva Srbije. U cilju bržeg, boljeg i merodavnijeg informisanja građana, odnosno pacijanata o lekovima i medicinskim sredstvima.

Tim apoteka "Džavić" se sastoji od 23 visoko kvalifikovanih farmaceuta i farmaceutskih tehničara.

Cilj poslovanja apoteke je konstantno praćenje novosti i na tržištu i uvođenje novih preparata u prodaju uz saradnju sa lekarima konsultantima i stalnim promocijama.



### 3. DEFINISANJE METODOLOGIJE I STRATEGIJE E-POSLOVANJA U APOTECI

Metodologija razvoja e-poslovanja apoteke obuhvata definisanje strategije razvoja e-poslovanja, definisanje internet biznis plana, implementaciju internet biznis plana i izradu veb sajta i veb aplikacija i unapredjenje poslovanja apoteke primenom savremenih elektronskih formi e-poslovanja.

U okviru strategije e-poslovanja apoteke definišu se osnovne aktivnosti apoteke, misija, vizija i ciljevi apoteke.

Osnovne aktivnosti apoteke su:

- Nabavka lekova - predstavništva i zastupništva
- Veleprodaja lekova - veledrogerije
- Proizvodnja lekova i medicinsko snabdevanje
- Nabavka Vitamina i suplemenata, raznih preparata, kozmetičkih proizvoda, preparati za bebe i hrana, Igračke

Apoteke "Džavić" za građane izdaju lekove na recept kao u državnim apotekama. Dobavljaju dekorativnu kozmetiku, igračke za kreativni razvoj dece, prave preparate za vene, gljivične infekcije, Šampone ...

Misija i vizija - Od osnivanja apoteke pre više od 23 godine, kompanije se razvija vrlo dinamično čineći jednu od retkih apoteka koje su veoma posvećeni svojim kupcima, pacijentima i poslovnim saradnicima. Pritom je sebi odredila jasnu viziju da budu u vrhu najboljih apoteka u Beogradu. Samim tim što su među prvima uveli prodaju lekova na recept. Što čini olakšicu starijim ljudima. Uz podršku celog kolektiva na svim lokacijama cilj apoteka je da se plasira elektronski da se napravi veb strana na kojoj će biti moguć pregled lekova, koji su povezani za registar lekova.

Cilj veb strane je takođe da se implementira online časkanje koje će omogućiti da svaki pacijent bude u mogućnosti da sazna podatke i da dobije konsultaciju od farmaceuta o određenom leku, ili da postavi pitanje vezane za svoj problem, zabrinutost.

Strateški ciljevi ove apoteke jeste da se plasira da bude prva u 21. veku na tržište elektronskog poslovanja. Ovaj vid poslovanja je u ranom razvitku u našoj zemlji.

Retke su apoteke koje imaju veoma dobro razvijen veb sajt i elektronsko poslovanje.

Cilj apoteka Džavić jeste da uvede i jedan novi vid poslovanja koji bi vezan za veb sajt i za mobilnu aplikaciju jeste dostava lekova na kućnu adresu.

Ovaj vid poslovanja u Srbiji ne postoji. Samim tim treba napraviti veoma dobar biznis plan što se tiče dostave. U početku vid poslovanja bio bi vezan za svaku apoteku zasebno.

Uvodilo bi se dostava lekova na svih 7 lokacija apoteka, i u krugu od 10 kilometara tih istih apoteka bi se vršila dostava.

### 4. SITUACIONA ANALIZA

Situaciona analiza obuhvata istraživanje marketinga, analizu konkurencije, analizu resursa, analizu okruženja, SWOT analizu i segmentaciju tržišta.

Istraživanje marketinga- Tržište apoteka je veoma veliko, posebno u većim gradovima. Podatak iz 2016. godine je da u Srbiji broj apoteka približan broju od 4100. Što neke čine državne a veći broj privatne farmaceutske apoteke. Farmaceutsko tržište u Srbiji je veoma dobro snabdeveno i da su svi lekovi koji se mogu naći prošli Agenciju za lekove.

Segmentacija tržišta - Kao što je gore u tekstu navedeno apoteka postoji već 23. godine i uspeli su da se prošire čak na sedam lokacija. Ova kompanija se trudi da bude inovativna i sa ovim predlogom za kreiranje veb strane, i aplikacije pa čak i dostave lekova izbacije sebe i svoje preduzeće na vrh lestvice i učiniće veoma jak udarac na svoje konkurente. Načini poslovanja apoteka "Džavić" se baziraju na klasičnoj prodaji i plasiranju lekova u samim apotekama. U pitanju je tržište okoline na svih 7 lokacija. Planirano je da pomoću veb strane se upute građani o mogućnosti poručivanja preko veb strane ili preko mobilne aplikacije i dostave ako to sam korisnik želi ili pak da dođu i sami pakupe proizvod u naznačenoj lokaciji.

Analiza okruženja - Uzećemo za primer apoteku na lokaciji "Beograd, Bežanijska kosa, Vajara Živojina Lukića 6". Nalazi se u mirnom kraju Beograda, blok 49, između dva velika naselja u takzvanoj prvoj mesnoj zajednici. Radno vreme apoteke je od 7 časova do 23. U krugu od 5km možemo naći barem desetak apoteka koji imaju slično radno vreme. Jedino što izdvaja apoteku na ovoj lokaciji jeste to, što pre otvaranje apoteke "Džavić" na ovoj lokaciji je i pre toga bila apoteka, koja je imala veoma dobru reputaciju. Nakon zatvaranje te apoteke došao je red na apoteku "Džavić" koja je bila upoznata sa radom predhodne i potrudila se da od otvaranja pruži ako ne istu onda i bolju, kvalitetniju uslugu za vrednost koju su dali. Do 2012 godine direktna konkurencija na ovu apoteku bila je apoteka nedaleko od nje, na nekih 300 metara koja je radila na principu 24 časa dnevno.

Analiza resursa - Iako su lokacije apoteka generelano pozicionirane u Beogradu, u samim apotekama radi 23 veoma odlično školovanih farmaceuta, koji imaju niz godina iskustva u samoj delatnosti i u radu sa kupcima. Pored samih farmaceuta postoji naravno i vlasnik. Sticajem okolnosti svih 7 apoteka imaju veću kvadraturu od 40 metara kvadranih, samim tim postoji mogućnost da ne bi trebalo da bude problema sa mogućim "dramatičnim promenama" za koje postoji indikacija da će apoteke u Srbiji morati da obezbede minimum 40 metara kvadratnih.

Analiza konkurencije - Konkurencija, će uvek postojati, ako ne postoji konkurencija to nije dobro. Zbog toga što ne uviđaju se lične greške, teško je sagledati sopstveni rad, valja imati nešto čime se možemo uporediti. "Lilly drogerie" predstavlja jedan vid konkurencije. Imaju veliki asortiman, ulažu u marketing, i promidžbeni program, flajere i akcije. Imaju zaseban deo gde im se nalazi apoteka, što neki kupci nisu primetili, ili jednostavno u trenutku se nisu setili da na tom mestu mogu kupiti lek ili pak posavetovati se. Ono što bi će apoteku "Džavić" izdvojiti jeste ta veb stranica, mobilna aplikacija, i dostupnost kupcima.

SWOT analiza je prikazana u Tabeli 1.

SWOT analiza obuhvata prikazivanje snage, slabosti, šansi i pretnji i to:

S – STRENGTH – snaga,  
W – WEAKNESSES – slabost,  
O - OPPORTUNITY – šansa,  
T – THREAT – pretnja

Tabela 1. SWOT analiza apoteke

SNAGA	SLABOST	ŠANSA	PRETNJA
Apoteka na više lokacija	Konstatno otvaranje novih apoteka u okruženju	Probijanje na tržište sa novim	Neobrazovanost korisnika za mobilne aplikacije
Rad dug niz godina	Loš marketing	Dostava lekova	Greške korisnika pri porudžbini lekova
Profesionalni kadar	Retke akcije	Brz odgovor na pitanje korisnika	
Dobre lokacije apoteka	Velika ulaganja	Savremena upotreba ePoslovanja	
	24/7		

## 5. INTERNET BIZNIS PLAN I IMPLEMENTACIJA E-POSLOVANJA

Razvoj internet biznis plana obuhvata: definisanje internet biznis plana, izradu i implementaciju veb sajta i kontrolnu fazu.

Bitni elementi koji čine internet biznis plan za apoteku koji u radu opisujem jesu:

- Odabir firme za pravljenje veb stranice
- Pravljenje mobilne aplikacije za različite platforme
- Implementacija dostave na veb stranu i mobilnu aplikaciju
- Upoznavanje korisnika sa mogućnostima da informacije o lekovima dobijaju na veb strani i

mobilnoj aplikaciju, sa obraćanjem farmaceuta u apotekama

- Pravljenje mape za dostavu radi lakšeg upoznavanja korisnika

Očekivano je da u početku sve to teče polako, dok se korisnici upoznaju sa datim procesima, sa veb stranama, dostavom i mobilnom aplikacijom.

Potrebno je nakon izvršenih proba i puštnje u rad, objasniti svakom novom kupcu da od sada postoji mogućnost završavanje putem interneta.

### Ciljevi veb sajta su:

- Upoznavanje korisnika sa veb sajtom
- Informisanje kupaca o mogućnostima poručivanja
- Informisanje kupaca o dostavi lekova uz uvid recepta online ili prilikom pouzeca
- Proširenje pristupačnosti apoteke sa dostavom
- Otvaranje novog vida poslovanja koji još uvek nije dostupa na našem tržištu
- Stvaranje novih kanala prodaje
- Uvođenje novih tehnologija u poslovanje
- Podrška tradicionalnom poslovanju
- Informatičko okruženje u svakoj apoteci bi činili personalni računari, sa konekcijom na internet, zatim štampač, skener, mobilni telefon sa Android aplikacijom, telefon za brz odgovor klijenata. Od operativnih sistema bi se koristili Windows 10 i Android.
- Marketinški treba pažljivo plasirati proizvod, da korisniku ne bude konfuzno i da mu pokažemo na što prostiji način, da bi izbegli negativnost i odbijanje na nešto inovativno i novo.
- Veb strana i mobilna aplikacija bi na početnim stranama imala nove akcije i mogućnost prijave korisnika radi lakšeg poslovanja sa klijentima. Unositi lokaciju na kojoj se korisnik nalazi i proveriti da li dostava važi za njegovu lokaciju.

U apotekama bi se uveo mobilni telefon ili laptop računari da bi farmaceuti mogli da odgovoraju na postavljena pitanja kupaca.

Samim tim bi doveli kupca u veoma veliku prednost, ne moraju da izlaze iz kuće a dobijaju profesionalnu informaciju o datom pitanju ili problemu.

Mane pri mobilnoj aplikaciji bi bila ta što osobe starije, koje su u penziji retko imaju smart telefone, pa ne bi bili toliko upoznati i ta ciljna grupa bi bila u zaostatku.

Ali svakako imaju mogućnost poziva telefonom apoteku i dobijanje informacije od farmaceuta i mogućnost pravljenja porudžbenice preko telefona.

Osim što bi to u početku bilo u zaostatku zbog ispitivanja tržišta i pregleda da li je potrebno uvesti centar samo za telefonske porudžbine. Treba videti koliko je to zastupljeno i naći najbolje rešenje.



Implementacija veb sajta radila bi se u fazama, kako se optimizovao proces odgovora farmaceuta na kupce, zatim obezbedio i obavestio korisnik o mogućnostima preko mobilnog telefona odnosno misli se na Android aplikaciju i u poslednjoj fazi bi se radilo na servisu dostava lekova na kućnu adresu u krugu označenom na mapi koja bi bila optimizovana za lokaciju koju bi korisnici podesili na svojim računarima ili na Android platformama.

Cilj samog internet poslovanja je taj da se uvede novi vid poslovanja u apotekama, da se koriste informacione tehnologije i da se bude u koraku sa vremenom i tržištem koji teži ka tome da im sve bude pristupačnije i prosto na jedan klik od samog mesta stanovanja.

Da se obezbedi bolja komunikacija između kupaca i farmaceuta, da ne postoji jaz i strah od nepoznatog.

Internet tržište što se tiče ovog vida poslovanja prosto ne postoji, možemo kod konkurencije naći samo informativni deo veb sajta koje neke apoteke poseduju.

## **6. UNAPREDJENJE POSLOVANJA APOTEKE PRIMENOM G2B FORME POSLOVANJA**

Prilikom plasiranja veb strane apoteka Džavić i prilikom puštanja Android aplikacije možemo uvideti da će se redovi u apotekama smanjiti, a zahtev za dostavu lekova i priliv pitanja od strane kupaca i korisnika povećati.

Prilikom posete samog sistema uviđamo da se svaki dan povećava broj prijava i registracija na sajtu i android aplikaciji.

Unapredjenje poslovanja apoteka je postignuto i primenom G2B formi e-poslovanja i to razvojem poslovanja apoteka i Agencije za lekove i medicinska sredstva Srbije.

Agencija za lekove i medicinska sredstva Srbije (ALIMS) osnovana je 1. oktobra 2004. godine na osnovu Zakona o lekovima i medicinskim sredstvima (Sl. glasnik RS, broj 84/04, 85/05 i 36/09-dr. zakon).”

Misija ALIMSa je da doprinese ostvarivanju osnovnog ljudskog prava za pristup kvalitetnim, bezbednim i efikasnim lekovima i medicinskim sredstvima, kao i da promovise i unapredi zdravlje ljudi i životinja kroz: izdavanje dozvola za stavljanje u promet isključivo kvalitetnih, bezbednih i efikasnih lekova i medicinskih sredstava, pružanje adekvatnih informacija, kako bi upotreba tih lekova i medicinskih sredstava bila bezbedna i racionalna. A i pri tome činiti i kontrolu kvaliteta lekova i medicinskih sredstava, koja je u potpunosti usaglašena sa svim nacionalnim i međunarodnim zakonima i standardima.

Vizija je je da bude moderna, efikasna i društveno odgovorna institucija, koja će postati lider u regionu jugoistočne Evrope. Viziju ostvaruje kroz efektivne i efikasne procese u okviru sistema menadžmenta

kvalitetom, usaglašenog sa zahtevima ISO 9001:2008, tako što uspostavlja:

Visoke standarde u postupku evaluacije dokumentacije, kontroli kvaliteta i pružanju adekvatnih informacija,

- Kontinuirano uči i razvija kompetentnosti,
- Kontinuirano poboljšava sistem menadžmenta kvalitetom,
- Izgradi jaku organizacionu kulturu i prepoznatljiv imidž,
- Ima lidersku ulogu rukovodstva u ostvarenju vizije.

Agencija za lekove i medicinska sredstva Srbije je nadležna da:

- Izdaje dozvole za lek, odlučuje o izmeni i dopuni, obnovi i prenosu, kao i prestanku važenja dozvole za lek;
- Vršiti upis medicinskog sredstva u registar medicinskih sredstava, odlučuje o izmeni i dopuni, obnovi upisa, kao i brisanju medicinskog sredstva iz registra medicinskih sredstava;
- Vršiti upis u registar tradicionalnih biljnih lekova, odnosno upis u registar homeopatskih lekova;
- Izdaje dozvole za sprovođenje kliničkog ispitivanja leka i medicinskog sredstva, odlučuje o izmeni i dopuni dozvole, odnosno protokola o sprovođenju kliničkog ispitivanja lekova, donosi odluke u vezi s prijavom kliničkog ispitivanja, vrši kontrolu sprovođenja kliničkog ispitivanja;
- Prati neželjene reakcije na lekove, kao i neželjene reakcije na medicinska sredstva;
- Izdaje uverenja za potrebe izvoza lekova i medicinskih sredstava u skladu s preporukama svetske zdravstvene organizacije;
- Odobrava uvoz lekova i medicinskih sredstava za lečenje određenog pacijenta ili grupe pacijenata, kao i lekova ili medicinskih sredstava za naučna i medicinska istraživanja;
- Vršiti kategorizaciju lekova, odnosno medicinskih sredstava;
- Odobrava oglašavanje lekova i medicinskih sredstava;
- Vršiti prikupljanje i obradu podataka o prometu i potrošnji lekova i medicinskih sredstava;
- Daje informacije i predloge za racionalno korišćenje lekova i medicinskih sredstava;
- Povezuje se sa međunarodnim mrežama informacija o lekovima i medicinskim sredstvima i sa agencijama nadležnim za lekove i medicinska sredstva i njihovim asocijacijama;
- Učestvuje u planiranju i sprovođenju sistematske kontrole lekova i medicinskih sredstava i uzimanju slučajnih uzoraka iz prometa;
- Daje mišljenja za uvoz i izvoz uzoraka ćelija, odnosno tkiva za postupak kliničkog ispitivanja lekovima;
- Vršiti kontrolu kvaliteta lekova i medicinskih sredstava;
- Priprema stručne publikacije iz nadležnosti Agencije;

Agencija aktivno učestvuje u razvoju farmaceutske delatnosti u Srbiji, izradi podzakonskih propisa, daljoj dogradnji nacionalne politike u oblasti lekova i medicinskih sredstava i međunarodnoj saradnji.

Agencija na svom veb sajtu ima razvijene Veb aplikacije koje omogućavaju pretraživanje lekova i medicinskih sredstava po različitim kriterijumima koje ću navesti u daljem tekstu.

Takodje, korišćenjem otvorenih podataka omogućeno je povbezivanje sa apotekama po pitanju merodavnih podataka o lekovima i medicinskim sredstvima.

Na osnovnoj strani ALIMSa nalaze se Veb aplikacije koje omogućavaju:

- Pretraživanje registrovanih lekova u humanoj medicini
- Pretraživanje registrovanih lekova u veterinarskoj medicini
- Pretraživanje registrovanih medicinskih sredstava
- Pretraživanje sertifikata humanih lekova
- Pretraživanje sertifikata veterinarskih lekova
- Pretraživanje veterinarska medicinska sredstava
- Pretraživanje odobrenih kliničkih ispitivanja
- Pretraživanje uvoznih dozvola za lek

Prilikom odlaska na sajt ALIMS-a moguće je odabrati oblast pretrage koje smo gore napomenuli.

Navedene Veb aplikacije omogućavaju farmaceutima u apoteci da u svakom trenutku imaju pravu informaciju da li je neki lek ili medicinsko sredstvo registrovano u Republici Srbiji i da li je izvršeno laboratorijsko ispitivanje leka odnosno medicinskog sredstva.

Navedene aplikacije omogućavaju inspektorima Ministarstva zdravlja da pretraže na licu mesta u samoj apoteci da li apoteka sadrži samo lekove koji se mogu biti u prometu.

Veb aplikacija „Pretraživanje registrovanih lekova u humanoj medicini“ omogućava pretraživanje po različitim kriterijumima kako bi korisniku aplikacije bilo omogućeno da što lakše dođe do tražene informacije o leku u humanoj medicini.

Da li to bio farmaceut ili fizičko lice svakako odlaskom na ovu stranicu može se učiniti pretragu. Svakako aplikacije koje nam je ALIMS omogućio čini veoma naprednu i korisnu bazu podataka.

Za koju je moguće u bilo kom trenutku uraditi pretragu i saznanje o leku, da se učini provera da li je registrovan lek i dali je laboratorijski ispitan u Republici Srbiji.

Neke od stavki koje je potrebno uneti za pretragu humanih lekova jeste: "Naziv leka, Generički naziv leka, proizvođač leka, nosioci dozvola, režim izdavanja, ATC šifra, JKL, Broj rešenja, datum rešenja, vrsta leka". Svakodnevno se vrši ažuriranje lekova.

Zanimljivo je da prilikom klika na taster pretraživanje dobijamo izlistane lekove, koji ukupno čine 6603 leka.

## 7. ZAKLJUČAK

Apoteke i farmaceutske tržište će uvek postojati, jer je potrebno građanima odnosno pacijentima.

Informacije o lekovima i medicinskim sredstvima će uvek biti neophodne građanima odnosno pacijentima.

Važno je da informacije o lekovima i medicinskim sredstvima budu tačne i merodavne.

Možda će neke apoteke biti više pristupačnije a neke manje, to sve zavisi od obrazovnog kadra i resursa koji će svaka apoteka imati, i za koje će zaposlene omogućiti određen način poslovanja.

Samim tim ukoliko se obezbedi lakši brži i efikasniji posao počev od farmaceuta, više će imati mogućnosti da se bave kupcima, korisnicima, i klijentima.

Sa ovim napretkom u 21. veku kao što tehnologija utiče na svet oko nas tako, možemo uzeti u obzir tu mogućnost elektronskog poslovanja i načiniti nam tržište lakšim pristupačnijim i savremenijim, a samim tim korisnike, kupce, klijente i poslovne partnere sretnijim.

Ovaj vid poslovanja koji smo prikazali u radi iako je tek u razvitku, verujemo da će se proširiti veoma brzo i naći svoje ciljno tržište, a time što pre nađemo ciljno tržište, možemo se razviti i prilagoditi, čim dobijem prve odgovore i sami korisnici, klijenti i poslovni partneri će nam omogućiti usavršavanje naših elektronskog poslovanja.

## LITERATURA

- [1] Tatjana M. Stojadinović, *Elektronsko poslovanje u regulativi lekova i medicinskih sredstava kao osnov za razvoj eFarmacija i eZdravstva, 2017*
- [2] <http://www.farmacijamedicina.rs/kompanije/lekovi/apoteke/apoteke-dzavic-lekovi-preparat-pregledan>
- [3] <http://www.mirandre.com/zravstvena-ustanova-apoteka-dzavic-pregledan>
- [4] <https://www.blic.rs/vesti/drustvo/farmaceutska-komora-potreban-jedinstveni-registar-apoteka-i-cene-lekova/sblkg11>
- [5] <https://www.alims.gov.rs/ciril/>

# POBOLJŠANJE SPREMNOSTI DRŽAVNIH ORGANA REPUBLIKE SRBIJE ZA ODGOVOR NA SAJBER NAPADE

## IMPROVING CYBER READINESS OF THE GOVERNMENT BODIES OF THE REPUBLIC OF SERBIA

Marko Krstić<sup>1</sup>, Dušan Raičević<sup>2</sup>

*Regulatorna agencija za elektronske komunikacije i poštanske usluge<sup>1</sup>  
Ministarstvo odbrane Republike Srbije<sup>2</sup>*

**Sadržaj** – Digitalizacijom i uvođenjem elektronske uprave povećava se broj usluga koje je moguće ponuditi korisnicima, ali samim tim raste i verovatnoća pojave nekog od bezbednosnih propusta. U ovom radu je opisan softverski alat koji daje mogućnost planiranja i realizacije različitih scenarija mrežnih napada. Primenom Blue Team Training Toolkit (BT3) softvera može da se uštedi dosta vremena, novca i opreme što daje mogućnost češćeg uvežbavanja odgovora na različite tipove sajber napada. Češćim uvežbavanjem ljudi, njihovim upoznavanjem i praktičnim radom sa novim izazovima u sajber prostoru kao i kroz saradnju državnih institucija povećava se bezbednost informaciono-komunikacionih (IKT) sistema.

**Abstract** – Digitisation and the introduction of electronic administration increases the number of services that can be offered to users, but as a result, the possibility of occurrence of some of the security deficiencies increases. This paper describes a software tool that provides the ability to plan and realize various scenarios of network attacks. Using the Blue Team Training Toolkit (BT3) software can save a lot of time, money, and equipment, giving you the ability to practice responses to different types of cyber attacks, frequently. Increased training of people, introduction and practical work with new challenges in the cyber space, as well as the cooperation of state institutions, increases the security of information and communication (ICT) systems.

### 1. UVOD

Digitalizacija i uvođenje elektronske uprave će građanima Republike Srbije omogućiti lakše i efikasnije korišćenje usluga koje pruža država [1]. Međutim, pored svih prednosti koje ovaj proces donosi, treba imati u vidu da se sa povećanjem broja elektronskih usluga i obima digitalizovanih podataka stvaraju dodatne mogućnosti za sajber napade. Prema poslednjem istraživanju Evropske agencije za bezbednost mreža i podataka (ENISA) 35,4% od ukupnog broja slučajeva povrede podataka se dešava u zdravstvenom sektoru, 8,1% u vladi/vojsci i 7,4% u obrazovnom sektoru [2]. Ovi podaci jasno ukazuju na to da zaposleni u državnim organima treba da budu obučeni da detektuju sajber napade i adekvatno reaguju na njih.

Iako postoje različiti načini obuke, posebno je interesantna obuka zaposlenih kroz sajber vežbe na kojima učesnici mogu da se upoznaju sa celim procesom

primene mera zaštite, kao i sa novim i aktuelnim sajber napadima koji još uvek nisu uključeni u sertifikovane obuke.

U ovom radu smo najpre naveli sve institucije koje se bave informacionom bezbednošću u Republici Srbiji, opisali način koordinisanja njihovog rada i analizirali trenutno primenjivane načine izvođenja sajber vežbi, a zatim i predložili novi način organizovanja sajber vežbe koji bi omogućio lakšu razmenu znanja i obuku većeg broja ljudi.

### 2. INSTITUCIJE KOJE SE BAVE INFORMACIONOM BEZBEDNOŠĆU U REPUBLICI SRBIJI

Dobra komunikacija i koordinacija između institucija zaduženih za poslove informacione bezbednosti su ključne za uspešno funkcionisanje IKT sistema na nacionalnom nivou [3].

Na osnovu Zakona o informacionoj bezbednosti [4] (u daljem tekstu Zakon) u Republici Srbiji je osnovano Telo za koordinaciju poslova informacione bezbednosti kao koordinaciono telo Vlade. Članovi ovog koordinacionog tela su predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Uprave za zajedničke poslove republičkih organa i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalnog CERT-a).

U cilju unapređenja pojedinih oblasti informacione bezbednosti, Zakon predviđa formiranje stručnih radnih grupa Tela za koordinaciju u koje se dodatno uključuju i predstavnici drugih organa javne vlasti, privrede, akademske zajednice i nevladinog sektora.

### 3. OBLICI IZVOĐENJA SAJBER VEŽBI U REPUBLICI SRBIJI

Jedan od vidova saradnje i razmene znanja u oblasti informacione bezbednosti u okviru Republike Srbije je organizovanje sajber vežbi.

Prema klasifikaciji sajber vežbi dostupnoj u izveštaju Evropske agencije za bezbednost mreža i podataka [5],

vežbe u Republici Srbiji se mogu podeliti na *table-top* vežbe i vežbe sa potpunom simulacijom aktivnosti napada i odbrane.

*Table-top* vežbe služe za razmatranje planova i procedura koje bi se koristile u slučaju sprovođenja predefinisano scenarija. Relativno ih je lako organizovati, pa ne čudi činjenica da je najveći broj vežbi izvedenih u Republici Srbiji upravo ovog tipa. Najveća mana *table-top* vežbi je što ne pružaju mogućnost stvarne reakcije učesnika, već se sve završava na nivou diskusije.

Zbog kompleksnosti organizovanja vežbi sa potpunom simulacijom napada i odbrane, kao i opreme i ljudstva neophodnih za njihovo uspešno izvođenje, u Republici Srbiji postoji samo jedna vežba ove vrste. Vežba pod nazivom "Cyber Tesla", koja se održava jednom godišnje, je jedina prilika za IT stručnjake da uvežbavaju odgovore na sajber napade u realnom vremenu.

Imajući u vidu da je praktičan rad najbolji način za profesionalno usavršavanje [6], lako je uočiti potrebu za većim brojem sajber vežbi čiji učesnici bi mogli da uvežbavaju odgovore na sajber napade u realnom okruženju, a ne samo na nivou diskusije.

#### 4. IZVOĐENJE SAJBER VEŽBE POMOĆU BT3 ALATA

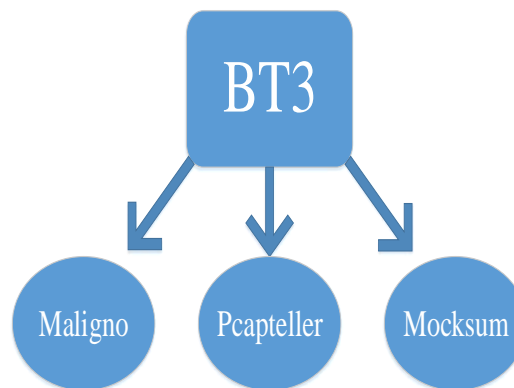
Prilikom odabira načina izvođenja sajber vežbe neophodno je uzeti u obzir sledeće aspekte:

- vreme potrebno za implementaciju okruženja u kojem se scenario izvršava,
- cenu,
- rizik po produkciono okruženje, i
- realističnost okruženja u kojem se vežba izvodi.

Iako su ovi aspekti vežbi međusobno povezani i u većini slučajeva ograničavaju jedni druge, pametnim izborom alata za kreiranje i izvođenje vežbi ova ograničenja se mogu prevazići.

*Blue Team Training Toolkit* (BT3) je alat koji organizatorima sajber vežbi daje mogućnost da efikasno, uz uštedu novca i vremena, naprave što je moguće realniji scenario mrežnog napada, vodeći računa da pritom ne izazovu nikakav rizik po produkciono okruženje [7]. Napisan je u programskom jeziku *Python* i dostupan za korišćenje kao *FreeBSD* softver otvorenog koda. BT3 pruža mogućnosti analize, reprodukcije i modifikacije mrežnog saobraćaja, uvežbavanja odgovora tima zaduženog za reagovanje na incidente (*plavog tima* – prema terminologiji sajber vežbi), i simulacije napada tima čiji je cilj da naruši informacionu bezbednost (*crvenog tima* – prema terminologiji sajber vežbi). Ove funkcionalnosti su realizovane kroz tri različita modula:

- *Maligno*,
- *Pcatteller* i
- *Mocksum*.

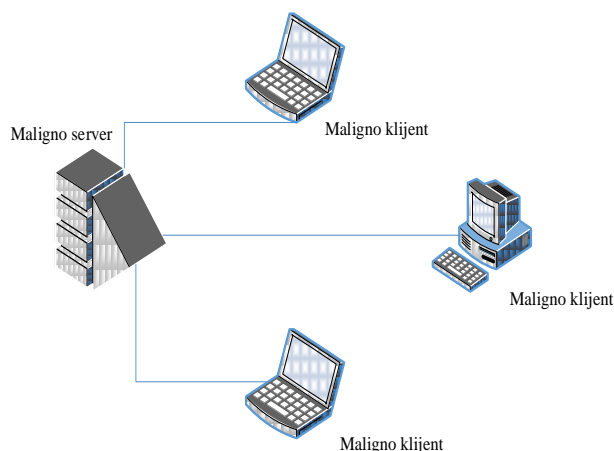


Slika 1. Moduli alata BT3

#### 4.1. MODULI ALATA BT3

*Maligno* je modul dizajniran za simuliranje napada sa fiktivnim zlonamernim softverom i napada sa uspostavom konekcije kroz koju se sa udaljene lokacije mogu izvršavati komande na računaru koji je meta napada.

Kao što se može videti na slici 2, modul *Maligno* je baziran na klijent-server arhitekturi. *Maligno* server je integrisan sa alatom BT3 i moguće ga je pokrenuti na 64-bitnim verzijama operativnih sistema *Kali Linux* i *Ubuntu 16.04 LTS*, kao i sam alat BT3. Sa druge strane, klijente je moguće razmestiti na bilo kom računaru sa operativnim sistemom Microsoft ili Linux, što daje širok spektar mogućnosti organizovanja scenarija napada. Kako su klijenti u stvari *Python* skripte koje *Maligno* server generiše, neophodno je na računare koji će simulirati mete napada instalirati Python 2.7. Komunikacija između servera i klijenata se bazira na protokolima *HTTP* ili *HTTPS*, koji se u praksi veoma često koriste za distribuciju zlonamernog softvera. Imajući u vidu raznolikost okruženja u kojima se potencijalno može koristiti *Maligno* modul, klijenti su napravljeni tako da budu svesni postojanja *proxy* servera u mreži i mogu uspostaviti komunikaciju sa *Maligno* serverom i u ovim okolnostima.



Slika 2. Maligno klijenti se mogu distribuirati na više računara u mreži

*Maligno* modul sadrži šest opcija koje je moguće definisati po željenim vrednostima. *LHOST* definiše *IP* adresu ili domensko ime (*FQDN*) hosta na kom će server da se nalazi. Na osnovu ovog parametra klijenti znaju kome da se obraćaju. *LPORT* govori klijentima preko kog *TCP* porta da se obrate serveru. *PROFILE* je u stvari ime profila indikatora napada. Indikator je programiran u programskom jeziku *Python* i u njemu je definisana komunikacija između servera i klijenta, koja može biti veoma kompleksna, a u zavisnosti od napada koji se simulira. U okviru samog alata *BT3* postoje već definisani indikatori, ali i sam korisnik može dodati nove napade koji mogu biti interesantni njegovoj organizaciji. U okviru opcije *SSL* definiše se da li će se za konekcije koristiti *SSL* (*Secure Socket Layer*) ili *TLS* (*Transport Layer Security*). Pored polja *SSL* postoji i *SSL\_CERT* u kom izdajemo sertifikat generisan tokom instalacije alata *BT3*. Da bi se polje *SSL\_CERT* koristilo, potrebno je da *SSL* bude omogućen i da se definisani sertifikat za potpisivanje, nalazi u direktorijumu "*certs*" unutar instalacionog foldera alata *BT3*.

*Pcatteller* modul pruža mogućnost reprodukcije *IP* paketa snimljenih u *PCAP* (*packet capture*) fajlovima, kao i mogućnost modifikovanja informacija sadržanih u zaglavlju *IP* paketa. Korišćenjem ovog modula moguće je saobraćaj snimljen tokom napada ili neke sajber vežbe prilagoditi tako da izgleda kao da se napad dešava u posmatranoj mreži ili nekom drugom okruženju za izvođenje sajber vežbe. Sa druge strane crveni tim koji ima dovoljno informacija o mreži, koristeći *Pcatteller* modul i *VPN* (*Virtual Private Network*) pivotiranje može izazvati diverziju u mreži, tako da plavi tim navede da istražuje lažni napad dok se u pozadini dešava pravi napad.

Opcije koje su nam na raspolaganju u *Pcattelleru* služe za manipulisanje paketima. Opcija *File* definiše ime *PCAP* fajla, koji mora biti smešten u direktorijumu "*pcaps*" instalacionog foldera *BT3*. Ukoliko je potrebno omogućiti fragmentaciju paketa, to se može uraditi unutar opcije *FRAGMENTATION*. Ova opcija je veoma korisna ukoliko su paketi fajla *PCAP* dosta veći od maksimalne veličine paketa u mreži (*MTU*). Na raspolaganju je mogućnost konfigurisanja i *MTU* opcije vrednostima u opsegu od 1B do 9000B. Kroz *INTERFACE* opciju definišemo koji interfejs u lokalnoj mreži će biti korišćen za reprodukciju paketa. *IP* adresa, *MAC* adresa i zaglavlje paketa definišu se u opcijama *PCAP\_IP\_LIST*, *PCAP\_MAC\_LIST* i *PCAP\_PLD\_LIST*. *WIRE\_IP\_LIST* i *WIRE\_MAC\_LIST* su opcije u kojima definišemo vrednosti *IP* i/ili *MAC* adresa koje će se tokom reprodukcije saobraćaja koristiti umesto vrednosti koje se nalaze u poljima *PCAP\_IP\_LIST* i/ili *PCAP\_MAC\_LIST*. Opcijom *PROTOCOL\_LIST* definišemo protokole, na koje će se modifikacije paketa primeniti. Podržani protokoli su: "*DNS*", "*NBNS*", "*SMB*", "*RAW*". Ukoliko za vrednost u *PROTOCOL\_LIST* izaberemo "*DNS*", svi *DNS* paketi, zahtevi i odgovori, biće modifikovani u skladu sa podešavanjima. Vrednošću *RAW* moguće je kontrolisati *HTTP*, *UDP* ili *ICMP* pakete. Kod ovih paketa moguće je modifikovati samo *ASCII*

vrednosti iz dela paketa koji prenosi korisničke podatke (*payload*). Ukoliko želimo da se prilikom reprodukcije poštuje vreme između slanja paketa iz originalnog saobraćaja potrebno je podesiti *REAL\_TIME* opciju. Ukoliko ova opcija nije podešena svi paketi će biti ubačeni u mrežu odjednom.

*Mocksum* je modul koji omogućuje pristup fajlovima koji imitiraju zlonameran softver pomoću *MD5 hash* kolizija. Fajlovi preuzeti pomoću *Mocksuma* modula omogućavaju da se napadi što realnije simuliraju čak i u produkcijom okruženju jer ovi fajlovi ne predstavljaju nikakav rizik. Jedina sličnost koji ovi fajlovi imaju sa pravim zlonamernim softverom je ista vrednost *MD5 hash*-a. Kako većina antivirusnih programa na osnovu *MD5 hash* sume pretpostavlja da su fajlovi iz *Mocksum* modula zlonamerni, oni se mogu koristiti za simulaciju napada.

Komande *BT3* alata se mogu jednostavno i brzo naučiti jer su slične sa komandama *Metasploit Framework* alata koji je jedan od osnovnih alata za testiranje informacione bezbednosti [8]. Pa se tako za izbor modula koristi komanda *USE*, za pregled opcija u okviru modula komanda *SHOW*, za podešavanje opcija komanda *SET*, i za izvršavanje izabranih opcija u okviru modula komanda *RUN*.

## 4.2. KONKRETNA PRIMENA U REPUBLICI SRBIJI

Kako se *Maligno* modul može koristiti za simulaciju napada u produkcijom okruženju, nema potrebe za uspostavljanjem posebne infrastrukture za izvođenje vežbe pa je vreme potrebno za realizaciju vežbe kraće. Takođe sa povećanjem broja dostupnih indikatora profila, koje svaka od državnih institucija može pisati za svoje potrebe, a zatim i međusobno razmenjivati, broj različitih vežbi dostupnih svim institucijama će značajno porasti. Pored povećanja broja vežbi i smanjenja vremena potrebnog za obuku svih zaposlenih sa ovim zaduženjima, postoji još jedna dodatna prednost. Za razliku od vežbe "Cyber Tesla" gde učesnici koriste alate izabrane za realizaciju te vežbe, zaposleni će moći da koriste alate dostupne u njihovom produkcijom okruženju, pa će samim tim biti spremniji na reakciju u slučaju pravog napada.

Sa druge strane, *Pcatteller* modul se može iskoristiti za prilagođavanje i retransmisiju saobraćaja snimljenog tokom vežbe "Cyber Tesla" ili tokom stvarnog napada na neku od institucija. U cilju smanjenja rizika, zlonameran softver u snimku saobraćaja treba zameniti sa fajlovima dobijenim kroz *Mocksum* modul ako je to moguće, ili koristiti interno okruženju namenjeno za izvođenje vežbi. Modifikacijama dostupnim u okviru *Pcatteller* modula, snimak saobraćaja se može prilagoditi da odgovara korišćenom okruženju.

Sam *BT3* alat nudi mogućnost korišćenja 63 indikatora profila, 6 tipova fajlova koji imitiraju zlonameran softver, i 73 *PCAP* fajlova sa snimcima napada, koji se mogu koristiti u početnoj fazi. Kreiranje naloga za pristup ovim

fajlovima je besplatno, ali korišćenje pojedinih fajlova ipak zahteva njihovo plaćanje.

## 5. ZAKLJUČAK

Broj sajber vežbi za obuku IT osoblja koji se trenutno izvodi u Republici Srbiji nije ni približno dovoljan za obuku zaposlenih u državnim organima. Imajući u vidu da će digitalizacija i uvođenje elektronske uprave pored svojih dobrih strana doneti i mogućnost većeg broja raznovrsnijih sajber napada, potrebno je pronaći način za bolju saradnju državnih institucija i izvođenje većeg broja sajber vežbi u realističnim okruženjima.

U ovom radu smo razmotrili korišćenje BT3 alata za izvođenje sajber vežbi. Teorijska razmatranja pokazuju da se njegovim korišćenjem vežbe mogu realizovati u produkcionom okruženju efikasno, uz uštedu novca i vremena, sa realističnim scenarijem i bez opasnosti po samo okruženje. Zaposleni u toku vežbe koristi alate koji su mu dostupni u svakodnevnom poslu, pa će u slučaju pravog napada biti uvežbaniji i spremniji da adekvatno odgovori na ovaj napad

## LITERATURA

[1] e-Serbia Digital Reform 2018, Office for IT and eGovernment, No. 1, 2018.

[2] ENISA Threat Landscape Landscape Report 2017. [online][https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at\\_download/fullReport](https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport)

[3] S. A. Adams, M. Brokx, L. D. Corte, M. Galić et al. "The Governance of Cybersecurity, A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherland and in the UK", Tilburg Institute for Law, Technology, and Society Research Portal, 2015.

[4] Zakon o informacionoj bezbednosti, Službeni glasnik Republike Srbije, br. 6/16, str. 50-55, 2016.

[5] National and International Cyber Security Exercises: Survey, Analysis & Recommendations, ENISA, 2012. [online][https://www.enisa.europa.eu/publications/exercise-survey2012/at\\_download/fullReport](https://www.enisa.europa.eu/publications/exercise-survey2012/at_download/fullReport)

[6] S. Billett, "Learning through Practice" in S. Billet (eds.) Learning through Practice: Models, Traditions, Orientations and Approaches, Springer, 2010, pp. 1-20.

[7] User Guide Blue Team Training Toolkit (BT3). [online][https://www.encrypted.no/forskning/whitepapers/BT3\\_User\\_Guide.pdf](https://www.encrypted.no/forskning/whitepapers/BT3_User_Guide.pdf)

[8] N. Jaswal, "Approaching a Penetration Test Using Metasploit" in Mastering Metasploit, Packt Publishing, 2014, pp. 9-48.

# DIGITALNA TRANSFORMACIJA POSLOVANJA

## DIGITAL TRANSFORMATION OF BUSINESS

Predrag Matković<sup>1</sup>, Mirjana Marić<sup>1</sup>, Pere Tumbas<sup>1</sup>, Jovica Đurković<sup>1</sup>

*Univerzitet u Novom Sadu, Ekonomski fakultet u Subotici<sup>1</sup>*

**Sadržaj** - Digitalna transformacija poslovanja predstavlja intenzivan proces izgradnje potpuno nove organizacije, uz primenu digitalnih tehnologija. Značaj upotrebe digitalnih tehnologija u savremenim organizacijama je neosporiv, stoga su u radu prikazane ključne digitalne tehnologije i njihove implikacije na transformaciju poslovanja. S obzirom na to da je njihovo uvođenje potreban ali ne i dovoljan uslov za ostvarivanje boljih poslovnih rezultata organizacija, autori su analizom referentne literature, identifikovali i u radu ukratko opisali i druge elemente značajne u digitalnoj transformaciji. Cilj rada je da se organizacijama daju smernice za uspešnu realizaciju digitalne transformacije.

**Abstract** - Digital transformation of business is an intensive process of building an entirely new organization with the application of digital technologies. The significance of digital technologies in modern organizations is unquestionable, and therefore, this paper presents key digital technologies and their specific implications to business transformation. In view of the fact that their introduction is not enough to achieve better business results, the authors conducted a review of relevant literature to identify other elements of significance to digital transformation. The aim of this paper is to provide organizations with guidelines for successful realization of digital transformation.

### 1. UVODNA RAZMATRANJA

Proces digitalizacije je u tesnoj vezi sa upotrebom digitalnih tehnologija i u poslednjoj deceniji zahvatio je sve pore savremenog društva. Uticao je podjednako na promenu stila i kvaliteta života pojedinaca kao i na promenu uslova u kojima organizacije treba da posluju i obezbede konkurentne prednosti na tržištu. Digitalno doba svakodnevno postavlja pred organizacije brojne izazove, koji zahtevaju promene u njihovom poslovanju.

Organizacije su primorane da promene svoj tradicionalan način poslovanja, način svoje interakcije sa kupcima, partnerima, dobavljačima, i način na koji organizuju svoje poslovanje. Interesenti se u poslovanju kontinuirano i značajno menjaju. Zanemarivanjem ove činjenice, stvara se jaz između onoga šta organizacije očekuju od interakcije sa svojim okruženjem i onoga šta isto može da obezbedi kao odgovor na izazove savremenih digitalnih trendova, što generiše ogroman rizik za celokupno poslovanje organizacija [1].

Razumljivo je dakle zašto je termin „digitalna transformacija“ postao danas jedan od najčešće korišćenih termina. Međutim, mora se naglasiti da on ujedno

predstavlja i jedan od slabije istraženih i definisanih termina u naučnoj i stručnoj literaturi, što vodi ka ozbiljnoj konfuziji na tržištu, prilikom implementacije ovog procesa u praksi.

Bitno je istaći da se digitalizacija ne može svesti isključivo na tehnološka pitanja, jer ulaganje novca na uvođenje novih, digitalnih tehnologija, nije dovoljno za ostvarivanje boljih poslovnih ishoda organizacija. Naime, organizacije treba da identifikuju set svojih poslovnih mogućnosti koji treba menjati i transformisati, uz primenu adekvatne digitalne tehnologije, čime bi postali konkurentniji. Digitalizacija je strateški važna za organizaciju i postaje sve više pitanje menadžmenta organizacije. Nijedna od poslovnih promena koje omogućavaju savremene tehnologije ne može biti ni efikasna ni efektivna ukoliko je ne prate organizacione promene.

U skladu sa identifikovanim i ukratko opisanim predmetom istraživanja, definisano je istraživačko pitanje u radu: *koji su ključni elementi digitalne transformacije poslovanja?*

Sadržaj rada organizovan je u četiri poglavlja. U uvodnom poglavlju je opisan predmet istraživanja i definisano istraživačko pitanje na koje će se dati odgovor u radu. Nakon toga u drugom poglavlju, uvidom u referentnu naučnu i stručnu literaturu, razmatra se pojam i sadržaj digitalne transformacije poslovanja. Pravi se distinkcija tradicionalne strategije implementacije informacionih tehnologija (nadalje IT), digitalne strategije i strategije digitalne transformacije. Treće poglavlje rada prikazuje neke od ključnih digitalnih tehnologija i njihove implikacije na transformaciju poslovanja. U poslednjem, četvrtom poglavlju, daju se zaključna razmatranja i smernice za uspešnu realizaciju digitalne transformacije.

### 2. POJAM I SADRŽAJ DIGITALNE TRANSFORMACIJE

Organizacije se poslednjih godina sve više okreću primeni savremenih digitalnih tehnologija, sa ciljem da iskoriste svoje kompetitivne prednosti u odnosu na konkurenciju i ostvare bolji poslovni rezultat.

Uvođenje digitalnih tehnologija u organizacije utiče na njihove proizvode, poslovne procese, prodajne kanale i lance snabdevanja. Potencijalne prednosti digitalizacije su raznovrsne i uključuju povećanje efektivnosti i efikasnosti poslovanja, povećanje prodaje ili produktivnosti, implementaciju inovacija u kreiranju vrednosti, kao i nove oblike interakcije sa kupcima. U skladu sa tim neophodno

je da postojeći poslovni modeli organizacija budu preoblikovani ili zamenjeni potpuno novim modelima poslovanja [2].

Drugim rečima, primena digitalnih tehnologija može biti efektivna i efikasna jedino ukoliko je organizacija spremna da sprovede čitav niz kompleksnih transformacija u svom poslovanju. Transformacija može zahvatati poslovne procese, poslovne modele, organizaciju i njenu strukturu, način upravljanja odnosima sa kupcima, pristup inovacijama i preduzetništvu, način upravljanja podacima, kao i same koncepte upravljanja organizacijom.

Uvođenjem digitalnih tehnologija omogućena je realizacija međuorganizacionih koreografija procesa, koje podrazumevaju globalno povezivanje procesa između organizacija, što obezbeđuje osnovu za prevazilaženje svih vremenskih i geografskih granica. U ovakvim uslovima neminovno je redefinisavanje tradicionalne poslovne strategije tj. redefinisavanje uloge IT strategije u odnosu na poslovnu strategiju [3,4,5].

Tačnije, digitalizacija je uticala na to da IT strategije ne mogu više biti strategije funkcionalnog nivoa, koje su suštinski podređene i prilagođene poslovnim strategijama organizacija, već je neophodna fuzija IT strategije i poslovne strategije u sveobuhvatan novi fenomen, koji se naziva „digitalna poslovna strategija“ [6].

Digitalne strategije predstavljaju osnovu za adekvatnu transformaciju poslovanja savremenih organizacija, jer koriste moć digitalnog načina razmišljanja i time omogućuju organizacijama da efikasnije i efektivnije koriste [1]:

- raspoložive ljudske resurse,
- sredstva i tehnologije,
- dizajniraju bolje, besprekorno povezane i automatizovane procese.

U sprovedenim intervjuima sa više izvršnih menadžera vodećih organizacija u Srbiji, autori rada su došli do zaključka da one u Srbiji uglavnom ne poseduju digitalne strategije, već iste poistovećuju sa poslovnim strategijama ili tradicionalnim IT strategijama, a koje uključuju digitalne tehnologije. Ovakvo njihovo pojmovno izjednačavanje, ukazuje na nedovoljno razumevanje i poznavanje suštine, sadržine i značaja digitalne strategije. Iz tog razloga se u nastavku opisuje njihova suštinska distinkcija.

IT strategija definiše aktuelne i buduće operativne aktivnosti koje je potrebno realizovati, neophodna softverska rešenja i informaciona infrastruktura za njihovo uspešno obavljanje, kao i odgovarajući organizacioni i finansijski okvir za uvođenje potrebnih informacionih tehnologija [1,7].

Prema Burg i Singleton strategija IT je funkcionalna strategija koja protežira primenu informacionih tehnologija u cilju uštede troškova i unapređenja efikasnosti poslovanja organizacija [8].

IT strategije fokusiraju se isključivo na upravljanje informacionim tehnologijama u organizaciji. Mogućnosti uvođenja inovacija u razvoj poslovanja, zasnovanih na informacionim tehnologijama, prevazilazi okvire ovih strategija. Takođe, ove strategije pružaju systemske putokaze o budućoj upotrebi tehnologija u organizaciji, koji ne uključuju obaveznu transformaciju proizvoda, procesa i strukturne aspekte usled integracije ovih tehnologija [1,9].

Za razliku od IT strategija, digitalne strategije sagledavaju mogućnosti i efekte od primene digitalnih tehnologija u organizaciji [1,6]. One opisuju očekivane buduće poslovne prilike i mogućnosti organizacije od uvođenja digitalnih tehnologija. Njima se uspostavljaju dugoročni ciljevi u digitalizaciji poslovanja, ali se ne razmatra način na koji će organizacija ostvariti transformaciju poslovanja i stići do željenog budućeg poslovnog stanja. Digitalna strategija je odgovor organizacije na eksterne mogućnosti i pretnje, i na interne prednosti i slabosti, kako bi se održala njena konkurentna pozicija [1,9,10].

Nijedna poslovna promena usled primene tehnologije ne može biti ni efikasna ni efektivna bez odgovarajućih organizacionih promena, koje bi je pratile. Stoga pojam digitalne transformacije poslovanja obuhvata sve organizacione promene koje se realizuju upotrebom digitalnih tehnologija i poslovnih modela sa ciljem unapređenja performanse poslovanja organizacije [9].

Da bi digitalna transformacije poslovanja bila uspešna, neophodno je da organizacije detaljno razmotre i opišu sledećih šest dimenzija transformacije [1,11]:

- Digitalna strategija i koncept primene inovacija u organizaciji;
- Detaljna analiza i istraživanje načina donošenja odluka kupaca;
- Automatizacija poslovnih procesa;
- Organizacija agilnih, promenljivih i kolaborativnih procesa, u savremenim modelima poslovanja;
- Informacione tehnologije u podršci osnovnih funkcija organizacije i njenog brzog razvoja; i
- Upotrebi i relevantni podaci i analitika podataka o kupcima u skladu sa ciljevima i strategijama organizacije.

Detaljnim opisom navedenih dimenzija transformacije poslovanja, stvaraju se uslovi za kreiranje strategije digitalne transformacije poslovanja. Strategija digitalne transformacije poslovanja je upravo strategija koja se fokusira na transformaciju proizvoda, poslovnih procesa i organizacionih aspekata zahvaljujući raspoloživim novim tehnologijama [9]. Ona zapravo predstavlja plan transformacije, kojim se detaljno opisuju sve aktivnosti koje je potrebno realizovati da bi organizacija uspešno prešla na novi način poslovanja[1].

Na slici 1, razmatrajući upravo napred navedene primarne sadržaje funkcionalne IT strategije, poslovne strategije i digitalne strategije, prikazano je mesto strategije digitalne transformacije poslovanja u odnosu na ostale organizacione strategije.





Slika 1. Mesto strategije digitalne transformacije u organizaciji

Iz prethodne kratke prezentacije distinkcija između digitalne transformacije i najčešće upotrebljavane transformacije omogućene primenom IT, može se jasno zaključiti da je kompleksnost digitalne transformacije mnogo veća, i da je nivo digitalne transformacije revolucionaran.

Pored toga, koristi organizacije od digitalne transformacije umnogome prevazilaze koristi transformacije omogućene primenom IT. Digitalna transformacija po svojoj sadržini, razvrstana po nivou kompleksnosti od najmanje kompleksne do najkompleksnije transformacije može imati sledeće pojavne oblike: redizajn poslovnih procesa, redizajn poslovne mreže, redizajn obima poslovanja, transformacija odnosa sa kupcima i transformacija poslovnog modela [12].

### 3. DIGITALNE TEHNOLOGIJE U TRANSFORMACIJI POSLOVANJA

Razvoj informacionih tehnologija i Interneta, uticao je na to da se, devedesitih godina prošlog veka, revolucionarno izmeni način komunikacije organizacija sa njihovim dobavljačima, partnerima i kupcima. Prirodan sled predstavljao je razvoj e-trgovine i e-poslovanja koji su postavili temelje današnjoj digitalizaciji. Uloga informacionih tehnologija se tada svodila na podršku postojećim poslovnim procesima, dok se danas IT koriste za razvoj novih poslovnih modela, proizvoda i usluga.

Danas su prisutna 4 ključna megatrenda, u domenu digitalnih tehnologija, koja su otvorila nove mogućnosti organizacijama i uticale na transformaciju njihovog poslovanja:

- „mobile“ ili mobilne tehnologije,
- „cloud computing“ ili računarstvo u oblaku,
- „big data“ ili veliki podaci.
- „social media“ ili društveni mediji,

*Mobilne tehnologije* u poslovanju podrazumevaju upotrebu mobilnih uređaja (smart telefona i tableta) i aplikacija za mobilne uređaje, koje su usmerene na kupce, partnere, dobavljače i zaposlene. Uvođenje mobilnih

tehnologija u poslovanje omogućava nove poslovne scenarije, što najbolje opisuje sledeći primer iz prakse.

„Delta Air Lines“ je jedna od organizacija koja je mobilne tehnologije iskoristila u službi inovacija poslovanja. Ovaj avio prevoznik je 2013. godine započeo opremanje svojih 19.000 stjuardesa mobilnim uređajima, što je doprinelo porastu prihoda od prodaje u toku letova. Mobilni uređaji, uporedo sa sve većim brojem televizora sa ravnim ekranom ugrađenih u sedišta, omogućili su da putnici tokom leta rezervišu nove karte, hotelske sobe i koriste druge slične usluge. Sledeći strateški korak ove organizacije bio je da stjuardesama, putem mobilnih uređaja, omogući pristup ličnim podacima o korisnicima (iz sistema za upravljanje odnosima sa kupcima - CRM), kako bi im pružali usluge višeg nivoa personalizacije [13].

Prema istraživanjima koje je sprovedla Harvard Business School identifikovane su sledeće prednosti od korišćenja mobilnih uređaja i aplikacija u poslovanju [13]:

- pristup korporativnim aplikacijama i podacima moguć sa bilo kog mesta,
- povećana produktivnost zaposlenih, i
- povećana kolaboracija zaposlenih.

*Računarstvo u oblaku* podrazumeva mogućnost korišćenja skalabilnih, elastičnih IT i softverskih rešenja na principu usluge koja se plaća ili pretplatom ili na osnovu obima korišćenja date usluge. Vodeće organizacije u svetu koriste ovu tehnologiju, ne samo kao način za smanjenje IT infrastrukture i troškova zaposlenih, već i da bi kreirale nove poslovne modele i usluge.

Organizacije danas moraju biti agilne, fleksibilne i brze u zadovoljavanju očekivanja svojih klijenata. Organizacija „Wipro“ je samo jedna od mnogih koja nije mogla odgovoriti na ova očekivanja, sve dok tradicionalan centar za podatke nije zamenila računarstvom u oblaku. Tek upotrebom računarstva u oblaku, koje optimizuje upravljanje podacima i sam prenos podataka, uspeła je da odgovori na ovaj dugogodišnji poslovni izazov [13].

Empirijski rezultati istraživanja ukazali su na sledeće prednosti korišćenja računarstva u oblaku [13]:

- fleksibilni kapaciteti: sposobnost skaliranja poslovanja u odnosu na potrebe/zahteve,
- povećanje poslovne agilnosti: sposobnost da se odgovori brzo na nove mogućnosti,
- niži fiksni troškovi.

*Tehnologija velikih podataka* odnosi se na raznovrsne podatke, velike zapremine, koji se u savremenom poslovanju generišu velikom brzinom. Ovi podaci su kako strukturirani tako i nestrukturirani, te tradicionalni načini njihovog procesuiranja nisu bili efikasni. Zahtevali su ekonomičnije i inovativnije oblike obrade, kako bi se koristili za pravovremeno i efektivno donošenja odluka u poslovanju. Pojava „in-memory computing“ tehnologije

omogućila je da se prevaziđu tradicionalne prepreke u analizi velikih podataka.

Organizacija „Progressive Insurance“ je bila među prvima koja je, upravo primenom ove tehnologije, uvela inovativni program u domenu auto osiguranja. Zahvaljujući dobroj primeni tehnologije velikih podataka, organizacija je tradicionalne varijable određivanja cena osiguranja automobila (godina proizvodnje i tip automobila) zamenila novom: auto osiguranje zasnovano na korišćenju.

Naime, organizacija je u automobilima svojih korisnika postavljala bežične uređaje koji su beležili sve informacije o vožnji i iste, u intervalima od jedne sekunde, prenosila u svoj centralni program. Korisnici koji su se pridržavali pravila bezbedne vožnje imali su mogućnost, da smanje svoje premije osiguranja, u proseku za 10%. Upotrebom tehnologije velikih podataka, organizacija je bila u mogućnosti da prikupi i analizira podatke u realnom vremenu, što je iskoristila kao svoju kompetitivnu prednost i ponudila klijentima bolju uslugu i novu kategoriju proizvoda: auto osiguranje zasnovano na korišćenju [13].

Prednosti korišćenja tehnologije velikih podataka u poslovanju [13]:

- brže generisanje uvida u podatke u realnom vremenu,
- integrisanje veće količine podataka u proces donošenja odluka,
- integrisanje različitih izvora podataka u analize.

*Društveni mediji* podrazumevaju tehnologije koje olakšavaju socijalne interakcije putem Interneta i mobilnih uređaja. Primeri društvenih medija su: socijalni vikiji, blogovi, društvene mreže i veb konferencije.

Sektor konsaltinga i poslovnih usluga bio je prvi po pitanju primene društvenih medija, koji su uticali na transformaciju ovog domena poslovanja. Rani poslovni uspesi sa društvenim umrežavanjem najočigledniji su u sferi marketinških aktivnosti. Danas su socijalni mediji postali ključni aspekt savremenog digitalnog marketinga, koji umnogome transformiše marketinšku funkciju.

Napredne organizacije, međutim, ne koriste društvene mreže samo da bi oslušivale i bolje razumele mišljenje potrošača o proizvodima, brendovima i organizaciji u celini. One društvene medije koriste i u domenu regrutovanja i upravljanja ljudskim resursima, kao i za saradnju i komunikacija sa zaposlenima, partnerima i dobavljačima.

„Ask.com“ je vodeći svetski brend za pitanja i odgovore, koji je pre par godina, imao cilj da unapredi potrošačko iskustvo i interno funkcionisanje tima za podršku. Uvođenjem CRM aplikacije koja poseduje funkcionalnosti za praćenje društvenih mreža, ova organizacija je transformisala oba. Ovom promenom bilo je omogućeno da tim za podršku korisnicima počne da upravlja i tiketima koji su generisani preko društvenih

medija, pomoću pametnih telefona, bez potrebe da klijenti budu za laptopom ili u kancelariji [13].

Prednosti korišćenja društvenih medija [13]:

- povećana sposobnost da se efikasno komunicira sa klijentima,
- povećana kolaboracija zaposlenih, i
- poboljšana sposobnost pružanja usluga klijentima.

Primena digitalnih tehnologija, uz prateće organizacione promene, utiče na poboljšanje performansi poslovanja. Veća performantnost može se ostvariti u sledećim oblastima: veći prihodi, bolja efikasnost i smanjeni troškovi, brže i uspešnije inovacije, efikasnije sakupljanje, deljenje i korišćenje znanja, bolje interakcije sa kupcima i pružanje kvalitetnijih usluga klijentima. Sve ove performanse poslovanja se mogu kvantifikovati, s obzirom da se njihovi indikatori mogu meriti i kontinuirano pratiti putem izveštaja. Upravo je merljiva priroda digitalnih tehnologija ključna za uspešan proces digitalne transformacije poslovanja [14].

#### 4. ZAKLJUČNA RAZMATRANJA

U radu su razmatrani pojam i sadržaj digitalne transformacije poslovanja, kako sa tehnološkog tako i sa strateškog aspekta, jer je njihova usklađenost neminovna za ovaj proces. Može se zaključiti da svaki tehnološki megatrend, nezavisno jedan od drugog, ima veliki uticaj na transformaciju poslovanja savremenih organizacija. Međutim, primenom integrisanih rešenja ostvaruje se daleko veći uticaj.

Bitno je naglasiti da nijedna od promena, koje omogućavaju savremene digitalne tehnologije ne donosi boljim poslovnim rezultatima bez pratećih organizacionih promena. Stoga autori zaključuju da su duboke organizacione promene, u kombinaciji sa primenom opisanih digitalnih tehnologija, put uspešne digitalne transformacije poslovanja i poslovnog uspeha savremenih organizacija.

Značaj strateškog pristupa digitalnoj transformaciji, potvrđuje činjenica da, uprkos inicijalnim naporima u istraživanju, akademiji i dalje nedostaju specifične smernice o tome kako organizacije da formulišu, implementiraju i evaluiraju strategije digitalne transformacije.

Uvidom u naučnu i stručnu literaturu zaključuje se, da je predmet istraživanja rada još uvek u povelju i da je neophodna veća angažovanost akademije, s obzirom da postoji širok istraživački prostor u kojem se tek očekuju naučni doprinosi. Autori su u radu dali smernice koje organizacijama mogu olakšati bolje razumevanje i implementaciju procesa digitalne transformacije.

#### LITERATURA

[1] Marić, M., Matković, P., Tumbas, P., & Pavličević, V. „Digitalna strategija u transformaciji poslovanja“. Zbornik radova Menadžment i marketing: trendovi i

- uticaji na efikasnost tržišta u Republici Srbiji, Subotica, 2017.
- [2] Downes, L., & Nunes, P. "Big-Bang Disruption", *Harvard Business Review*, 91(3), 44–56, 2013.
- [3] Rai, A., Pavlou, P. A., Im, G., & Du, S. "Interfirm IT Capability Profiles and Communications for Cocreating Relational Value: Evidence from the Logistics Industry", *MIS Quarterly*, 36(1), 233–262, 2012.
- [4] Grover, V., & Kohli, R. "Revealing your hand: Caveats in implementing digital business strategy", *MIS Quarterly*, 37(2), 655–662, 2013.
- [5] Banker, R. D., Bardhan, I. R., Chang, H., & Lin, S. "Plant Information Systems, Manufacturing Capabilities, and Plant Performance", *MIS Quarterly*, 30(2), 315–337, 2006.
- [6] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, V. "Visions and Voices on Emerging Challenges in Digital Business Strategy", *MIS Quarterly*, 37(2), 633–661, 2013.
- [7] Teubner, R. A. "Information Systems Strategy", *Business and Information Systems Engineering*, 5(4), 243–257, 2013.
- [8] Burg, W. D., & Singleton, T. W. "Assessing the value of IT: Understanding and measuring the link between IT and strategy", *Information Systems Control Journal*, 3, 2005.
- [9] Matt, C., Hess, T., & Benlian, A. "Digital Transformation Strategies", *Business and Information Systems Engineering*, 57(5), 339–343, 2015.
- [10] Ross, J. W., Beath, S., Sebastian, I., Mocker, M., Moloney, K. G., & Fonstad, N. O. "Designing and Executing Digital Strategies", In *Proceedings of the International Conference on Information Systems (ICIS)*. Dublin, 2016.
- [11] Desmet, D., Duncan, E., Scanlan, J., & Singer, M. "Six building blocks for creating a highperforming digital enterprise", *McKinsey Quarterly* 3(8), 1–9, 2017.
- [12] Ismail, M.H., Khater, M., Zaki, M. "Digital Business Transformation and Strategy: What Do We Know So Far?", *Cambridge Service Alliance, Working Paper*, 2017.
- [13] A Harvard Business Review Analytic Services Report. "Digital Transformation of Business", *Harvard Business School Publishing*, 2015.
- [14] Wade, M. "Digital Business Transformation - A Conceptual Framework", *Global Center for Digital Business Transformation*, 2015.

# Achieving interoperability in European Electronic Toll Collection Systems (EETCS) based on Automatic License Plate Recognition (ALPR)

Miloš Ivanović

University of Belgrade, Faculty of Organizational Sciences, Serbia

**Abstract** — This paper is based on study of some problems of the EETC interoperability and presents ALPR solution for achieving interoperability. Today, when technology develops rapidly, many manufactures of road charging systems are using state-of-art technologies. In EETC are many systems which are developed from different manufacturer, and the main interoperability problem is how European user which is using On Board Units (OBU) in his vehicle or using vehicle license plate number can travel across borders at different geographic locations, and can communicate with all roadside equipment from different manufactures. Electronic Fee Collection is one of priority area for interoperability. Interoperability of road charging solutions is a objective of the Electronic Collection and the directive 2004/52/EC.

According to directive EETCS should use one or more of the following technologies: satellite positioning (GPS/GSM), mobile communications using the GSM-GPRS standard and 5, 8 GHz microwave. The aim of this paper is to research how ALPR technology can solve the problem of EETC interoperability in the way to replace the existing technologies from directive EETCS.

## I. INTRODUCTION

The ability of different Intelligent Transport Systems (ITS) devices and components to exchange directly through a common communication interface, and to use the exchanged data to operate together effectively is called **interoperability**. Interoperability is a key to achieving the full potential of ITS. Electronic Toll Collection systems are the part of ITS.

The aim of Directive 2004/52/EC is to coordinate that Member States develop strategy for the convergence of Electronic Fee Collection systems in order to achieve interoperability at European level on appropriate level. [1] ITS standards are open interface standards that establish communication rules for how ITS devices can perform, how they can connect, and how they can exchange data in order to interoperate. Standardization is the key of the achieving interoperability of any system. The aim of Directive is to achieve interoperability between ETC systems, and this Directive push the manufactures of ETC equipment to implement standards and integrate with other manufactures. There are two types of European Electronic Tolling Service: [4]

1. Dedicated Short Range Communication (DSRC 5.8 GHz).
2. GPS/GSM based systems.

All electronic toll systems using microwave technology all over the world have the same structure, which utilize vehicles equipped with On Board Units (tags) (Figure 1.), toll and control gantries, inroad/ roadside detection and

classification sensors, computerized system (hardware and software) and wireless communication (5,8 GHz nearly all over the world, only 5,9 GHz in USA), as well as enforcement technologies.



Figure 1. On-Board-Unit (OBU)

GPS/GSM system is based on an innovative combination of mobile telecommunications technology (GSM) and the satellite-based Global Positioning System (GPS). The main element of the automatic log-on system is the On-Board Unit (OBU). With the aid of GPS satellite signals and other positioning sensors, the OBU automatically determines how many kilometers have already been driven on the toll route, calculates the toll based on the vehicle and toll rate information that has been entered, and transmits this information to the computer center for further processing.

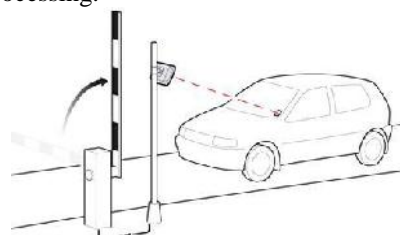


Figure 2. Identification OBU via DSRC

Benefits of achieving interoperability in electronic toll collection systems:

- The waiting time of vehicles on toll roads is reduced.
- System maintenance costs will reduce approx. 40 percent.
- The use of cash money for collection and printing fiscal clauses is abolished, thereby reducing costs and corruption.
- Centralization of all toll stations of one state in a single command center for monitoring and management of ETC system.
- Search, alarms and vehicle reports that have passed through the toll station are simplified with high coefficient accuracy and relevance.
- Simplicity in supplementing cash on the OBU owned by the driver (via Web, SMS, payment to account etc.).

- TIME is MONEY, waiting time is reduced by 60% and thus the profit of all participants in this traffic increases.



Figure 3. Electronic Toll Collection – Vrčin in Belgrade ( “future task: all lanes are automatic electronic payment via ALPR technology”) [modified picture]

## II. INTELLIGENT TRANSPORT SYSTEMS INTEROPERABILITY

Intelligent Transport Systems or ITS means systems in which information and communication technologies are applied in the field of the road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport.

Interoperability in intelligent transport systems is a complex problem. Intelligent management of transport systems is still under development and will only be fully implemented in a few years, for the simple reason that existing systems should be integrated and adapted to new technologies applied in the transport infrastructure.

Interoperability is defined as a common set of processes, procedures and equipment adopted by more than one provider, to support and improve ease of use for users and data acquisition. In interoperate system, users can easily switch between heterogeneous system, components and that takes the same data to integrate quality information suitable for achieving good results system. At the highest level of interoperability between heterogeneous system boundaries are invisible to the user, in order that these background processes and procedures work together and provide the user performing the transaction systems, data exchange, data warehousing and distributing data to other parts of the system.

“ITS interoperability is the ability of ITS-based systems to provide services (data, information, and control commands) to other systems and to accept services from those other systems so that the inter-connected systems operate effectively together. Systems are interoperable when the ITS services are seamlessly provided in real-time including between different organizations and/or at different locations”. [2]

ITS architecture development is good opportunity for system harmonization and consensus building among ITS

users, service operators, road network operators, public agencies and other stakeholders.

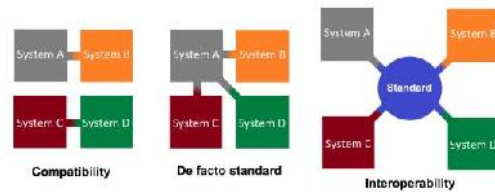


Figure 4. Achieving interoperability between various systems (Standardization is the key of interoperability)

There are four aspects of ITS interoperability [3,7]:

1. Technical interoperability
  2. Functional/logical interoperability
  3. Contractual/institutional interoperability
  4. Procedural interoperability
- **technical interoperability**, which is the capability of the technical subsystems to communicate with each other by using standardized interfaces and communication protocols. Typical issues are the physical layers and data layers for radio transmission (for example 5.8 GHz Dedicated Short Range Communication (DSRC) for Electronic Fee Collection).
  - **procedural interoperability** is achieved when common procedures are used by all involved road network operators and by the users. Typical issues are harmonised data dictionaries (for example NTCIP in USA or DATEX in Europe or common human machine interfaces (HMI)).
  - **contractual interoperability** requires agreements between network operators about service levels, financial transactions, data security, enforcement, and the assignment of roles and responsibilities.

## III. RCI PILOT PROJECT

The objective of the RCI project was to develop an open, integrated framework enabling road charging interoperability at the technical (and related procedural) level based on the key existing and planned road charging deployments in Europe (AUTOPASSEUROPPASS, LSVA, TELEPASS, TIS, TOLLCOLLECT, VIA-T and VIA VERDE). [7]

It implemented and tested this framework at next sites:

- Austria (EUROPPASS),
- France (TIS),
- Germany (TOLLCOLLECT),
- Italy (TELEPASS),



- Switzerland (LSVA) and Spain (VIA-T).

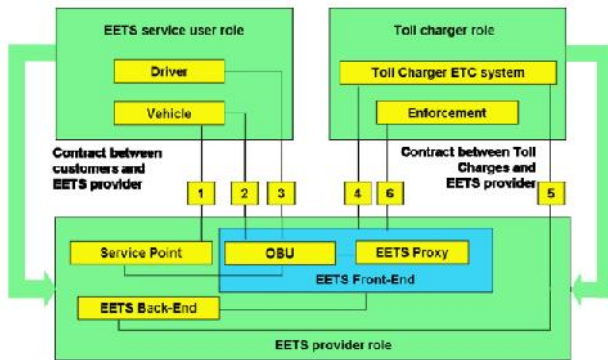


Figure 5. RCI architecture [4]

In the RCI architecture two charging principles for a tolled infrastructure are supported: [4]

1. **DSRC-based tolled infrastructure:** Charging data is generated in a real-time DSRC communication between the OBU and roadside microwave beacons.
2. **GNSS enabled tolled infrastructure:** Data enabling GNSS tolling is generated in the OBU autonomously and the GNSS charge data is forwarded via the central system of the EETS. The Toll Charger receives the GNSS charge data through a back-office interface and can use DSRC for enforcement and localization support. It is mentioned that within this concept, two or more tolled infrastructures could overlap. It is also noted that the DSRC-based tolled infrastructure could be deployed anywhere, including inside the domain of GNSS-enabled tolled infrastructure.

The RCI project **first** consolidated the EETS specifications with those of existing solutions and specified the framework for interoperability across six major European tolling sites: [7]

- ✓ systems based on 5.8 GHz CEN norm,
- ✓ according to the CESARE/CARDME specifications,
- ✓ non-compliant but upgradeable to CESARE/CARDME specifications,
- ✓ non-compliant and non-upgradeable to the CESARE/CARDME specifications,
- ✓ Italian system 5.8 GHz DSRC Telepass,
- ✓ German system, based on three technologies (GPS/GNSS, GSM/GPRS, infrared communication used for vehicle positioning, mobile and stationary enforcement and communication between the OBE and RSE and including but not using 5.8 GHz CEN DSRC as fourth technology.

**Secondly** the project implemented and tested two different types of prototypes, both interoperable across all test sites and based on specifications that:

- ✓ define interfaces that can 'open existing systems' by allowing different suppliers to manufacture equipment that can be certified against these specifications and that can operate in different contexts (CEN DSRC/CARDME, Autostrada DSRC, 'Multi technologies' as in Germany and in Switzerland);
- ✓ contribute to the convergence of future tolling systems and the evolution of existing tolling systems as such allowing for a greater reusability of standard components across different systems;
- ✓ be open, public and available on a non-discriminatory basis to any stakeholder including all system suppliers.

#### IV. PROBLEMS OF ITS AND EETCS INTEROPERABILITY

The ETC systems in the European Union member states **are not interoperable** due to differences in charging concepts, technology standards, classification and tariff structure, legal and institutional backgrounds. European Commission has taken bold steps to address that issue.

##### Directive 2004/52/EC

The Directive 2004/52/EC has stressed next main priority areas for the development and use of specifications, technologies and standards: [1]

a) *The majority of Member States which have installed electronic toll systems to finance road infrastructure costs or to collect road usage fees use short-range microwave technology and frequencies close to 5,8 GHz, but these systems are currently not totally compatible. The work on microwave technology undertaken by the European Committee for Standardisation (CEN) resulted in January 2003 in the preparation of technical standards making for the compatibility of 5,8 GHz microwave electronic toll systems, following the adoption of technical pre-standards in 1997. However, these pre-standards do not cover all the Dedicated Short-Range Communications (DSRC) 5,8 GHz systems in operation in the Community and encompass two variants which are not totally compatible. They are based on the Open Systems Interconnection model defined by the International Standardisation Organisation for communication between computer systems.*

b) *Manufacturers of equipment and infrastructure managers have nonetheless agreed, within the Community, to develop interoperable products based on existing DSRC 5,8 GHz systems.*

c) *The electronic toll systems should be interoperable and based on open and public standards, available on a non-discriminatory basis to all system suppliers.*

d) *Artificial barriers to the operation of the internal market should be removed, while still allowing the Member States and the Community to implement a variety of road-charging policies for all types of vehicles at local, national or international level. The equipment installed in vehicles should allow such road-charging policies to be implemented in accordance with the principles of non-discrimination between the citizens of all Member States. **The interoperability of electronic toll systems at Community level therefore needs to be ensured as soon as possible.***

One of interoperability problem was decision to launch Europe's own Galileo system that is predicted to improve upon both the accuracy and reliability of GPS.

On June 26, 2004, the US and EU signed an agreement to coordinate Galileo and GPS.

#### **Mandate 453**

The objective of Mandate 453 is to invite the European Standardization Organizations, ETSI, CEN, CENELEC to prepare a coherent set of standards, specifications and guidelines to support European Community wide implementation and deployment of Co-operative ITS systems. [10]

This Mandate supports the development of technical standards and specifications for Intelligent Transport Systems (ITS) within the European Standards Organizations in order to ensure the deployment and interoperability of Co-operative systems, in particular those operating in the 5 GHz frequency band, within the European Community. Standardization is a priority area for the European Commission in the ITS Action Plan in order to achieve European and global ITS co-operation and coordination. Standardization for Cooperative ITS systems has already been initiated both by ETSI and ISO as well as within other international standards organizations. European standardization activities to provide the standardized solutions for Cooperative ITS services are therefore closely related to the world wide standardization activities. [6]

Other intelligent transport systems interoperability problems are:

a) *Functional design system per the designed requirements*

The problem of Intelligent Transport Systems (ITS) and services interoperability in the EU environment. The problem is associated with multi-level models and functional system design per the defined requirements. The first result of the research is a formalized comprehensive procedure for ITS functional system formulation. The national ITS architecture development is suggested as a necessary systematic framework for the

deployment of dozens of new ITS applications in CSEE countries. [3]

ITS functional analysis has to resolve iteratively the "top-level" system design into simpler system design problems. ITS functional analysis is a three-step iterative process: [3]

**Step 1.** Decompose the top-level requirements into set of functional requirements, where each functional requirement is in the same format and consistent with the top-level (interoperability) requirement.

**Step 2.** Decompose requirements in all other categories of the top-level system design and allocate them to the functional (interoperability) requirements defined in Step 1.

**Step 3.** Validate that the system design problem resolution is consistent with the top-level system design problem according to the defined criteria and additional consistency condition.

b) *Specific projects, tools for monitoring the problem related to the ITS interoperability*

The European Commission takes care of the ITS and telecommunication systems interoperability problems: [9]

-There are no specific projects related to the ITS interoperability in the country.

-There are no the tools for this problem monitoring, evaluation and management.

In the most general approach the ITS systems interoperability is achieved through: [9]

I. **Unification** – the application of compatible norms, standards and procedures, starting from the stage of system designing.

II. **Interchangeability** – e.g. of a product (subsystem, service, process) in a way imperceptible to ITS systems recipients/users.

III. **Compatibility** – product suitability for use, once the requirements are met and there are no undesirable impacts.

c) *Non-interoperability between ITS systems at EU level*

Non-interoperability between ITS systems at EU level in six priority areas: [8]

1. Optimal use of road, traffic and travel data
2. Continuity of traffic and freight management ITS services in European transport corridors and conurbations
3. Road safety and security
4. Integration of the vehicle into the transport infrastructure
5. Data security and protection and liability issues
6. European ITS cooperation and coordination

*Intelligent Transport Systems and Services (ITS) refers to the integration of information and communication technologies with transport infrastructure to improve economic performance, safety, mobility and environmental sustainability for the benefit of all European citizens.*

Action plan includes: [8]

1. Evolving approach to safety
2. New approaches to traffic management and intelligent infrastructures
3. Towards holistic solutions
4. Making the most of multimodality
5. International cooperation

## V. CASE STUDY: IMPROVING EETCS BASED ON AUTOMATIC LICENCE PLATE RECOGNITION TECHNOLOGY

The main problem of ETC interoperability is how users (drivers) can travel across the continent (or World) with using one OBU or one type of *equipment which can achieve interoperability*. In this chapter, will be presented solution that is based on using only Automatic License Plate Recognition (ALPR) of technology working together with police department license plate database in aim to achieve the interoperability of whole ETC system (Figure 8). The aim of this paper is to present this solution which excludes existing OBU, and include ALPR technology for ETC. Also, use GPRS service for establishing connection between systems. It is important, because there are many tolling stations which are out of the city and don't have possibility for optical network. The key of interoperability of any heteronyms system is standardization. The existing problem of non-interoperable ETC systems, is that manufactures of ETC systems are not using open standards in communication protocol of their system. So, every manufacturer has own protocol in their systems.

In this solution, will be presented DATEX II standard which will be used for communication protocols between systems in ETC. DATEX II standard provides a standardized way of communicating and exchanging traffic information between traffic centers, service providers, traffic operators and media partners.

**DATEX II** – The standard for ITS in European Roads – CEN TS 16157

“DATEX II standard has been developed to provide a standardized way of communicating and exchanging traffic information between traffic centers, service providers, traffic operators and media partners. The specification provides for a harmonized way of exchanging data across boundaries, at a system level, to enable better management of the European road network.” [11]

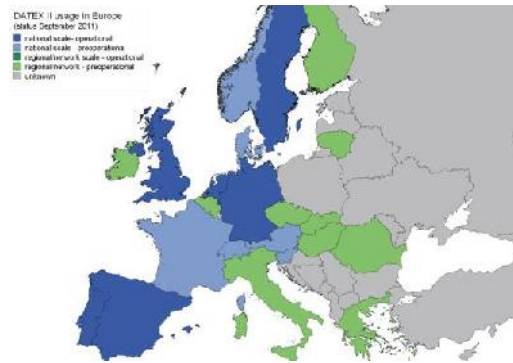


Figure 6. DATEX II finds increasing application all over Europe on different scales and stages of development. [18]

DATEX II data model is currently mapped to XML schema as the exchange message syntax but may in future, or for different operational environments be mapped to other platforms (e.g. ASN.1) in the same way, without losing the interoperability of the applications behind the exchange. [18]

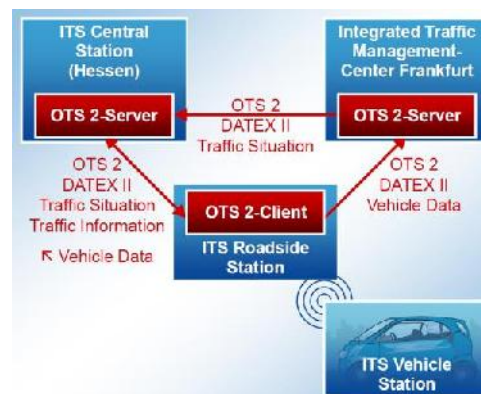


Figure 7. Example of OTS2 system architecture with DATEX II standard [13]

On figure 7 is shown OTS2 system architecture, OTS2 + DATEX II. OTS2 is used as protocol to establish communication between central systems and between central station and roadside stations (e.g. traffic controller, car, VMS etc.). DATEX II used as data model for exchanged traffic information.

Automatic license plate recognition is a technology that uses optical character recognition on images to read vehicle registration plates. It can use existing closed-circuit television, road-rule enforcement cameras, or cameras specifically designed for the task.



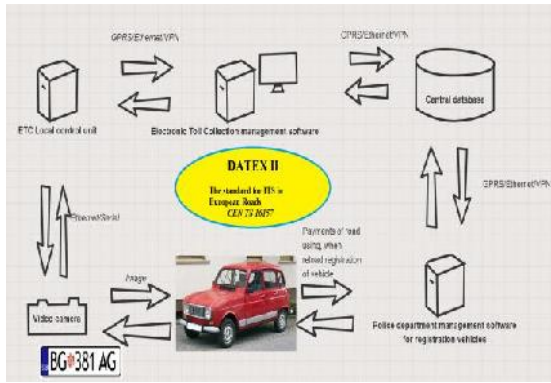


Figure 8. Architecture of interoperable ETC system based on ALPR technology

In next paragraph, will be described the functionality of interoperable ETC system based on ALPR on figure 5.

**First step:** vehicle is coming on tolling station and video camera for capturing images of license plates is established on gate of station. For better percent of reading license plates, its recommended to use two video cameras. One to catch front license plate and second to catch license plate from back of vehicle.

**Second step:** Video camera catch the image in different formats (.BMP, .JPEG etc.) and frames, then it sends image to Local Control Unit (LCU). LCU is in ETC local system, and the objective of this unit is to process the image and read the license plate from image. For processing image and reading license plate in this solution will use Q-Free Intrada ALPR engine (Figure 9). Intrada ALPR is the Q-Free software solution for Automatic License/Number Plate Recognition (ALPR/ANPR). Intrada ALPR offers an SDK for reading registration numbers from images. We offer an API for easy integration with C++, C, C# and other .NET applications. [12]



Figure 9. Q-Free Intrada ALPR engine (SDK) [12]

**Third step:** Local Control Unit (LCU) after successfully reading license plate, send it to ETC management software in command center. ETC management software collect this image in central database with next format of record (table 1.):

License Plate	ETC_Entrance	Lane	DateTime	ETC_EXIT	Lane	DateTime
BG381AG	ETC Belgrade	1	9/21/2017 7:43	ETC NIS	2	9/21/2017 10:43

Table 1. License plate record in central database

**Fourth step:** When the ETC management software store the vehicle license plate, and keep the history of his road using, then police department management software load the history of every vehicle by license plate number.

**Final step:** The charging of the services for the use of the highway can be calculated periodically and sent to the user at the address or during the one-year registration of the vehicle.

## VI. CONCLUSION

Benefits of using this interoperable ETC system are:

- ✓ Users don't need On-Board-Units (no extra costs).
- ✓ No risk of battery in OBU fails or broken OBU.
- ✓ No need for extra services for using OBU.
- ✓ Users don't need to care about extra equipment for road charging like Vignette, OBU etc...
- ✓ Using license plate of vehicles like main parameter for road charging.
- ✓ This solution is using open standard for ITS in European Roads CEN TS 16157 which plays key role in achieving interoperability

## REFERENCES

- [1] Directive 2004/52/EC, Official Journal of the European Union, April 2004.
- [2] World Road Association mondiale de la route, <https://rno-its.piarc.org/en/rno-basics-integrated-operations-systems-integration/interoperability>, August 2017.
- [3] Multi-layered model of intelligent transport systems and services interoperability, Bosnjak, I., Domandzic, D., Simunovic, Lj., U.D.C 656.681.518, 2003.
- [4] Some problems of the European Electronic Toll Service interoperability, Nowacki G., Niedzicka A., ISBN: 978-9984-818-21-4, 2004.
- [5] Bold steps of interoperability status of European Electronic Tolling Service, Nowacki G., Mitraszewska I., Kaminski T., 2009.
- [6] Interoperability problems of especially electronic toll collection, Nowacki G., 2011.
- [7] Road Charge Interoperability pilot project, <http://www.transport-research.info/project/road-charging-interoperability-pilot-project>, August 2017.
- [8] Intelligent Transport Systems, European Commission, Directorate general for Research, ISBN: 9789279164019, 2010
- [9] Interoperability of intelligent transport systems, Kowalewski, B., Kowalczyk, B., Chojnacki, B., Parapura, H., National Institute of telecommunications, Szachowa 1, Warsaw Poland.
- [10] Mandate 453, Standardization mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the European community, European Commission, October 2009.
- [11] DATEX II standard for ITS in Europe, [http://www.datex2.eu/sites/www.datex2.eu/files/Datex\\_Brochure\\_2011.pdf](http://www.datex2.eu/sites/www.datex2.eu/files/Datex_Brochure_2011.pdf), August 2017.
- [12] Q-Free Intrada ALPR engine, <https://www.q-free.com/product/intrada-alpr/>, August 2017.
- [13] OTS 2 Standardisation, Schön T., Datex II Forum Berlin, March 2010.
- [14] Achieving interoperability of parking system based on RFID technology, Ivanovic M., ISBN: 978-86-85525-18-6, conference ICIST 2016.

# AUTONOMNI SAMOVOZEĆI AUTOMOBILI

## AUTONOMOUS SELF-DRIVING CARS

Gyula Mester

*Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary*

**Sadržaj** – *Autonomni samovozeći automobili učestvuju u saobraćaju na putevima bez vozača, detektuju okolinu, donose potrebne odluke za bezbedno upravljanje automobilom. Razvoj autonomnih samovozećih automobila bazira se na rezultatima istraživanja inteligentnih robota. Prikazujemo 5 nivoa automatizacije vožnje.*

**Abstract** - *Autonomous self-driving cars are capable of driving on the road without human intervention, sensing and evaluating the environment, navigating without hesitation, using digital technologies, navigating itself. The development of autonomous self-driving cars is based on the results of intelligent robot research. We review the 5 levels for automated driving systems.*

### 1. UVOD

Razvoj električnih autonomnih samovozećih vozila prouzrokuje brzu transformacije automobilske industrije i društva. Autonomne samovozeće automobile razvijamo u cilju poboljšanja bezbednosti saobraćaja. U datim uslovima saobraćaja, autonomni samovozeći automobil (self-driving car, robotic car) kreće se bez intervencije vozača, sensorima detektuje okolinu, aplikacijom digitalnih tehnologija donosi potrebne odluke za bezbedno upravljanje automobilom. Vreme reagovanja prosečnog vozača na opasnu situaciju iznosi 0.8 s, što nemože da se uporedi sa parametrima savremenih digitalnih senzora autonomnih samovozećih vozila. Dok vozač ima relativno usko vidno polje, automatika samovozećeg vozila detektuje okolinu za 360°.

Prednost samovozećih autonomnih vozila ogleda se u eliminaciji greške vozača u procesu donošenja odluka u toku vožnje, što rezultira manji broj saobraćajnih nezgoda. Autonomna vožnja obuhvata putnički saobraćaj (automobili, taksi vozila, autobusi) kao i teretni saobraćaj (kamioni).

Pogon autonomnih samovozećih vozila je električni, što će izazvati pad tržišne vrednosti vozila sa benzinskim i dizel motorima.

Razvoj autonomnih samovozećih automobila robotičari su najavili od sredine 90-ih godina i bazira se na rezultatima istraživanja inteligentnih robota [1-3].

Sve veći broj autonomnih samovozećih vozila, smanjiće broj privatnih vozila (posedovanje vozila stavlja u drugi plan) i deljenje automobila (car sharing) sve više dolazi do izražaja.

Danas na razvoju autonomnih samovozećih vozila u svetu radi veći broj kompanija kao što su: Google, Tesla Motors, Nissan, Toyota, Volkswagen/Audi, Mercedes-Benz, Delphi Automotive i Bosch.

### 2. NIVOI AUTOMATIZACIJE VOŽNJE

Američka asocijacija SAE (Society of Automotive Engineers) International, 2014 god. definisala je nivoje automatizacije vožnje [4]. Prema ovoj definiciji prikazujemo 6 nivoa automatizacije vožnje:

Nivo 0, Level 0, No Automation: vozilom upravlja vozač, nema automatizacije, uslove saobraćaja nadzire vozač.

Nivo 1, Level 1, hands on, Drive Assistance: vozilom upravlja vozač, podrška za upravljanje ili kočenje/urbzanje, uslove saobraćaja nadzire vozač.

Nivo 2, Level 2, hands off, Partial Automation: vozilom upravlja vozač, delimična automatizacija, podrška za upravljanje i kočenje/urbzanje, uslove saobraćaja nadzire vozač.

Nivo 3, Level 3, eyes off, Conditional Automation: uslovna automatizacija, vozilom upravlja vozač, delimična automatizacija, istovremena podrška za upravljanje i kočenje/urbzanje, uslove saobraćaja nadzire automatika.

Nivo 4, Level 4, mind off, High Automation: visoki stepen automatizacije, automatika upravlja dinamikom vozila, uslove saobraćaja nadzire automatika.

Nivo 5, Level 5, steering wheel optional, Full Automation: potpuna automatizacija, automatika upravlja dinamikom vozila, uslove saobraćaja nadzire automatika, vozilo u saobraćaju može da se kreće bez vozača.

### 3. ELEKTRIČNI AUTOMOBILI

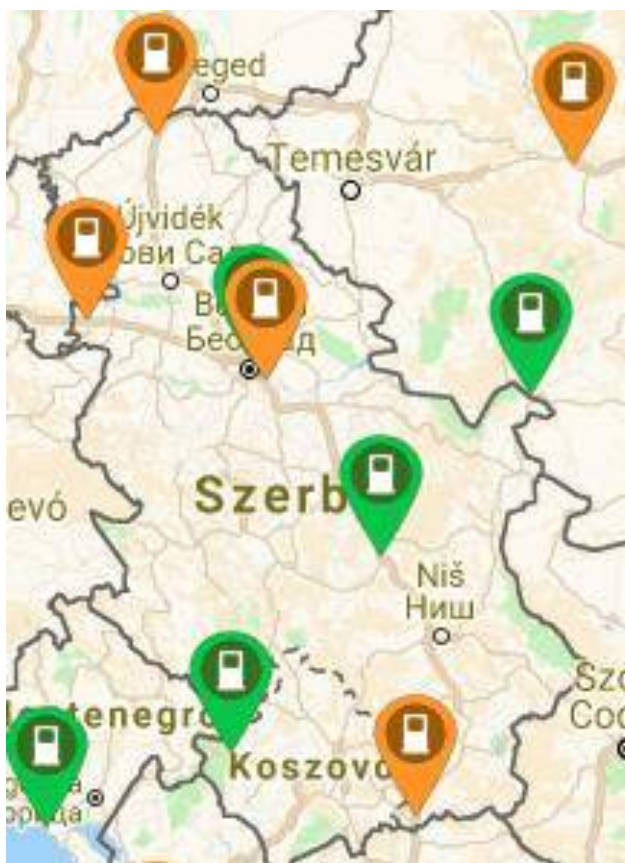
Električni automobil Nissan Leaf, pojavio se na tržištu krajem 2010 god. i dosada je prodato u više od 300.000 primeraka. Slika 1 prikazuje Nissan Leaf, model 2018, radijus kretanja (driving range) 378 km.



Slika 1. Nissan Leaf električni automobil



Širenje tržišta električnih automobila u svetu zavisi od više faktora kao što su: kapacitet i brzina punjenja akumulatora, radijus kretanja, infrastruktura punjača, državne subvencije. U Norveškoj električni automobili su oslobođeni od plaćanja PDV-a, a od 2025 god. biće zabranjena prodaja automobila sa benzinskim i dizel motorom. Danas u Evropi ima 100.000 punjača za električne automobile (od kojih 1300 su brzi punjači), za sada punjenje je besplatno. Slika 2 prikazuje punjače električnih automobila u našem regionu.



Slika 2. Punjači električnih automobila u regionu [5]

2013 god. u Japanu jedna taksi kompanija zamenila je taksi vozila sa električnim Nissan Leafovima. Danas u svetu u 26 država i 113 gradova imamo taksi kompanije sa električnim Nissan Leafovima. U Budimpešti Green Taxi kompanija takodje ima električne automobile Nissan Leaf, slika 3.



Slika 3. Nissan Leaf električni GreenTaxi, Budimpešta [6]

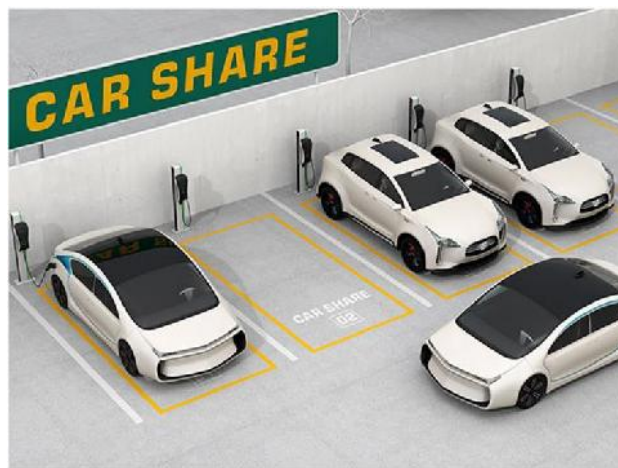
Efektivni radijus kretanja (driving range) električnih automobila zavisi od više uticajnih faktora kao što su:

- brzina kretanja vozila,
- korišćenje klima uredjaja,
- spoljašnja temperatura (u zimskim uslovima radijus kretanja električnih automobila bitno se smanjuje).

Navodimo i ostale električne automobile: Tesla Model S, Tesla Model 3, BMW i3, Volkswagen e-Golf, Volkswagen e-Up, Renault Zoe, Ford Focus Electric, Kia Soul EV, Chevrolet Bolt EV, Honda Clarity Electric, Mercedes-Benz Electric.

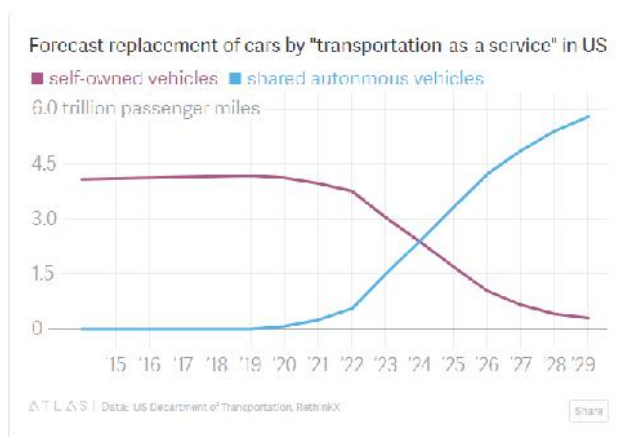
#### 4. DELJENJE AUTOMOBILA – CAR SHARING

Širenjem tržišta električnih i samovozećih automobila saobraćaj sve više postaje uslužna delatnost (Transport-as-a-Service (TaaS)). Vlasnici automobila postaju iznajmljivači (slika 4) i predviđa se drastično smanjenje broja privatnih automobila (The End of Individual Car Ownership).



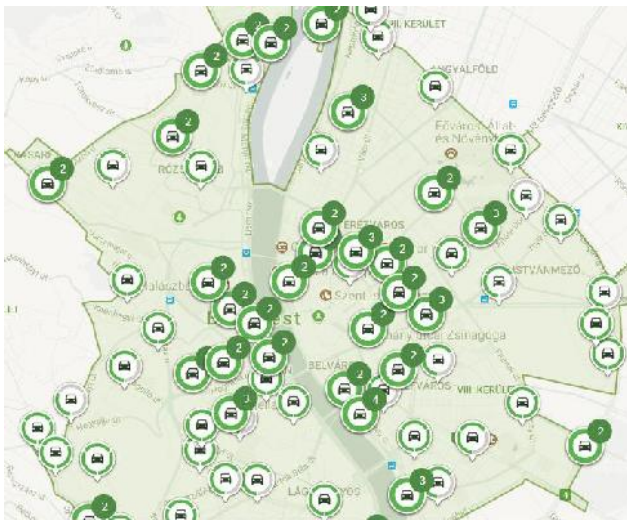
Slika 4. Deljenje automobila, Car Sharing [7]

Slika 5. (Data: US Department of Transportation, RethinkX) prezentuje predviđanje, da u Sjedinjenim Američkim Držvama, već od 2025 godine više kilometara će se prelaziti iznajmljenim nego privatnim automobilima.



Slika 5. Deljenje automobila – predviđanja, Forecast replacement of cars by „transportation-as-a service“ in USA [7]

U Budimpešti, ako na mobilni telefon instaliramo iOS ili Android aplikaciju GreenGo, nakon izvršene registracije, dostupna su nam električna vozila Volkswagen e-Up koja se mogu iznajmiti. Na slici 6 prikazano je dostupnost ovih automobila (lokacija i broj) u Budimpešti.



Slika 6. GreenGo iznajmljivanje električnih vozila Volkswagen e-Up u Budimpešti – lokacija i broj [8]

Podaci za registraciju su:

- login ime, lozinka,
- e-mail adresa,
- podaci bankovne kartice i
- vozačka dozvola.

Nakon registracije u središtu GreenGo kompanije dokumenti se prikazuju i potpisuje se ugovor.

Možemo konstatovati da manji troškovi eksploatacije (manji troškovi servisa i goriva) i deljenje električnih samovozećih automobila prouzrokuje pad tržišne vrednosti klasičnih automobila sa benzinskim i dizel motorima.

## 5. AUTONOMNI SAMOVOZEĆI AUTOMOBILI

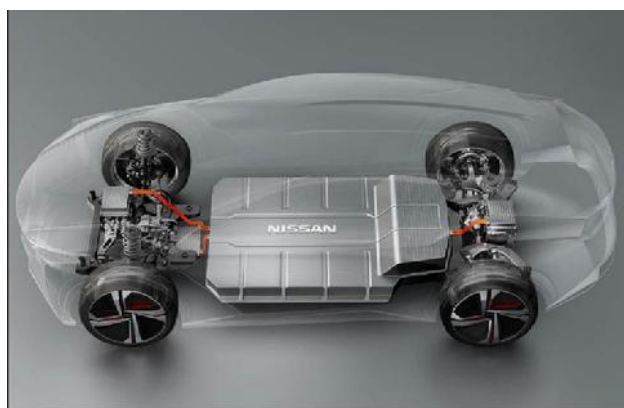
Na sajmu automobila u Tokiju, oktobra 2017 god., iz kompanije Nissan prikazali su električni autonomni samovozeći automobil koncept Nissan IMx crossover, slika 7 sa radijusom kretanja preko 600 km [9].



Slika 7. Nissan IMx električni autonomni samovozeći automobil



Slika 8. Unutrašnjost autonomnog samovozećeg automobila Nissan IMx



Slika 9. Pogon na 4 točka autonomnog samovozećeg automobila Nissan IMx sa dva elektromotora (na prednjoj i zadnjoj osovini)

Nissan IMx električni autonomni samovozeći automobil koncept predstavlja strategiju Nissana u budućnosti 'Nissan Intelligent Mobility' i daje odgovore na integraciju autonomnih samovozećih automobila u društvo, naročito iz aspekta bezbednosti i komfora (slika 8.) u vožnji.

Cilj Nissana je da sa strategijom 'Nissan Intelligent Mobility' dugoročno promeni komunikaciju između čoveka i automobila i društveno prihvatanje autonomnih samovozećih automobila.

ProPilot je centralna upravljačka jedinica Nissan IMx automobila [9] i aktiviranjem ProPilota uvlači se volan i omogućuje se potpuna automatizacija vožnje, u cilju poboljšanja komfora u vožnji nasloni sedišta se pomeraju unazad, tada se vozilo u saobraćaju kreće bez vozača, slika 8. Ako se izabere manuelni, klasičan način vožnje, volan i nasloni sedišta se postavljaju u prethodni položaj i vozač upravlja automobilom.

Nissan IMx električni automobil na EV-platfomi, ima dva elektromotora koji su postavljeni na prednjoj i zadnjoj osovini i pogon na 4 točka, slika 9. EV-platfoma omogućuje ravan pod automobila, što rezultira veliki unutrašnji prostor za putnike. Položaj akumulatora smanjuje visinu težišta automobila i poboljšava stabilnost kretanja autonomnog samovozećeg crossover automobila Nissan IMx.



Drugoj polovini novembra 2017 god. predstavili su autonomni samovozeći automobil Tesla Roadster [10], model 2020, slika 10.



Slika 10. Tesla Roadster električni samovozeći automobil, © Tesla

Tesla Roadster ima pogon na 4 točka, 3 elektromotora (jedan na prednjoj dva na zadnjoj osovini).

Osnovni podaci Roadstera su:

akumulator: 200 kWh, radijus kretanja: 1000 km, ubrzanje: 0 – 100 km/h-ra 2.1 s, maksimalna brzina: 400 km/h.

Tesla Semi električni poluautomatski kamion, slika 11, prikazan je u drugoj polovini novembra 2017.



Slika 11. Tesla Semi električni kamion, © Tesla

Opremljen je tehnologijom za automatsko održavanje kamiona u okvirima saobraćajne trake kojom se kreće i sistemom autonomnog kočenja za slučaj opasnosti. U cilju smanjenja otpora vazduha kamion ima aerodinamični dizajn tako da je radijus kretanja (autonomija) kamiona 800 km.

Akumulatori su smešteni ispod sedišta vozača, ima 4 elektromotora koji pokreću zadnje točkove kamiona. Vozač kamiona, sa obe strane volana (slika 11) ima na raspolaganju dva velika tableta na kojima prati sve funkcije vozila, zadaje komande i vrši podešavanja. Pod punim opterećenjem od 0 do 96 km/h ubrzava za 20 s.

## 6. ZAKLJUČAK

Autonomne samovozeće automobile razvijamo u cilju poboljšanja bezbednosti saobraćaja. Razvoj električnih autonomnih samovozećih vozila prouzrokuje brzu transformacije automobilske industrije i društva. U datim uslovima saobraćaja, autonomni samovozeći automobil kreće se bez intervencije vozača, sensorima detektuje okolinu i donosi potrebne odluke za bezbedno upravljanje automobilom. Navodimo 6 nivoa automatizacije vožnje. U radu prikazujemo električni automobil Nissan Leaf, mrežu punjača električnih automobila u regionu, deljenje automobila, električni autonomni samovozeći automobil koncept Nissan IMx sa ProPilot je centralnom upravljačkom jedinicom, autonomni samovozeći automobil Tesla Roadster i Tesla Semi električni poluautomatski kamion. Razvoj autonomnih samovozećih automobila bazira se na rezultatima istraživanja inteligentnih robota.

## LITERATURA

- [1] Mester G., Pletl S., Pajor G., Jeges Z., Flexible Planetary Gear Drives in Robotics, Proceedings of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation - Robotics, CIM and Automation, Emerging Technologies, IEEE IECON '92, Vol. 2, pp. 646-649, ISBN 0-7803-0582-5, DOI: 10.1109/IECON.1992.254556, San Diego, California, USA, November 9-13, 1992.
- [2] Mester G., Pletl S., Pajor G., and Rudas L., Adaptive Control of Robot Manipulators with Fuzzy Supervisor Using Genetic Algorithms, Proceedings of International Conference on Recent Advances in Mechatronics, ICRAM'95, O. Kaynak (ed.), Vol. 2, pp. 661-666, ISBN 975-518-063-X, Istanbul, Turkey, August 14-16, 1995.
- [3] Rodic A., Mester G., and Stojković I., Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors, pp. 115-134, Intelligent Systems: Models and Applications, Endre Pap (Ed.), Topics in Intelligent Engineering and Informatics, Vol. 3, Part. 2, TIEI 3, ISSN 2193-9411, ISBN 978-3-642-33958-5, DOI 10.1007/978-3-642-33959-2\_7, Springer Verlag Berlin Heidelberg, 2013.
- [4] <https://www.sae.org/news/3544>
- [5] <https://www.plugshare.com>
- [6] <http://www.greentaxi.hu>
- [7] <https://www.rethinkx.com/transportation>
- [8] <https://www.greengo.hu>
- [9] <https://auto.ndtv.com/news/tokyo-motor-show-2017-nissan-imx-all-electric-crossover-concept-unveiled-1766909>
- [10] <https://www.tesla.com/roadster>

# KOEFICIJENT RAZLIČITOSTI ZA REŠAVANJE PROBLEMA FORMIRANJA PROIZVODNIH ČELIJA A DISSIMILARITY COEFFICIENT FOR SOLVING THE MANUFACTURING CELL FORMATION PROBLEM

Miloš Danilović, Oliver Ilić  
*Fakultet organizacionih nauka u Beogradu*

**Sadržaj** – *Formiranje proizvodnih ćelija je prvi i najvažniji korak u projektovanju fleksibilnog proizvodnog sistema. U literaturi su predlagani različiti koeficijenti sličnosti, korišćeni u postupcima za formiranje proizvodnih ćelija. Mera sličnosti, međutim, nije dovoljna da u svim situacijama pravilno razvrsta mašine i delove u ćelije. U cilju prevazilaženja ovih nedostataka, u literaturi je predložena mera različitosti koja predstavlja prosečne vrednosti praznina. U ovom radu je predložena nova mera različitosti za rešavanje problema formiranja proizvodnih ćelija. Ova mera može efikasno da se koristi za smanjenje dopustivog skupa originalnog problema. Mašine ili delovi čija je mera različitosti ispod definisanog praga, ne mogu da pripadaju istoj proizvodnoj ćeliji. Eksperimentalna provera na kompletnom skupu problema, korišćenih u relevantnoj literaturi, pokazuje da se vremenska efikasnost algoritama značajno povećava kada se koristi predloženi koeficijent različitosti.*

**Abstract** – *Manufacturing cell formation is the first and foremost issue in designing cellular manufacturing system. Many similarity coefficient method-based approaches have been proposed to solve the cell formation problem in the literature. However, the measure of similarity cannot always represent accurately the similarity between two groups. In order to overcome these limitations, the average voids value measure was proposed in literature. In this paper, a new, dissimilarity measure for solving the cell formation problem is proposed. This measure can effectively be used to reduce the feasible solution set of the original problem. All machines or parts, having the value of this measure below the defined threshold can't be merged to the same cell. Experimental tests on the set of all test problems used in relevant literature show that the time efficiency can be significantly increased when the proposed measure is used.*

## 1. UVOD

Grupisanje proizvodne opreme u ćelije, koje su specijalizovane za proizvodnju jedne familije delova, naziva se ćelijska proizvodnja. Ćelijska proizvodnja je važan segment štedljive (*lean*) proizvodnje i jedna od glavnih odrednica grupne tehnologije u proizvodnji. Jedan od najvažnijih problema u ćelijskoj proizvodnji je problem formiranja proizvodnih ćelija (*Cell Formation Problem - CFP*). Cilj je da se maksimizira broj operacija

unutar ćelija, a minimizira broj operacija između ćelija. CFP je NP težak problem optimizacije [1], te su razvijeni raznovrsni heuristički algoritmi za rešavanje ovog problema.

U literaturi postoje više pristupa za rešavanje CFP. Sveobuhvatan pregled ovih pristupa je prikazan u [5, 6, 11, 12, 13]. Yin i Yasuda [15] su klasifikovali CF procedure u tri klase: modele matematičkog programiranja, metaheuristike i metode zasnovane na koeficijentima sličnosti (*similarity coefficient methods - SCM*). Oni su zaključili da su SCM metode fleksibilnije u odnosu na druge dve klase. U njihovom radu je dat sveobuhvatan pregled SCM algoritama. Objavljen je veliki broj radova u kojima su predstavljene heuristike za rešavanje CFP u kojima su korišćeni raznovrsni koeficijenti sličnosti kao osnovna mera na osnovu koje se obavlja grupisanje u ćelije. U radu [15] je dat pregled 20 koeficijenata sličnosti, objavljenih u najpoznatijim radovima iz ove oblasti. U tom radu je sprovedena opsežna eksperimentalna evaluacija ovih koeficijenata, i zaključeno je da analizirane mere sličnosti nisu dovoljne da u svim situacijama omoguće pravilno formiranje grupa. U [14] je predložena mera različitosti koja bi omogućila korekciju grupisanja ostvarenu primenom koeficijenata sličnosti.

U ovom radu je predložena nova mera različitosti za rešavanje problema formiranja proizvodnih ćelija. Predloženi koeficijent je denormalizovan, tako da otklanja nedostatak većine koeficijenata sličnosti, čija je vrednost, po pravilu u opsegu (0, 1). Naime vrednost 0 ovih koeficijenata sakriva ogroman opseg stepena različitosti, te je posledica da ovi koeficijenti nisu u stanju da rangiraju različitost. Mera, predložena u ovom radu, omogućuje da mašine ili delovi čija je mera različitosti ispod definisanog praga, ne mogu da pripadaju istoj proizvodnoj ćeliji. Na ovaj način se značajno povećava efikasnost algoritama, pošto se iz razmatranja uklanjaju nedopustiva grupisanja.

Eksperimentalna evaluacija predloženog koeficijenta različitosti je sprovedena na opšte prihvaćenom skupu test instanci objavljenih u [7], koje mogu da se preuzmu sa [8]. Eksperimenti potvrđuju da primena predloženog koeficijenta značajno povećava efikasnost postupaka za formiranje proizvodnih ćelija.

Rad je organizovan na sledeći način. U delu 2 su date definicije problema i pregled najpoznatijih koeficijenata sličnosti. U delu 3 je opisan koeficijent različitosti, predložen u [14]. Novi koeficijent je predstavljen u delu 4, dok je eksperimentalna evaluacija prikazana u delu 5 rada. Zaključna razmatranja su data u delu 6 ovog rada.

## 2. DEFINICIJE POJMOVA

CFP predstavlja grupisanje delova u familije, mašina u ćelije, i dodeljivanje ćelijama odgovarajuće familije delova. Cilj je povećanje efikasnosti i efektivnosti grupisanja podelom sistema na podsisteme koji će biti što autonomniji, u smislu da su interakcije između mašina i delova unutar podsistema maksimizirane, dok su interakcije između podsistema minimizirane [16].

U postupku formiranja ćelija se konstruišu ćelije mašina i familije delova, a zatim se familije delova dodeljuju ćelijama tako da se optimizuje odabrana mera kvaliteta. Sve korišćene mere uključuju dve promenljive: **izuzetke** i **praznine**. Mašina i deo obrazuju izuzetak ako se deo obrađuje na mašini, a pri tome su deo i mašina raspoređeni u različite ćelije; Mašina i deo obrazuju prazninu ako pripadaju istoj ćeliji, a deo se ne obrađuje na mašini.

U radu su, zbog dualnosti, u cilju jasnijeg izlaganja, mašine i delovi označeni kao *entiteti*. Broj entiteta (mašina, odnosno delova) je označen sa  $N$ . Za svaki entitet se definišu *susedi* koji predstavljaju skup entiteta drugog tipa koji ima operaciju nad tim entitetom (npr. susedi određene mašine čine skup svih delova koji se obrađuju na toj mašini).

Koeficijent sličnosti predstavlja meru sličnosti između entiteta, koji se koristi za njihovo grupisanje. Svrha korišćenja koeficijenata sličnosti je da definišu meru koja će da odredi koliko će svrstavanje dva entiteta u istu ćeliju da doprinese vrednosti ciljne funkcije. Prema tome, koeficijent sličnosti direktno zavisi od definicije ciljne funkcije, te je izuzetno važno da se prilikom konstruisanja novih postupaka za CFP ustanovi koji je koeficijent sličnosti najpodesniji za usvojenu ciljnu funkciju.

U algoritmima za CFP je najčešće korišćen Jakardov koeficijent sličnosti [10]:

$$s(i, j) = \frac{q(i, j)}{q(i, j) + g(i, j)}; 0 \leq s(i, j) \leq 1.$$

Promenljiva  $q(i, j)$  predstavlja broj zajedničkih suseda entiteta  $i$  i  $j$ , a  $g(i, j)$  predstavlja broj entiteta koji su susedi samo jednom od ova dva entiteta. Odgovarajuća matrica je matrica sličnosti  $S = \|s(i, j)\|; 1 \leq i \leq N; 1 \leq j \leq N$ .

U literaturi je predložen veliki broj raznovrsnih koeficijenata sličnosti. U velikom broju definicija ovih koeficijenata je, iz neopravdanih razloga, promenljiva  $g(i, j)$  razložena na  $b(i, j) + c(i, j)$ , gde je  $b(i, j)$  broj operacija koje se obavljaju u entitetu  $i$ , a ne u entitetu  $j$ ,

dok je  $c(i, j)$  broj operacija koje se obavljaju u entitetu  $j$ , a ne u entitetu  $i$ . Šta više, koristi se i redundantna promenljiva  $d(i, j)$  koja predstavlja broj operacija koje se istovremeno ne obavljaju ni u jednom od odgovarajućih entiteta. Lako može da se pokaže da je  $d = N - q - b - c$ .

U Tabeli 1 je prikazano 20 koeficijenata sličnosti koji su razmatrani u radu [15].

**Tabela 1.** Koeficijenti sličnosti

Rb.	Koeficijent	Formula
1	Jaccard	$a/(a+b+c)$
2	Hamann	$[(a+d)-(b+c)]/[(a+d)+(b+c)]$
3	Yule	$(ad-bc)/(ad+bc)$
4	Simple matching	$(a+d)/(a+b+c+d)$
5	Sorenson	$2a/(2a+b+c)$
6	Rogers and Tanimoto	$(a+d)/[a+2(b+c)+d]$
7	Sokal and Sneath	$2(a+d)/[2(a+d)+b+c]$
8	Rusell and Rao	$a/(a+b+c+d)$
9	Baroni-Urbani and Buser	$[a+(ad)^{1/2}]/[a+b+c+(ad)^{1/2}]$
10	Phi	$(ad-bc)/[(a+b)(a+c)(b+d)(c+d)^{1/2}]$
11	Ochiai	$a/[(a+b)(a+c)^{1/2}]$
12	PSC	$a^2/[(b+a)(c+a)]$
13	Dot-product	$a/(b+c+2a)$
14	Kulczynski	$1/2[a/(a+b)+a/(a+c)]$
15	Sokal and Sneath 2	$a/[a+2(b+c)]$
16	Sokal and Sneath 4	$1/4[a/(a+b)+a/(a+c)+d/(b+d)+d/(c+d)]$
17	Relative matching	$[a+(ad)^{1/2}]/[a+b+c+d+(ad)^{1/2}]$
18	Chandrasekharan and Rajagopalan	$a/\text{Min}[(a+b),(a+c)]$
19	MaxSC	$\text{Max}[a/(a+b), a/(a+c)]$
20	Baker and Maropoulos	$a/\text{Max}[(a+b),(a+c)]$

Vrednosti koeficijenata 2,3 i 10 su u opsegu  $[-1,1]$ , dok su sve ostale vrednosti koeficijenata u  $[0,1]$ .

Autori sprovode opsežne eksperimentalne testove da bi utvrdili koji su koeficijenti sličnosti najbolji za primenu u postupcima za formiranje proizvodnih ćelija. U tu svrhu su autori eksperimentalno testirali ove koeficijenate u postupcima koji koriste 9 različitih ciljnih funkcija. Analiza je pokazala da su najbolji koeficijenti 1, 5 i 15, dok su izuzetno nepodesni 2, 4, 6, 7 i 8.

U radovima [2, 9] je pokazano da su dobijeni eksperimentalni zaključci mogli da se dobiju i primenom samo teorijskih razmatranja. Teorijski je dokazana nepodesnost koeficijenata koji sadrže parametar  $d$  (koeficijenti 2,4,6,7,8). Kako je ovaj parametar linearno



zavisan od ostalih parametara, posle sređivanja, dobijaju se izrazi koji ne zavise od  $a$ , tako da, npr. parovi objekata:

1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	1	0	0	0	0
i														
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0

daju istu vrednost koeficijenta sličnosti.

Takođe, iz razmatranja treba izbaciti koeficijente sličnosti koji daju različita vrednovanja parametrima  $b$  i  $c$ . Kao primer može da posluži bilo koji od koeficijenata koji koriste min ili max, npr. koeficijent 18. Za ovaj koeficijent sličnosti par objekata:

1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

daje 1 za vrednost koeficijenta sličnosti.

Prema tome, ustanovljeno je da iz razmatranja unapred treba da se izbace nepodesni koeficijenti, i da za poređenje ostaju samo koeficijenti 1, 5, 13, 14 i 15, od kojih su zaista najbolji koeficijenti 1, 5 i 15.

### 3. VREDNOST PROSEČNIH PRAZNINA

U [14] je predstavljena mera različitosti kao **vrednost prosečnih praznina** (*Average Voids Value – AVV*). Ova mera se koristi na isti način u algoritmima za CFP kao i koeficijenti sličnosti. Jedina je razlika u tome što se dva entiteta dodeljuju istoj ćeliji kada imaju malu vrednost koeficijenta različitosti.

AVV predstavlja prosečan broj novih praznina koji se dobija kada se nova grupa mašina oformi sastavljanjem dve grupe mašina, odnosno dve mašine, odnosno mašine i grupe mašina:

$$AVV = \frac{v_{ij} - v_i}{M_i} + \frac{v_{ij} - v_j}{M_j}$$

Izraz predstavlja sumu dve prosečne vrednosti. Prvi sabirak predstavlja prosečan broj novih praznina u odnosu na broj praznina u grupi  $i$ , kada se spoje grupe  $i$  i  $j$ . Analogno ovome, drugi sabirak predstavlja prosečan broj novih praznina u odnosu na broj praznina u grupi  $j$ , kada se spoje grupe  $i$  i  $j$ . Relacija između dve grupe mašina je zasnovana na relaciji svake od mašina prve grupe sa drugom grupom umesto na relaciji svake od mašina prve grupe sa svakom od mašina druge grupe.

Predloženi koeficijent ima značaj u unapređenju postupka za grupisanje entiteta, ali ima i čitav niz nedostataka. Kao prvo, prosek uvek prikriva neke bitne parametre koji određuju karakter grupisanja. U prethodnom izrazu, grupa je predstavljena jednom vrednošću, broju praznina u toj grupi. Na taj način se gubi informacija o uticaju pojedinih

mašina u grupi na ukupan broj praznina. Ovo dalje prouzrokuje da se gubi mogućnost da se od dve grupe, formiraju dve grupe različite po sastavu od prethodnih grupa, umesto da se formira sumarna grupa.

Drugi nedostatak je odsustvo razmatranja izuzetaka. Može da se navede čitav niz primera gde izuzeci imaju mnogo značajniji uticaj na vrednost ciljne funkcije od praznina.

Najzad, primena ovog koeficijenta ne predstavlja nikakvu novinu u postupku formiranja ćelija. Grupisanje se vrši po istom postupku kao i kada se primenjuje koeficijent sličnosti, sa jedinom razlikom što se u ovom slučaju bira najmanja, a ne najveća vrednost koeficijenta.

### 4. NOVI KOEFICIJENT RAZLIČITOSTI

Prethodni nedostaci mogu da se prevaziđu primenom redukovane matrice  $B$ , predložene u radu [2]. Ova matrica odražava trenutni sastav ćelija u toku procesa formiranja ćelija. Na početku postupka ona je jednaka matrici susedstva, a tokom postupka predstavlja ulazni podatak koji u potpunosti zamenjuje matricu susedstva. U radu [2] je dokazano da svi koeficijenti, korišćeni u radovima za CFP mogu jednoznačno da se izračunaju, koristeći samo matricu  $B$ .

Elementi matrice  $B = \|b(i, j)\|$  su jednaki sumi odgovarajućih elemenata matrice susedstva  $A$ , pri čemu se sumiraju elementi koji pripadaju istoj grupi entiteta. Na ovaj način je broj kolona matrice  $B$  jednak broju familija delova, dok je broj redova jednak broju grupa mašina. Kao primer koristimo matricu susedstva prikazanu u Tabeli 2:

Tabela 2. Matrica  $A$  za dati primer

M/D	1	2	3	4	5	6	7	8
1	0	1	0	1	0	0	1	0
2	1	1	1	0	1	1	1	1
3	0	0	1	0	0	1	0	1
4	0	0	0	1	0	0	1	0
5	1	0	1	0	1	1	0	1
6	0	0	0	1	0	0	1	0

Tabela 2 predstavlja matricu susedstva za primer od 6 mašina i 8 delova. Naka su grupe mašina  $\{\{4,6\}, \{1\}, \{2\}, \{3\}, \{5\}\}$ , a grupe delova  $\{\{1,5\}, \{3,6,8\}, \{2\}, \{4\}, \{7\}\}$ . Matrica  $B$  je prikazana u Tabeli 3.

Najzad, uvodi se matrica  $H = \|h(i, j)\|$  čiji elementi predstavljaju dimenzije odgovarajućih grupa. Za prethodni primer, matrica  $H$  je prikazana u Tabeli 4.

**Tabela 3.** Matrica  $B$  za dati primer

	1	2	3	4	5
1	0	0	0	2	2
2	0	0	1	1	1
3	2	3	1	0	1
4	0	3	0	0	0
5	2	3	0	0	0

**Tabela 4.** Matrica  $H$  za dati primer

	1	2	3	4	5
1	4	6	2	2	2
2	2	3	1	1	1
3	2	3	1	1	1
4	2	3	1	1	1
5	2	3	1	1	1

U radu [2] je dokazano sledeće tvrđenje:

**Stav 1.** Ako  $b(i, j)$  pripada grupi, on doprinosi ukupnom broju praznina sa  $h(i, j) - b(i, j)$ , inače, doprinosi ukupnom broju izuzetaka sa  $b(i, j)$ .

Ovo je suštinski zaključak koji omogućuje da iz matrice  $B$  dobijemo koeficijente sličnosti i različitosti koji ispravljaju tri pomenuta nedostatka koeficijenta AVV. Kao prvo, koeficijenti mogu da se definišu bez korišćenja prosečnih vrednosti, pošto se prati sastav oformljenih grupa. Drugo, paralelno sa prazninama koriste se i podaci o izuzecima. Najzad, matrica  $B$  omogućuje da se definiše potpuno novi postupak kojim bi se definisale grupe koje ne mogu da se spajaju u postupku formiranja ćelija.

Predloženi koeficijent različitosti se definiše kao:

$t(i, j) = q(i, j) - g(i, j)$ , a  $T = \|t(i, j)\|, 1 \leq i \leq N; 1 \leq j \leq N$  predstavlja matricu različitosti.

Elementi matrica  $S$  i  $T$  su funkcije zajedničkih suseda,  $q(i, j)$  i zasebnih suseda,  $g(i, j)$ . U procesu formiranja proizvodnih ćelija, određivanje zajedničkih i zasebnih suseda na osnovu matrica  $B$  i  $H$  je veoma jednostavno. Neka je  $l$  entitet drugog tipa u odnosu na entitete  $i$  i  $j$ . Označimo sa  $b_1$  element od  $B$  koji odgovara entitetima  $i$  i  $l$ , a sa  $b_2$  element matrice  $B$  koji odgovara entitetima  $j$  i  $l$ . Ukoliko entitet  $l$  učestvuje u vrednosti  $q(i, j)$  sa  $Q$ , a  $l$  učestvuje u vrednosti  $g(i, j)$  sa  $G$ , mogu da nastupe dva slučaja: Kada je  $h_1 + h_2 \geq 2(b_1 + b_2)$  tada je  $Q=0$  i  $G=b_1+b_2$ . Inače,  $Q=\min(b_1, b_2)$  i  $G=h_1+h_2-b_1-b_2$ . Matrica  $T$  predstavlja pogodnu meru za kvantifikovanje različitosti. Ova mera može efektivno da se iskoristi u cilju smanjenja dopustivog skupa na sledeći način. Svaki par entiteta  $i$  i  $j$  za koje je vrednost  $t(i, j)$  ispod unapred definisanog praga mora u konačnom grupisanju da pripada različitim ćelijama. U eksperimentalnoj evaluaciji prag je određen

kao prosečna vrednost elemenata u  $T$ . Ovako definisan prag je bio ispravan izbor za svaku od testiranih instanci.

## 5. EKSPERIMENTALNI REZULTATI

Skoro svi relevantni postupci za rešavanje CFP su testirani na skupu od 35 instanci predstavljenih u [7]. Tabela 5 predstavlja spisak ovih instanci pri čemu kolona  $N_m$  sadrži broj mašina, kolona  $N_d$  broj delova, a kolona Autor, imena autora i godinu objavljivanja.

**Tabela 5.** Spisak referentnih instanci

Rb.	$N_m$	$N_d$	Autor
1	5	7	(King & Nakornchai, 1982)
2	5	7	(Waghodekar & Sahu, 1984)
3	5	18	(Seifoddini H., 1989)
4	6	8	(Kusiak & Cho, 1992)
5	7	11	(Kusiak & Chow, 1987)
6	7	11	(Boctor, 1991)
7	8	12	(Seifoddini & Wolfe, 1986)
8	8	20	(Chandras. & Rajagopalan, 1986)
9	8	20	(Chandras. & Rajagopalan, 1986)
10	10	10	(Mosier & Taube, 1985)
11	10	15	(Chan & Milner, 1982)
12	14	23	(Askin & Subramanian, 1987)
13	14	24	(Stanfel, 1985)
14	16	23	(McCormick <i>et all</i> , 1972)
15	16	30	(Srinivasan <i>et all</i> , 1990)
16	16	43	(King J., 1980)
17	18	24	(Carrie, 1973)
18	20	20	(Mosier & Taube, 1985a)
19	20	23	(Kumar <i>et all</i> , 1986)
20	20	35	(Carrie, 1973)
21	20	35	(Boe & Cheng, 1991)
22	24	40	(Chandras. & Rajagopalan, 1989)
23	24	40	(Chandras. & Rajagopalan, 1989)
24	24	40	(Chandras. & Rajagopalan, 1989)
25	24	40	(Chandras. & Rajagopalan, 1989)
26	24	40	(Chandras. & Rajagopalan, 1989)
27	24	40	(Chandras. & Rajagopalan, 1989)
28	27	27	(McCormick <i>et all</i> 1972)
29	28	46	(Carrie, 1973)
30	30	41	(Kumar & Vannelli, 1987)
31	30	50	(Stanfel, 1985)
32	30	50	(Stanfel, 1985)
33	30	90	(King & Nakornchai, 1982)
34	37	53	(McCormick <i>et all</i> 1972)
35	40	100	(Chandras. & Rajagopalan, 1987)

Evaluacija parametara je sprovedena na sledeći način. Za svaku instancu je izvršeno grupisanje entiteta na osnovu maksimalnih vrednosti njihovih koeficijenata sličnosti. Dobijena matrica  $B$  je zatim korišćena kao ulazni parametar iz koga su određeni parovi entiteta sa vrednošću koeficijenta različitosti ispod praga, definisanog u prethodnom odeljku. Zatim je izvršena provera nad optimalnim ćelijskim grupisanjem za tu instancu i izračunat broj slučajeva u kojima je odluka o

zabrani grupisanja bila pogrešna. Rezultat evaluacije je potvrdio ispravnost odluke o zabrani grupisanja u 100% testiranih parova na svakoj od testiranih instanci

Postupak evaluacije može da se prikaže na primeru najveće instance, Rb. 35 (40x100).

Posle grupisanja na osnovu koeficijenata sličnosti, dobijena je matrica  $B$ , dimenzija 14x17, prikazana u Tabeli 6. Odgovarajuća grupisanja mašina, odnosno delova su:

$$E^M = \{\{2,10,16,21,31\}, \{1,3,7,32\}, \{6,12,26,38,40\}, \{18,33,34\}, \{5,8,22,23,37,39\}, \{19,25,28\}, \{14,35\}, \{11,13\}, \{4,9,20\}, \{24,27,29\}, \{15\}, \{17\}, \{30\}, \{36\}\}.$$

$$E^P = \{\{36,38,42,51,52,64,65,70,72,74,75,76,80,87\}, \{45,67,71,91\}, \{6,15,16,24,27,60\}, \{35,47,53,78,79,83,88,93\}, \{8,11,13,14,20,22,23,32\}, \{39,73\}, \{10,18,29,33,34,37,44,49,50,54,55\}, \{63,66,68,69,82,84,85,89,90,92,94,96,97,98,99,100\}, \{1,2,3,4,5,7,21,25,28\}, \{9,12,17,19,26,30,31,40,43,46\}, \{56,57,58,59,61,62\}, \{41\}, \{48\}, \{77\}, \{81\}, \{86\}, \{95\}\}.$$

Tabela 6. Matrica  $B$  za instancu Rb. 35

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1		2				36								4		1	
2								40	1			3	1				
3	62			2			1	1							4	4	1
4		11				5		1									
5	1									1				1		1	5
6		1				1		1		1	18				1		
7				12			1		1								
8			2						18	1			2				
9						23		1									
10										30		1					
11		4											1				
12			4						1						1		
13		1		1	1						6						
14	1	3		1	1	2	1										

Prag za mašine je -42 i broj parova ispod ovog praga je 33. Za delove, prag je -29 i broj parova ispod ovog praga je 46. Slika 1 prikazuje matricu  $T$  za mašine, dok Slika 2 prikazuje matricu  $T$  za delove. Žutom bojom su označeni elementi matrice koji odgovaraju entitetima čiji je koeficijent različitosti ispod praga. Zelenom bojom je označena maksimalna, a crvenom bojom minimalna vrednost koeficijenta  $t(i, j)$ .

Prvih deset grupisanih mašina i prvih 11 grupisanih delova formiraju jasno izražene pod-matrice. Sa Slike 2 je jasno da svaki od ovih 11 grupisanih delova, izuzev dela 6 moraju da formiraju zasebnu ćeliju. Grupisani deo 6 ne može da bude u ćeliji u kojoj je deo 1. Na ovaj način je definisano svih deset ćelija iz optimalnog grupisanja. Ovo dalje omogućuje da se, koristeći bilo koji poznati postupak pridruživanja mašina ovako formiranim ćelijama, trenutno odredi optimalno grupisanje delova u familije i mašina u ćelije. U sprovedenom eksperimentu

za instancu Rb. 35 (najveća instanca iz Tabele 5), optimalno rešenje je dobijeno za 0.9sec. Poređenja radi, egzaktni algoritam CPLEX [4], dobija isti rezultat za 1,572,184.5 sec, dok najbolje poznate heuristike isti rezultat dobijaju za oko 300 sec.

avg. : -42, Treshold: -42, number of pairs: 33														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
01	0	-88	-118	-52	-140	-58	-40	-49	-59	-66	-22	-23	-23	-22
02	-88		-120	-59	-126	-65	-45	-54	-66	-71	-24	-25	-28	-27
03	-118	-120		-80	-167	-83	-61	-70	-87	-94	-36	-34	-40	-36
04	-52	-59	-80		-78	-40	-26	-38	-41	-48	-2	-15	-15	-2
05	-140	-126	-167	-78		-84	-61	-70	-85	-95	-35	-36	-39	-35
06	-58	-65	-83	-40	-84		-31	-40	-47	-51	-16	-17	-2	-19
07	-40	-45	-61	-26	-61	-31		-28	-32	-35	-13	-2	-17	-16
08	-49	-54	-70	-38	-70	-40	-28		-41	-41	-15	-16	-22	-21
09	-59	-66	-87	-41	-85	-47	-32	-41		-55	-15	-16	-16	-18
10	-66	-71	-94	-48	-95	-51	-35	-41	-55		-16	-17	-20	-19
11	-22	-24	-36	-2	-35	-16	-13	-15	-15	-16		-11	-11	-4
12	-23	-25	-34	-15	-36	-17	-2	-16	-16	-17	-11		-15	-14
13	-23	-28	-40	-15	-39	-2	-17	-22	-16	-20	-11	-15		-17
14	-22	-27	-36	-2	-35	-19	-16	-21	-18	-19	-4	-14	-17	

Slika 1. Matrica  $T$  za mašine

avg. : -29, Treshold: -29, number of pairs: 46																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
01	0	-52	-60	-86	-76	-31	-105	-159	-78	-95	-66	-21	-21	-22	-11	-11	-20
02	-52		-34	-48	-34	-2	-41	-57	-31	-35	-30	-13	-10	-14	-15	-15	-15
03	-60	-34		-56	-38	-16	-47	-67	-27	-39	-42	-11	-11	-12	-10	-13	-13
04	-86	-48	-56		-64	-27	-77	-101	-59	-67	-62	-17	-17	-6	-19	-16	-19
05	-76	-34	-38	-64		-17	-61	-85	-43	-51	-44	-9	-9	-10	-11	-11	-11
06	-31	-2	-16	-27	-17		-22	-34	-16	-18	-14	-11	-11	-12	-13	-13	-13
07	-105	-41	-47	-77	-61	-22		-120	-59	-74	-53	-4	-10	-14	-15	-15	-15
08	-159	-57	-67	-101	-85	-34	-120		-88	-103	-73	-23	-23	-21	-25	-22	-10
09	-78	-31	-27	-59	-43	-16	-59	-88		-51	-39	-9	-3	-10	-11	-11	-11
10	-95	-35	-39	-67	-51	-18	-74	-103	-51		-45	-7	-10	-11	-12	-12	-12
11	-66	-30	-42	-62	-44	-14	-53	-73	-39	-45		-8	-8	-9	-7	-10	-10
12	-21	-13	-11	-17	-9	-11	-4	-23	-9	-7	-8		-8	-9	-10	-10	-10
13	-21	-10	-11	-17	-9	-11	-10	-23	-3	-10	-8	-8		-9	-10	-10	-10
14	-22	-14	-12	-6	-10	-12	-14	-21	-10	-11	-9	-9	-9		-11	-11	-11
15	-11	-15	-10	-19	-11	-13	-15	-25	-11	-12	-7	-10	-10	-11		-2	-12
16	-11	-15	-13	-16	-11	-13	-15	-22	-11	-12	-10	-10	-10	-11	-2		-12
17	-20	-15	-13	-19	-11	-13	-15	-10	-11	-12	-10	-10	-10	-11	-12	-12	

Slika 2. Matrica  $T$  za delove

## 6. ZAKLJUČAK

U radu je predložen novi koeficijent različitosti između entiteta za primenu u postupcima za rešavanje problema formiranja proizvodnih ćelija. Za razliku od koeficijenata sličnosti, koji se decenijama primenjuju u postupcima za rešavanje CFP, jedan koeficijent različitosti je predstavljen u radu [14]. Ovaj koeficijent je u tom radu primenjen na isti način kao i ostali koeficijenti sličnosti, sa jedinom razlikom što je grupisanje određivala najmanja, a ne najveća vrednost koeficijenta.

Koeficijent, predložen u ovom radu, predstavlja kvalitativno nov pristup primene koeficijenata u problemima za rešavanje CFP. Na osnovu vrednosti ovog koeficijenta određuju se parovi entiteta koji ne mogu da pripadaju istim ćelijama u optimalnom grupisanju entiteta. Na ovaj način se dopustivi skup rešenja smanjuje, čime se povećava efikasnost postupka za CFP koji primenjuje ovaj koeficijent.

Eksperimentalna provera ovog koeficijenta na referentnom skupu od 35 instanci je nedvosmisleno potvrdila značaj primene ovog koeficijenta u postupcima za CFP. Usvojeni prag vrednosti je omogućio da, ni za jedan par entiteta, odluka o zabrani grupisanja nije bila pogrešna.

Budući pravac istraživanja bi podrazumevao primenu ovog koeficijenta u najboljim poznatim heuristikama za CFP i utvrđivanje poboljšanja koja prouzrokuje primena ovog koeficijenta. Takođe, istraživanja mogu da budu usmerena i ka definisanju novog postupka koji primenjuje ovaj koeficijent i koji bi bio efektivniji i efikasniji od poznatih algoritama za CFP.

## LITERATURA

- [1] Ballakur, A., & Steudel, H. (1987). A within-in cell utilization based heuristic for designing cellular manufacturing system. *International Journal of Production Research*, 25, 639–55.
- [2] Danilović, M., & Ilić, O. (2018) A novel problem reduction approach to manufacturing cell formation, submitted to *Computers & Industrial Engineering*
- [3] Даниловић, М., Илић, О., Кнежевић И., Величковић, Ј., & Ђајић, З. (2017). Избор коефицијента сличности за проблем формирања производних ћелија, *SPIN 2017, XI Скуп привредника и научника, Факултет организационих наука, Универзитет у Београду, Зборник радова*, стр. 39-46, ISBN: 978-86-7680-343-9
- [4] Elbenani, B., & Ferland, J. (2012). An Exact Method for Solving the Manufacturing Cell Formation Problem. *International Journal of Production Research*, 50, 4038-4045.
- [5] Ghosh, T., Dan, P., Sengupta, S., & Chattopadhyay, M. (2010). Genetic rule based techniques in cellular manufacturing (1992–2010): a systematic survey. *International Journal of Engineering, Science and Technology*, 2(5), 198–215.
- [6] Ghosh, T., Sengupta, S., Chattopadhyay, M., & Dan, P. (2010). Meta-heuristics in cellular manufacturing: a state-of-the-art review. *International Journal of Industrial Engineering Computations*, 2, 87–122.
- [7] Goncalves, J., & Resende, M. (2004). An evolutionary algorithm for manufacturing cell formation. *Computers & Industrial Engineering*, 47, 247–73.
- [8] <http://mauricio.resende.info/data/cell-formation/>.
- [9] Илић, О., Даниловић, М., Стојкоски, А., & Микашевић, А. (2017). Поређење коефицијената сличности за проблем формирања производних ћелија, *SPIN 2017, XI Скуп привредника и научника, Факултет организационих наука, Универзитет у Београду, Зборник радова*, стр. 47-54, ISBN: 978-86-7680-343-9.
- [10] Jaccard, P. (1908). Nouvelles recherches sur la distribution florale. *Bulletin de la Societe` Vaudoise des Sciences Naturelles*, 44.
- [11] Papaioannou, G., & Wilson, J. (2010). The evolution of cell formation problem methodologies based on recent studies (1997–2008): Review and directions for future research. *European Journal of Operational Research*, 206(3), 509–21.
- [12] Paydar, M., & Saidi-Mehrabad, M. (2013). A Hybrid Genetic-Variable Neighborhood Cell Formation Problem Based on Group Efficiency. *Computers & Operations Research*, 40, 980-990.
- [13] Singh, N. (1993). Design of cellular manufacturing systems: An invited review. *European Journal of Operational Research*, 69, 284–291.
- [14] Yasuda, K., & Yin, Y. (2001). A dissimilarity measure for solving the cell formation problem in cellular manufacturing, *Computers & Industrial Engineering* 39, 1-17.
- [15] Yin, Y., & Yasuda, K. (2006). Similarity coefficient methods applied to the cell formation problem: A taxonomy and review. *International Journal of Production Economics*, 101, 329–352.
- [16] Wu, T., Chang, C., & Yeh, J. (2009). A hybrid heuristic algorithm adopting both Boltzmann function and mutation operator for manufacturing cell formation problems. *International Journal of Production Economics*, 120, 669–88.

# OBELODANJIVANJE FINANSIJSKIH INFORMACIJA JAVNOG SEKTORA NA INTERNETU

## DISCLOSURE OF PUBLIC SECTOR FINANCIAL INFORMATION ON THE INTERNET

Kristina Mijić<sup>1</sup>

*Univerzitet u Novom Sadu, Ekonomski fakultet u Subotici<sup>1</sup>*

**Sadržaj** – *Finansijski izveštaji korisnika budžetskih sredstava, koji predstavljaju osnovu za donošenje poslovnih odluka pre svega investitora, nisu javno dostupni posredstvom jedinstvenog registra. Kao jedan od načina dostupnosti finansijskih izveštaja i drugih informacija o poslovanju entiteta javnog sektora ističe se obelodanjivanje finansijskih informacija na veb-sajtu korisnika budžetskih sredstava. Predmet istraživanja predstavlja merenje kvaliteta obelodanjivanja finansijskih izveštaja i drugih informacija kao što su budžet, rebalansi budžeta, prospekti za investitore i dr. na veb-sajtu korisnika budžetskih sredstava i to na uzorku od 32 veb-sajta gradova i opština u Republici Srbiji. Kvalitet obelodanjivanja finansijskih informacija meren je na bazi indeksa sadržaja i indeksa dostupnosti informacija na veb-sajtu gradova i opština. Rezultati istraživanja ukazuju da gradovi obelodanjuju više informacija o poslovanju na veb-sajtu u odnosu na opštine. Dalje, rezultati istraživanja identifikovali su nekoliko kritičnih područja koja ukazuju na potrebna unapređenja kvaliteta finansijskog izveštavanja na veb-sajtu gradova i opština.*

**Ključne reči:** *Finansijski izveštaji, internet, javni sektor, veb-sajt.*

**Abstract** – *Public sector financial statements represent the basis for decision making primarily for investors and are not publicly available through a web based register. One of the way of accessing financial reports and other information of public sectors entities is disclosure of financial information through website of entities. The aim of this paper is to investigate the quality of disclosure of financial statements and other information such as budget, budget rebalances, information for investors, etc. on the website of the cities and municipalities in the Republic of Serbia. The quality of disclosure of financial information was measured on the basis of index of content and index of accessibility of financial information on the website of cities and municipalities. The results indicate that cities disclose more financial information on the website compared to the municipalities. Furthermore, the research results indicate to several critical areas that point to the necessary improvements of the financial reporting system quality on the website of cities and municipalities.*  
**Keywords:** *financial statements, internet, public sector, website.*

### 1. UVOD

Finansijski izveštaji i druge informacije o poslovanju entiteta javnog sektora predmet su interesovanja velikog broja korisnika, bilo da oni imaju cilj da samo sagledaju kako je entitet javnog sektora upravljao budžetskim

sredstvima, ili imaju cilj i da donesu poslovnu odluku. Adekvatno poslovno odlučivanje korisnika izveštaja o poslovanju entiteta javnog sektora, kao što su investitori, kreditori i drugi, treba da rezultira ostvarivanjem prinosa na osnovu izvršenih ulaganja. Sa druge strane, entiteti javnog sektora ulaganja treba da koriste namenski za programske aktivnosti koje će rezultirati rastom i razvojem. Prema tome, kao pretpostavka razvoja entiteta javnog sektora ističe se obezbeđivanje kvalitetnog sistema finansijskog izveštavanja.

U današnje vreme ne može se zamisliti proces i sistem finansijskog izveštavanja bez upotrebe informacionih sistema i interneta. Posmatrajući sistem finansijskog izveštavanja u Republici Srbiji za entitete javnog sektora uočava se nepostojanje jedinstvene javno dostupne baze finansijskih izveštaja i drugih informacija o poslovanju entiteta javnog sektora. Kako bi se obezbedila blagovremena i javna dostupnost finansijskih izveštaja i drugih informacija o poslovanju entiteta javnog sektora u Republici Srbiji kao adekvatan sistem finansijskog izveštavanja ističe se obelodanjivanje informacija o poslovanju na veb-sajtu entiteta javnog sektora, koje je poznato i pod nazivom internet finansijsko izveštavanje. Internet finansijsko izveštavanje se može definisati kao distribucija finansijskih izveštaja i drugih informacija o performansama poslovanja entiteta posredstvom internet tehnologije kao što je WWW [5]. Sa aspekta kreatora izveštaja obelodanjivanje finansijskih izveštaja i drugih informacija o poslovanju na veb-sajtu eliminiše nedostatke finansijskog izveštavanja u papirnoj formi kao što su smanjenje vremena distribucije izveštaja korisnicima, smanjenje troškova kreiranja izveštaja i sl. Kao značajna prednost finansijskog izveštavanja putem veb-sajta sa aspekta korisnika ističe se preuzimanje izveštaja uz značajno niže troškove i skraćanje vremena [9]. Takođe, eliminisanje papirne forme finansijskog izveštavanja zahteva od kreatora i korisnika izveštaja digitalnu pismenost. Digitalna pismenost predstavlja sposobnost osobe da efektivno koristi računar u svoj radu i van radnog mesta [2]. Izgradnja kvalitetnog sistema finansijskog izveštavanja na veb-sajtu u nadležnosti je svakog pojedinačnog entiteta javnog sektora. Sistem finansijskog izveštavanja na veb-sajtu entiteta javnog sektora treba da se zasniva na pružanju svih relevantnih i pravovremenih informacija za sve zainteresovane korisnika.

U radu će se istražiti kvalitet obelodanjivanja finansijskih informacija gradova i opština u Republici Srbiji na veb-sajtovima. Istraživanje obuhvata pretraživanje 32 veb-sajta gradova i opština sa aspekta sadržaja finansijskih informacija i sa aspekta dostupnosti.

## **2. REGULATIVA I ULOGA FINANSIJSKOG IZVEŠTAVANJA LOKALNE SAMOUPRAVE U REPUBLICI SRBIJI**

Finansijsko izveštavanje korisnika budžetskih sredstava u Republici Srbiji detaljnije je regulisano Zakonom o budžetskom sistemu („Sl. glasnik RS“ br. 113/2017), Pravilnikom o načinu pripreme, sastavljanja i podnošenja finansijskih izveštaja korisnika budžetskih sredstava, korisnika sredstava organizacija za obavezno socijalno osiguranje i budžetskih fondova („Sl. glasnik RS“, br. 18/2015), Uredbom o budžetskom računovodstvu („Sl. glasnik RS“, br. 125/03 i 12/06) i drugim relevantnim propisima. Budžetsko računovodstvo u Republici Srbiji zasnovano je na gotovinskoj osnovi [10]. Standardni set finansijskog izveštaja obuhvata: bilans stanja, bilans prihoda i rashoda, izveštaj o kapitalnim izdacima i primanjima, izveštaj o novčanim tokovima i izveštaj o izvršenju budžeta [11]. Forma finansijskih izveštaja korisnika budžetskih sredstava je propisana Pravilnikom. Ukoliko su se u toku poslovne godine realizovale specifične poslovne transakcije korisnici budžetskih sredstava treba da dostave i sledeće izveštaje: objašnjenje velikih odstupanja između odobrenih sredstava i izvršenja, izveštaj o korišćenju sredstava tekuće i stalne budžetske rezerve, izveštaj o garancijama datim u toku fiskalne godine i pregled primljenih donacija i kredita, domaćih i stranih, kao i izvršenih otplata kredita [11]. Forma navedenih dodatnih elemenata finansijskog izveštaja korisnika budžetskih sredstava nije propisana. Kao obavezan element završnog računa lokalne vlasti jeste i izveštaj eksterne revizije koji ukazuje na istinitost i objektivnost sastavljenih finansijskih izveštaja i usklađenosti sa regulativom finansijskog izveštavanja [11]. Pored finansijskog izveštaja lokalna vlast sastavlja i brojne druge izveštaje kao što su budžet, rebalansi budžeta, prospekti za investitore i slično. Završni račun, odnosno finansijski izveštaj i izveštaj eksternog revizora, lokalna vlast mora predati Upravi za trezor najkasnije do 15. juna, odnosno 01. jula ukoliko je u pitanju konsolidovani izveštaj grada [12].

Uprava za trezor prikuplja, obrađuje i formira bazu korisnika budžetskih sredstava i njihovih finansijskih izveštaja. Međutim, finansijski izveštaji putem veb-sajta Uprave za trezor nisu javno dostupni. Naime, u Republici Srbiji ne postoji javno dostupan registar finansijskih izveštaja korisnika budžetskih sredstava, kao npr. što postoji javno dostupan registar finansijskih izveštaja privrednih društava na veb-sajtu Agencije za privredne registre. U ovakvim uslovima dovodi se u pitanje ostvarivanje osnovnog cilja finansijskog izveštavanja u javnom sektoru u Republici Srbiji.

Osnovni cilj finansijskog izveštavanja u javnom sektoru jeste da se obelodane informacije iz finansijskog izveštaja i druge informacije o poslovanju korisnika budžetskih sredstava koje su od značaja brojnim korisnicima. Kao korisnici finansijskih izveštaja i drugih informacija o poslovanju javnog sektora ističu se pre svega postojeći i potencijalni investitori, kreditori, donatori, državni organi,

statistički zavodi, poreski obveznici i dr. Korisnici finansijskih izveštaja i drugih informacija o poslovanju entiteta javnog sektora donose različite poslovne odluke. Tako npr. postojeći i potencijalni investitori na osnovu informacija o poslovanju entiteta javnog sektora donose odluke o nastavku ili pokretanju novih ulaganja u osnivanje privrednih društava i zapošljavanje radnika. Interes države u finansijskom izveštavanju javnog sektora ogleda se pre svega u sagledavanju izvršenja budžeta, radi pripreme budžeta za naredni period. Kreditori odnosno banke na osnovu informacija iz finansijskih izveštaja i drugih relevantnih informacija donose odluke o odobravanju kredita entitetima javnog sektora.

U cilju donošenja adekvatnih poslovnih odluka koje treba da rezultiraju ostvarivanjem buduće ekonomske koristi korisnicima finansijskih izveštaja javnog sektora treba da se obezbede istinite i blagovremene informacije. Na osnovu informacija iz finansijskih izveštaja i drugih informacija o poslovanju javnog sektora korisnici će moći da sagledaju performanse javnog sektora, solventnost i likvidnost, da procene dugoročnu održivost aktivnosti javnog sektora, i procene sposobnost prilagođavanja promenama iz okruženja [7]. Obezbeđivanjem kvalitetnog sistema finansijskog izveštavanja, odnosno pružanjem potpunih, istinitih i blagovremenih informacija o poslovanju javnog sektora, korisnici izveštaja smanjuju rizik neadekvatnog poslovnog odlučivanja.

## **3. KAKO MERITI KVALITET IZVEŠTAVANJA ENTITETA JAVNOG SEKTORA NA INTERNETU?**

Istraživanja na temu izveštavanja entiteta javnog sektora na internetu, odnosno putem veb-sajta entiteta javnog sektora, manje su zastupljena od istraživanja internet izveštavanja privrednih društava iz realnog sektora. Autori istraživanja internet finansijskog izveštavanja privrednih društava baziraju na oceni kvaliteta internet finansijskog izveštavanja, putem indeksa finansijskog izveštavanja, kao i na analizi faktora koji utiču na ocenu kvaliteta internet finansijskog izveštavanja [opširnije videti: 1, 3, 9]. Kada je reč o istraživanjima kvaliteta izveštavanja javnog sektora na veb-sajtu, autori analiziraju dve komponente kvaliteta, a to su: sadržaj i dostupnost. Autori Groff i Pitmann su istraživali sadržaj i dostupnost finansijskih informacija na 100 veb-sajtova opština u Sjedinjenim Američkim Državama [6], a potom su se istim pitanjem na bazi uzorka od 300 veb-sajtova opština bavili autori Styles i Tennyson [13]. Autori Laswar i saradnici istraživali su kvalitet finansijskog izveštavanja 30 entiteta lokalne samouprave na Novom Zelandu na veb-sajtu uz identifikaciju faktora koji utiču na kvalitet sa aspekta sadržaja [8]. Dalje, autor Verawaty je istraživao kvalitet finansijskog izveštavanja sa aspekta dostupnosti informacija putem veb-sajta kao i postojanje razlika u kvalitetu između pokrajina i opština [14]. Sadržaj kao komponenta kvaliteta internet finansijskog izveštavanja entiteta javnog sektora ukazuje na obavezna i dopunska obelodanjivanja na veb-sajtu entiteta javnog sektora kao što su: godišnji finansijski izveštaj, izveštaj nezavisnog revizora, budžet, rebalansi budžeta, prospekti za investitore i slično. Broj obeležja koji čine komponentu sadržaja zavisi pre svega od zakonske

regulative finansijskog izveštavanja javnog sektora. Ukoliko se neko obeležje, odnosno element sadržaja finansijskog izveštavanja nalazi na veb-sajtu entiteta javnog sektora, dodeljuje se vrednost 1, u suprotnom vrednost 0. Konačna ocena za sadržaj se iskazuje obično u procentima obelodanijenih elemenata. Prema tome, sadržaj kao mera kvaliteta finansijskog izveštavanja entiteta javnog sektora se izračunava na sledeći način:

$$\text{Sadržaj} = \frac{\sum_{i=1}^n X_i}{n} \times 100$$

Gde je:

$X_i$  – obeležja sadržaja

Dostupnost kao mera kvaliteta finansijskog izveštavanja entiteta javnog sektora na internetu ukazuje na format prikaza finansijskih informacija, mogućnost pretraživanja finansijskih izveštaja i drugih informacija na veb-sajtu, mogućnost preuzimanja i štampanja izveštaja i slično. Istraživanja dostupnosti obično se zasnivaju na metodologiji koja obuhvata ispitivanje standardnog seta od deset obeležja [6]. Vrednost komponente dostupnosti računa se prema istom principu kao i vrednost sadržaja. Prema tome, dostupnost se može iskazati putem sledeće formule:

$$\text{Dostupnost} = \frac{\sum_{i=1}^{10} Y_i}{10} \times 100$$

Gde je:

$Y_i$  – obeležja dostupnosti

#### 4. METODOLOGIJA ISTRAŽIVANJA I OPIS UZORKA

Osnovni cilj rada jeste da se istraži kvalitet finansijskog izveštavanja na veb-sajtovima gradova i opština kao entiteta javnog sektora u Republici Srbiji. Istraživanje kvaliteta finansijskog izveštavanja sprovedeno je prema sledećim fazama:

- Ocena nivoa kvaliteta finansijskog izveštavanja gradova i opština na veb-sajtu.
- Ispitivanje značajnosti razlika u ocenama kvaliteta finansijskog izveštavanja između gradova i opština na veb-sajtu.

Ocena kvaliteta finansijskog izveštavanja gradova i opština na internetu merena je putem dva pokazatelja: sadržaja i dostupnosti. U cilju ispitivanja da li postoje razlike u nivou kvaliteta finansijskog izveštavanja na veb-sajtu između gradova i opština u Republici Srbiji postavljene su sledeće hipoteze:

$H_1$ : Ne postoji statistički značajna razlika u kvalitetu finansijskog izveštavanja na veb-sajtu između gradova i opština u Republici Srbiji sa aspekta sadržaja.

$H_2$ : Ne postoji statistički značajna razlika u kvalitetu finansijskog izveštavanja na veb-sajtu između gradova i opština u Republici Srbiji sa aspekta dostupnosti.

U cilju testiranja navedenih hipoteza korišćen je statistički test Student t-test koji ispituje postojanje razlika u aritmetičkim sredinama između dve grupe [4]. Podaci su analizirani u statističkom softveru SPSS v.23.

Za potrebu istraživanja korišćen je slučajni uzorak od 32 entiteta javnog sektora, odnosno 12 gradova i 20 opština. Istraživanje je sprovedeno u poslednjem kvartalu 2017. godine. Fokus istraživanja predstavlja obelodanjivanje finansijskih izveštaja za 2016. godinu kao i obelodanjivanje drugih relevantnih informacija za poslovno odlučivanje eksternih korisnika.

#### 5. REZULTATI ISTRAŽIVANJA

Rezultati analize postojanja veb-sajta ukazuju da svi gradovi i opštine u Republici Srbiji uzeti u uzorak imaju zvaničnu veb-sajt prezentaciju. Dalji rezultati kvaliteta izveštavanja gradova i opština na veb-sajtovima sa aspekta sadržaja su prikazani u sledećoj tabeli:

Tabela 1. Rezultati istraživanja kvaliteta finansijskog izveštavanja gradova i opština u Republici Srbiji sa aspekta sadržaja na veb-sajtu

Obeležja sadržaja	Gradovi	Opštine
Finansijski izveštaj	93%	90%
Izveštaj revizora	85%	70%
Izvršenje budžeta na kvartalnom ili mesečnom nivou	85%	55%
Budžet	92%	95%
Rebalansi	92%	95%
Objašnjenje velikih odstupanja	0%	5%
Izveštaj o korišćenju sredstava rezervi	15%	5%
Izveštaj o garancijama	0%	0%
Pregled primljenih donacija i kredita	15%	10%
Informacije za investitore	100%	95%
Informator o radu	100%	85%
Javne nabavke	100%	90%
Organizaciona struktura	100%	85%
<b>Prosečna ocena sadržaj</b>	<b>68%</b>	<b>59%</b>
<b>Minimalna ocena sadržaja</b>	<b>38%</b>	<b>31%</b>
<b>Maksimalna ocena sadržaja</b>	<b>78%</b>	<b>69%</b>

Analiza kvaliteta finansijskog izveštavanja sa aspekta sadržaja ukazuje da gradovi u proseku imaju bolji kvalitet izveštavanja na veb-sajtu. Gradovi u Republici Srbiji u



proseku obelodanjuju veći obim informacija koji je od interesa pre svega za eksterne korisnike, u odnosu na opštine. Značajna razlika u obelodanjivanju ogleda se kod izveštaja revizora i izveštaja o izvršenju budžeta na kvartalnom ili mesečnom nivou. Gradovi u 80% slučajeva obelodanjuju revizorski izveštaj, dok u proseku svaka treća opština nema obelodanjen revizorski izveštaj. Neobelodanjivanje revizorskog izveštaja, kao ključne informacione podrške u procesu poslovnog odlučivanja, značajno umanjuje kvalitet finansijskog izveštavanja. Dalje, primetno je da gradovi i opštine koriste sredstva rezervi, pre svega sredstva tekuće rezerve, ali izveštaje obelodanjuju na veb-sajtu u svega 15% na nivou gradova, odnosno 5% na nivou opština. Analiza malog broja obelodanjivanja izveštaja o garancijama, objašnjenja velikih odstupanja, pregleda primljenih donacija i kredita i izveštaja o garancijama treba da bude usmerena na ispitivanje da li su se navedene transakcije kod gradova i opština realizovale. Kvalitet obelodanjivanja dodatnih informacija kao što su informator o radu, javne nabavke, organizaciona struktura i informacije za investitore je visok, posebno na nivou gradova.

Rezultati analize kvaliteta sa aspekta komponente dostupnosti su prikazani u narednoj tabeli.

Tabela 2. Rezultati istraživanja kvaliteta finansijskog izveštavanja gradova i opština u Republici Srbiji sa aspekta dostupnosti na veb-sajtu

Obeležja dostupnosti	Gradovi	Opštine
Veb-sajt na prvoj stranici pretraživača	100%	100%
Na naslovnoj stranici veb-sajta postoji link za finansijske izveštaje	14%	5%
Pretraga finansijskih izveštaja	92%	85%
Dostupnost izveštaja do 3 veb stranice	23%	5%
Pdf format	100%	100%
Individualni elementi finansijskih izveštaja	7%	5%
Individualni elementi finansijskih izveštaja do 3MB	7%	5%
Štampanje	100%	100%
Finansijski izveštaji za prethodnu godinu	69%	90%
Kontakt	100%	10%
<b>Prosečna ocena dostupnosti</b>	<b>60%</b>	<b>58%</b>
<b>Minimalna ocena</b>	<b>40%</b>	<b>40%</b>
<b>Maksimalna ocena</b>	<b>100%</b>	<b>75%</b>

Rezultati analize dostupnosti finansijskih i drugih informacija na veb-sajtu gradova i opština ukazuje na izuzetno visok kvalitet sa aspekta pretrage finansijskih izveštaja, preuzimanja, štampanja, kontakt informacija i pronalazjenja veb-sajta na prvoj stranici pretraživača (google i yahoo). Veoma mali broj gradova i opština ima na naslovnoj stranici veb-sajta link za informacije o

finansijskim izveštajima. Prilikom pretraživanja finansijskih izveštaja, budžeta i drugih informacija u velikom broju slučajeva potrebno je više od 3 koraka u pretraživanju. Takođe, uočeno je da se finansijski i drugi izveštaji nalaze u različitim segmentima veb-sajta kao što su segmenti „o nama“, „dokumenta“, „informacije o radu“ i sl. Takođe, analiza dostupnosti je ukazala da se finansijski izveštaj u najvećem broju slučajeva obelodanjuje kao jedinstveni dokument, dok pojedinačni elementi finansijskog izveštaja na veb-sajtu gradova se obelodanjuju u svega 7% slučajeva, odnosno 5% na nivou opština. U cilju lakše pretrage informacija od strane korisnika izveštaja poželjno je da elementi finansijskog izveštaja budu obelodanjeni kao posebna dokumenta na veb-sajtu gradova i opština.

Analiza kvaliteta finansijskog izveštavanja ukazuje da gradovi u Republici Srbiji imaju bolji kvalitet izveštavanja na veb-sajtovima i sa aspekta sadržaja i dostupnosti. Kako bi se dao odgovor na pitanje da li su razlike u nivou kvaliteta izveštavanja između gradova i opštine značajne sproveden je t test. Rezultati sprovedenog t testa prikazani su u narednoj tabeli.

Tabela 3. Rezultati t test-a

Kvalitet	Levinov test jednakosti varijansi		t test		
	F	p	t	df	p
Ocena sadržaja	0,521	0,476	2,251	31	0,032
Ocena dostupnosti	1,657	0,208	0,578	31	0,567

Dobijena vrednost  $p=0,032$  je manja od granične vrednosti (0,05) i ukazuje da su razlike u kvalitetu finansijskog izveštavanja između gradova i opština u Republici Srbiji sa aspekta sadržaja značajne. Prema tome hipoteza  $H_1$  se odbacuje i prihvata se alternativna hipoteza. Dakle, zaključuje se da je kvalitet finansijskog izveštavanja gradova na veb-sajtovima sa aspekta sadržaja na značajno boljem nivou od kvaliteta izveštavanja na nivou veb-sajtova opština.

Dobijena vrednost  $p=0,567$  je veća od granične vrednosti (0,05) i ukazuje da razlike u kvalitetu izveštavanja gradova i opština na veb-sajtu sa aspekta dostupnosti nisu značajne. Prema tome prihvata se hipoteza  $H_2$  i zaključuje se da je kvalitet sa aspekta dostupnosti informacija o poslovanju gradova i opština preko veb-sajtova na relativno istom nivou.

## 6. ZAKLJUČAK

Obezbeđivanje kvalitetnog sistema finansijskog izveštavanja na nivou gradova i opština od izuzetnog je značaja za korisnike informacija o poslovanju navedenih entiteta javnog sektora u procesu poslovnog odlučivanja, a time i za razvoj gradova i opština. Kvalitetan sistem finansijskog izveštavanja treba da obezbedi potpune informacije o poslovanju gradova i opština kao entiteta

javnog sektora i da pruži informacije blagovremeno. Kao rešenje za obezbeđivanje kvalitetnog sistema finansijskog izveštavanja ističe se obelodanjivanje informacija o poslovanju na veb-sajtu gradova i opština. U cilju privlačenja investicija gradovi i opštine treba da obezbede potpunu i lako dostupnu informacionu osnovu potencijalnim i postojećim investitorima. Prema tome neophodno je na veb-sajtu gradova i opština obelodaniti ne samo informacije iz finansijskih izveštaja i izveštaja revizora, nego i druge informacije za poslovno odlučivanje kao što su budžet, rebalansi, informacije za investitore, izveštaje o korišćenju sredstva rezervi i dr. Takođe, neophodno je sve izveštaje o poslovanju postaviti blagovremeno na veb-sajt gradova i opština kako bi informacije bile relevantne za poslovno odlučivanje.

Rezultati istraživanja kvaliteta finansijskog izveštavanja gradova i opština sa aspekta sadržaja odbacuju hipotezu  $H_1$  i ukazuju da gradovi u Republici Srbiji imaju bolji kvalitet, odnosno da obelodanjuju više informacija o poslovanju na veb-sajtu. Gradovi u 93%, a opštine u 90% slučajeva obelodanjuju finansijski izveštaj za prethodnu godinu, što ukazuje na visoki kvalitet i blagovremenost obelodanjivanja. Kao kritična područja obelodanjivanja sa aspekta sadržaja kod opština ističe se obelodanjivanje izveštaja revizora, jer u proseku kod svake treće opštine finansijski izveštaj koji je obelodanjen nije praćen eksternom potvrdom, odnosno izveštajem revizora. Na osnovu rezultata istraživanja može se reći da u proseku svaka druga opština obelodanjuje informacije o kvartalnom ili mesečnom izvršenju budžeta, što takođe predstavlja jedno od kritičnih područja koje je potrebno unaprediti.

Sa aspekta dostupnosti rezultati istraživanja potvrđuju hipotezu  $H_2$  i ukazuju da ne postoje značajne razlike u kvalitetu obelodanjivanja informacija na veb-sajtu između gradova i opština. Visoki kvalitet se pripisuje dostupnosti veb-sajta gradova i opština na prvoj stranici pretraživača i mogućnosti pretraživanja finansijskog izveštaja na veb-sajtu. Kao kritična područja sa aspekta dostupnosti ističe se pre svega nepostojanje elemenata finansijskog izveštaja kao posebnih dokumenata, što otežava pronalazjenje informacija u jednom relativno obimnom dokumentu. Dalje, pretraživanje informacija o poslovanju na veb-sajtu traje relativno duži vremenski period, jer link za finansijske izveštaje na naslovnoj strani veb-sajta je prisutan kod 14% veb-sajtova gradova i svega 5% veb-sajtova opština. Takođe, pronalazak traženih informacija o poslovanju gradova i opština na većini veb-sajtova zahteva pretraživanje više od 3 stranice na veb-sajtu.

Kao polazna preporuka za obezbeđivanjem kvalitetnog finansijskog izveštavanja gradova i opština na veb-sajtu ističe se prevazilaženje i unapređenje kritičnih područja koja su identifikovana kroz rezultate sprovedenog istraživanja. Takođe, kao preporuka ističe se i formiranje jedinstvene javno dostupne baze informacija o poslovanju entiteta javnog sektora. Unapređenje kvaliteta izveštavanja i na nivou veb-sajta gradova i opština i na nivou jedinstvene baze obezbeđuje adekvatnu informacionu podršku potencijalnim i postojećim domaćim i stranim

investitorima i drugim zainteresovanim stranama, što će indirektno uticati i na razvoj gradova i opština.

## LITERATURA

- [1] Basuony, M. and Mohamed, E. "Determinants of Internet Financial Disclosure in GCC Countries", *Asian Journal of Finance & Accounting*, Vol. 6, No. 1, pp 70-89, 2014.
- [2] Dimitrijević, D., Tasić, S., Tasić, Z., Janković, M., Andrejević, D. "The Impact of Digital Literacy on the Performance and Productivity of Employees", *Zbornik radova, YUINFO2017*, str. 6-12. Beograd, 2017
- [3] Dolinšek, T., Tominc, P. and Skerbinjek, A. L. "The Determinants of Internet Financial Reporting in Slovenia", *Online Information Review*, Vol. 38, No. 7, pp 842-860, 2014.
- [4] Field, A., *Discovering statistics using SPSS*, England: Sage Publication, 2009.
- [5] Financial Accounting Standard Board, *Electronic distribution of business reporting information: business reporting research project*, USA: FASB, 2000.
- [6] Groff, J.E., Pitman, M.K. "Municipal Financial Reporting on the World Wide Web: A Survey of Financial Data Displayed on the Official Websites of the 100 Largest U.S. Municipalities." *Journal of Government Financial Management*, Vol. 53, No. 2, 20-30, 2004.
- [7] Jović, D. "Finansijsko izveštavanje i vrednovanje performansi entiteta javnog sektora" doktorska disertacija, Beograd, 2016.
- [8] Laswad, F., Fisher, R., Oyelere, P. "Determinants of Voluntary Internet Financial Reporting by Local Government Authorities", *Journal of Accounting and Public Policy*, No. 24, pp. 101-121, 2005
- [9] Mijić, K. "The Quality and Determinants of Internet Financial Reporting in Serbia", *Zbornik radova, YUINFO2017*, str. 23-28. Beograd, 2017.
- [10] Sl. glasnik RS", br. 125/03 i 12/06, "Uredba o budžetskom računovodstvu", Beograd, 2006.
- [11] Sl. glasnik RS, br. 18/2015, "Pravilnik o načinu pripreme, sastavljanja i podnošenja finansijskih izveštaja korisnika budžetskih sredstava, korisnika sredstava organizacija za obavezno socijalno osiguranje i budžetskih fondova", Beograd, 2015.
- [12] Sl. glasnik RS" br. 113/2017, "Zakon o budžetskom sistemu", Beograd, 2017.
- [13] Styles, A., Tennyson, M. "The Accessibility of Financial Reporting of U.S. Municipalities on the Internet", *Journal of Public Budgeting, Accounting & Financial Management*, Vol. 19, No. 1, pp.56-92, 2007.
- [14] Varewaty, "The Comparative Analysis of Accessibility Index Value of Government Internet Financial Reporting in Indonesia", *Applied Finance and Accounting*, Vol. 2, No. 2, pp. 2374-2429, 2016.

# NEKE OD PRIMENA BESPILOTNIH LETELICA U ŠUMARSTVU I ZAŠTITI ŽIVOTNE SREDINE

## SOME OF THE APPLICATIONS OF UNMANNED AERIAL VEHICLES (UAV) IN FORESTRY AND ENVIRONMENTAL PROTECTION

Dejan Pavlović, dipl. inž. el.<sup>1</sup>  
JP „Nacionalni park Đerdap“<sup>41</sup>

**Sadržaj** – Upotreba bespilotnih letelica poslednjih godina sve je češća usled razvoja tehnologije, smanjenja cene proizvodnje samih letelica, kao i samog razvoja i minijaturizacije korisne opreme koju mogu da nose. Često se koriste za monitoring oblasti od interesa, fotografisanje tj. snimanje terena, izradu 3D modela i ostale primene. U ovom radu pažnja će biti posvećena na primeni bespilotnih letelica (malih dronova) u šumarstvu i zaštiti životne sredine, opremi koju nose i biće objašnjeni neki od realizovanih tj. već primenjenih sistema u praksi kao i mogućnosti primene istih ili sličnih - modifikovanih sistema za potrebe monitoringa i zaštite šuma u našoj zemlji.

**Abstract** - The use of unmanned aerial vehicles - UAV, in recent years is increasingly more frequent due to the development of technology, reduction in the cost of UAV manufacturing and also of the development and miniaturization of useful equipment they can carry. They are very often used for monitoring areas of interest, taking pictures, recording of the terrains, creating 3D models and for the other applications. In this paper, attention will be given to the use of unmanned aerial vehicles (small drones) in forestry and environmental protection, equipment they can carry, and also will be explained some of the realized, i.e. already implemented systems in practice, as well as the possibility of using the same, or similar - modified systems for the purpose of monitoring and protecting forests in our country.

### 1. UVOD

U početku su se bespilotne letelice koristile isključivo u vojne svrhe, ali korišćenjem tehnologije kao što je GPS značajnu primenu postižu i u civilne svrhe, a naročito za mapiranje, monitoring (osmatranje) i upravljanje staništima i prirodnim resursima. Postojeći tipovi bespilotnih letelica mogu se klasifikovati na osnovu raznih kriterijuma. Prema [1] klasifikuju se na osnovu veličine i nosivosti korisnog tereta, kontrolnog sistema i opsega leta (visine i dužine trajanja leta). Bespilotne letelice se takođe prema [1,2] mogu svrstati i u jednu od četiri kategorije u zavisnosti od dizajna (oblika letelice) i režima leta na:

- 1) Balone, zmajeve i paraglajdere,
- 2) Letelice sa rotirajućim krilima (bespilotni helikopteri i multikopteri),
- 3) Letelice sa nagibnim krilima i

#### 4) Letelice sa fiksnim krilima

Takođe na osnovu [3] mogu se podeliti: *prema veličini* (velike, srednje, male, mini, mikro i nano), *prema visini i dužini trajanja leta* (kratkog trajanja leta na malim visinama – LASE, dugog trajanja leta na malim visinama – LALE, dugog trajanja leta na srednjim visinama – MALE i dugog trajanja leta na velikim visinama – HALE), *nameni* (kao mamci, za izviđanje, za borbu, za razvoj i istraživanje kao i na civilnu ili komercijalnu upotrebu), *po načinu poletanja i sletanja* (horizontalno poletanje i sletanje kao i vertikalno poletanje i sletanje). Za horizontalno poletanje i sletanje su karakteristične letelice sa fiksnim krilima – *avioni*, dok se za vertikalno poletanje i sletanje koriste letelice sa pokretnim krilima – *multikopteri* (*helikopteri, kvadrokopteri, optokopteri itd.*), kao i letelice sa nagibnim krilima. Slikom 1. prikazani su neki od tipova bespilotnih letelica (malih dronova).



Slika 1. Gore levo prikazana je letelica sa fiksnim krilima, gore desno letelica sa nagibnim krilima, dole levo letelica sa rotirajućim krilima (bespilotni helikopter) i dole desno letelica sa rotirajućim krilima (kvadrokopter) [2]

Za pokretanje bespilotnih letelica u civilne svrhe danas se koriste ekološki elektromotori i motori sa unutrašnjim sagorevanjem. Ekološki elektromotori ne zagađuju životnu sredinu i ne proizvode puno buke tokom svog rada. Ovo je naročito važno ako se bespilotne letelice koriste u gusto naseljenim mestima ili zaštićenim sredinama gde bi buka motora mogla uznemiriti životinje ili ptice. Zamena baterije je relativno jeftina, ali težina same baterije znatno utiče na dužinu tj. trajanje leta letelice.

Bespilotne letelice sa motorima sa unutrašnjim sagorevanjem imaju znatno duži opseg leta koji se može

jednostavno povećati povećanjem rezervoara za gorivo. Problem je u tome što ovakvi tipovi motora stvaraju buku i zagađuju okolinu. Danas se razvijaju i letelice sa hibridnim tipom pogona – elektromotorima i motorom sa unutrašnjim sagorevanjem. Motor sa unutrašnjim sagorevanjem se koristi za let na daljinu, dok se elektromotori koriste za poletanje i sletanje i za rad u sredinama gde se zahteva tišina.

## 2. PREDNOSTI I NEDOSTACI TIPOVA BESPILOTNIH LETELICA

Svaki od tipova bespilotnih letelica (malih dronova) imaju svoje prednosti i nedostatke u odnosu jedni na druge, a koji tip će se koristiti isključivo zavisi od namene. Prednosti i nedostaci pojedinih tipova su prema [2] dati tabelom 1:

Tabela 1.

Tip drona	Prednosti	Nedostaci
Sa fiksnim krilima	- Veliki opseg leta - Izdržljivost	- Horizontalno poletanje i sletanje - Zahtevaju prostor za poletanje i sletanje kao i za održavanje (neki zahtevaju katapult)
Sa nagibnim krilima	- Kombinacija fiksnih krila i prednosti vertikalnog poletanja i sletanja	- Tehnološki kompleksni - Skupi
Sa rotirajućim krilima (bespilotni helikopteri)	- Vertikalno poletanje i sletanje - Manevarska sposobnost - Mogućnost velike nosivosti korisnog tereta	- Skupi - Visoki zahtevi za održavanjem
Sa rotirajućim krilima (multikopteri)	- Jeftini - Jednostavni za pokretanje - Laki	- Ograničena težina korisnog tereta - Osetljivi na vetar zbog male težine

Većina bespilotnih letelica (malih dronova) koje se danas koriste za potrebe ekologije imaju malu korisnu nosivost, pokrivaju manja rastojanja (imaju kraći domet leta) i lete na nižim visinama.

## 3. PRIMENA MALIH DRONOVA U ŠUMARSTVU

Korišćenje malih dronova u šumarstvu danas je široko rasprostranjeno u svetu. Imaju primenu kao aerofotogrametrijski sistemi, kao sistemi za monitoring šumskih zajednica - staništa, a koriste se i za praćenje i predikciju širenja šumskih požara. Jedna od najvećih prednosti ovakvih sistema je visoka fleksibilnost i

relativno niski operativni troškovi. Takođe, povećana je pouzdanost navigacionih sistema letelica i izvršena značajna minijaturizacija senzora koji se koriste.

*Baloni, zmajevi i paraglajderi* za monitoring šumskih zajednica (šumskih staništa ili šumskih ekosistema) nisu pogodni jer se ovakvim tipovima letelica teško pokrivaju velike površine. Ovakav tip letelice je najbolje koristiti za lokalni monitoring npr. za primenu konstantnog protivpožarnog nadzora. Mali dronovi *sa rotirajućim krilima* kao što su helikopteri i multikopteri (kvadrokopteri, oktokopteri) nisu pogodni za monitoring šumskih zajednica jer mogu da pokriju kraća rastojanja sa kraćom dužinom trajanja leta (tipično 30-40 minuta). Međutim, ovakvi tipovi dronova su pogodniji za primenu monitoringa šumskih zajednica u odnosu na male dronove sa fiksnim krilima u onim šumskim oblastima gde su krošnje drveća velike i guste, te je vertikalno poletanje i sletanje letelica sa rotirajućim krilima znatno pogodnije nego poletanje i sletanje sa fiksnim krilima. Bespilotne letelice *sa fiksnim krilima* imaju mogućnost jedrenja tako da imaju znatno veći domet (trajanje) leta nego letelice sa rotirajućim krilima i pokrivaju znatno veće oblasti (domet leta 15-20 km). Zbog ove svoje osobine imaju veliku primenu u monitoringu šumskih zajednica tropskih šuma. Štaviše, većina letelica sa fiksnim krilima se može realizovati korišćenjem delova jeftinijih modela aviona hobi namene, pri čemu se značajno smanjuje cena izgradnje, dok sposobnost jedrenja letelica omogućava nošenje veće mase korisnog tereta. Ovo praktično znači da se ovakav tip letelica može opremiti većim brojem različitih tipova senzora, kamera ili drugom korisnom opremom nego letelice sa rotirajućim krilima [1].

## 4. KORIŠĆENJE SENZORA, SKENERA I KAMERA KAO KORISNOG TERETA

Oprema neophodna za modeliranje, mapiranje i monitoring vegetacije uglavnom se sastoji od senzora za snimanje u kombinaciji sa GPS-om i inercijalno-navigacionim sistemom (INS) [4]. Postojeća tehnologija omogućava korišćenje senzora veoma visoke rezolucije i male težine po povoljnoj ceni. Senzori se dele na *pasivne* koji koriste spoljašnji izvor svetlosti kao npr. sunčevu svetlost neophodnu za posmatranje cilja, i na *aktivne* senzore koji koriste sopstvene izvore svetlosti za osvetljavanje cilja – predmeta, tako da se energija svetlosti koja se reflektuje može meriti.

LiDAR je aktivni optički senzor (skener) koji šalje veliki broj laserskih svetlosnih impulsa po jedinici vremena prema ciljanoj meti - predmetu. Vreme od emitovanja svetlosnog impulsa pa do povratka na senzor sistema nakon refleksije od predmeta se meri da bi se izračunalo rastojanje. Udaljenost se zatim kombinuje sa informacijama o poziciji letelice korišćenjem GPS-a i INS-a kako bi se generisala visoko precizna georeferencirana tačka. Na bespilotnim letelicama često se koristi *Ibeo LUKS LiDAR* sistem. Karakteristike ovog sistema su maksimalni opeg od 200 metara, maksimalni opeg skeniranja 110° sa korekcijom  $\pm 30^\circ$ , rezolucijom 4 cm, ugaonom rezolucijom 0,25 cm i težinom od 1 kg.

Neke od primena LiDAR sistema u šumarstvu su [5]:

- *Upravljanje i planiranje u šumarstvu* – koristi se za merenje vertikalne strukture krošnje stabla (gustine i visine krošnje od baze stabla) kao i za merenje visine stabla da bi se procenila ekspanzija korena;
- *Monitoring šumskih požara* – LiDAR omogućava praćenje moguće zone požara tzv. modelom mapiranja goriva, odnosno „modelom ponašanja požara“;
- *Precizno šumarstvo* – definiše se kao planiranje i upravljanje specifičnim šumskim područjem kako bi se povećao kvalitet drveta, smanjili troškovi proizvodnje, povećao profit i zadržao kvalitet životne sredine. LiDAR se u kombinaciji sa fotografijama iz vazduha koristi za realizaciju preciznog šumarstva.

Primene LiDAR sistema za zaštitu životne sredine [5]:

- *Turizam i upravljanje parkovima* – obzirom da je upravljanje parkovima složen posao, LiDAR tehnologija igra ključnu ulogu kao ispodom pri upravljanju. Koristi se za planiranje upravljanja turističkim područjima i područjima parkova. Visoko precizan 3D model površine tla pomaže u pronalaženju odgovarajućih oblasti, a posebno je pogodan kao ispodom pri trasiranju pešačkih staza. 3D model parka tj. model zaštićenog područja korišćenjem LiDAR tehnologije značajno pomaže u budućem razvoju i očuvanju zaštićenog područja;
- *Procena u zaštiti životne sredine* – podaci sa mikro topografija korišćenjem LiDAR sistema koriste se za procenu zaštite životne sredine. Ova procena se prvenstveno koristi radi zaštite biljnog i životinjskog sveta, a takođe se koristi i za identifikovanje ugroženih područja usled ljudskih aktivnosti;
- *Očuvanje biodiverziteta ptica* – šume su staništa različitih vrsta ptica, životinja i insekata. Na osnovu podataka LiDAR sistema vrši se analiza šumskih ekosistema (vertikalna struktura) da bi se utvrdilo da li su pogodno mesto za život pojedinih vrsta. Vertikalna struktura drveća, grmlja i drugih biljaka govore o vrsti ptica koja može živeti i opstati na određenom području;
- *Izrada modela poplava* – LiDAR pruža veoma precizne podatke. Koristi se za generisanje površinskog modela reka u visokoj rezoluciji. Ovi modeli se mogu koristiti za bolje planiranje izgradnje objekata na obalama reka;
- *Mapiranje vodotokova* – LiDAR se koristi za generisanje modela područja slivova i razdvajanje linija vodotokova. Na ovaj način se može izračunati vodostaj određenih vodotokova ili kanala ispunjenih vodom;
- *Ekološka klasifikacija zemljišta* – vrši se da bi se obezbedile biološke i fizičke informacije oblasti u cilju održivog upravljanja. Omogućava planiranje korišćenja zemljišta, uravljanje šumama, upravljanje staništima, proceni životne sredine i još mnogo toga. Tokom klasifikacije zemljišta podaci visoke rezolucije dobijeni

pomoću LiDAR sistema pomažu u razumevanju prirode i vrste zemljišta;

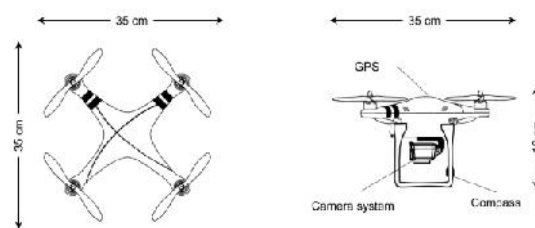
- *Izrada modela zagađenosti* – opseg talasnih dužina koji koristi LiDAR sistem kreće se od ultraljubičastog preko vidljivog pa sve do infracrvenog elektromagnetnog spektra. Pomoću LiDAR-a je moguće otkriti zagađujuće čestice kao što su čestice ugljen-dioksida, sumpordioksida ili metana. Ove informacije omogućavaju generisanje mapa gustine zagađenja pojedinih područja u cilju boljeg upravljanja;
- *Mapiranje* – Model kreiran pomoću LiDAR sistema koristi se za dodavanje grafičke komponente mapama. U kombinaciji sa aerofotografijama koristi se za dobijanje 3D modela koji olakšava planiranje izgradnje puteva, mostova ili drugih objekata.

Od nedavno su u upotrebi relativno jeftine mikro-hiper spektralne kamere male težine i koje su mali potrošači energije. Hiperspektralni senzor slike koristi na stotine susjednih spektralnih kanala u širem spektralnom opsegu. Često je u upotrebi mikro-hiperspektralna kamera *Micro-Hyperspec VNIR* koja koristi 260 susjednih kanala spektralnog opsega od 400-1000 nm i koja je težine 450g.

Od pasivne opreme koriste se optičke RGB kamere visoke rezolucije.

## 5. MONITORING ŠUMSKIH EKOSISTEMA I ZAŠTIĆENIH PODRUČJA

U radu [6] opisana je realizacija sistema za monitoring zaštićenog rečnog šumskog ekosistema Atlantskih šuma oblasti Rio de Žaneira. Korišćen je kvadrokopter *DJI Phantom Vision 2+* (prikazan slikom 2) i opremljen optičkom RGB kamerom visoke rezolucije.



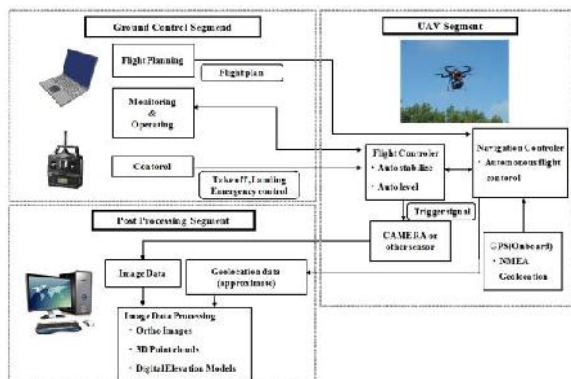
Slika 2. DJI Phantom Vision 2+

Težina ovog modela je 1,2 kg i može se jednostavno transportovati korišćenjem ranca. Može da izvodi kraće letove trajanja do 25 minuta na visinama do 300 metara. Takođe poseduje sistem za stabilizaciju RGB kamere rezolucije 14 mega piksela (4383x3288) i prostorne rezolucije manje od 3 cm po pikselu. Osim toga, upravljanje ovim dronom moguće je na udaljenosti od 500 do 700 metara i kompatibilan je sa mobilnim uređajima koji koriste iOS ili Android operativni sistem.

Svaka misija pažljivo je programirana uzimajući u obzir prisustvo visokog drveća, planina, kuća, električnih kablova, a takođe se vodilo računa i o atmosferskim uslovima kao što su kiša i brzina vetra. Nadgledanje

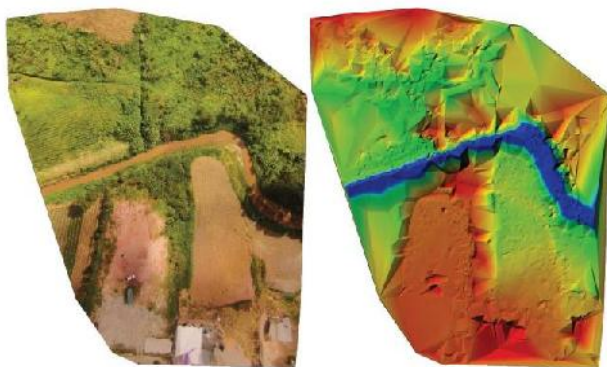


terena vršeno je uz dozvolu za izvođenje letova i obezbeđeni su preduslovi kako se ne bi nanela šteta trećim licima. Sistem je prikazan slikom 3.



Slika 3.

Nakon prikupljanja fotografija korišćen je softver za generisanje ortomozaika – za izradu DSM (*Digital Surface Models*) i DTM (*Digital Terrain Models*) modela. Tokom obrade izvršena je i korekcija tzv. „ribljeg-oka“ efekta na fotografijama koji inače utiče na realne dimenzije predmeta. Ovako korigovane fotografije konvertovane su u ortofotografije. Ortofotografija je geometrijski korigovana na taj način da može da prikaže realne dimenzije (širinu, visinu i dužinu) predmeta. Slikom 4. prikazan je orto-foto i DSM model fotografije.



Slika 4. Levo – orto-foto model, desno – DSM model

Korišćenjem *DJI Phantom Vision 2+* malog drona opremljenog kamerom visoke rezolucije (manje od 3 cm po pikselu) moguće je generisati veoma precizne mape tj. modele različitog formata u zavisnosti od vrste analize koja se zahteva (ortomozaik ili DSM), čineći ovakav tip letelice potencijalnim alatom za potrebe monitoringa životne sredine. Smanjena je potreba za radnom snagom u slučajevima monitoringa velikih površina. Korišćeni kapacitet baterije omogućavao je u proseku let od 25 minuta na visini od 50 metara pri brzini vetra od 4 m/s. Nadgledana površina bila je u proseku 2 hektara. Vreme neophodno za obradu fotografija i odgovarajućeg digitalnog modela kretalo se od 30 do 60 minuta u zavisnosti od jačine korišćenog hardvera.

Radom [7] opisan je prenosni LiDAR sistem razvijen na *Univerzitetu Tasmanija*. Platforma se sastoji od multirotor bespilotne letelice (*OktoKopter Droidworx/MikroKopter*

*AD-8*) i senzorskog sistema *Ibeo LUX* težine oko 2.8 kg. Ova platforma može da leti od 3 do 4 minute što je dovoljno vremena da se snimi površina parcele unutar 100 metara od poletne tačke. Sistem je opremljen autopilotom koji omogućava predefinisani let radi efikasnijeg korišćenje vremena leta. Senzorski sistem je izolovan od vibracija koji proizvodi letelica korišćenjem četiri silikonska nosača. Koristan teret letelice sačinjen je od *POS sistema* – sistema za pozicioniranje i orijentaciju, laserskog skenera (*LiDAR-a*) i računara za prikupljanje i evidenciju podataka. POS sistem se sastoji od *inercijalno-navigacionog sistema (INS)* koji služi za manevrisanje letelicom, *dvofrekventnog GPS prijemnika* i *HD video kamere*. Velika brzina očitavanja podataka INS-a omogućena je fuzijom podataka o položaju (poziciji) letelice i njene brzine pomoću GPS-a. Orijehtacija kamere takođe omogućava visoku tačnost osmatranja. Za laserski skener (*LiDAR*) korišćen je *Ibeo LUX* skener.

## 6. MONITORING ŠUMSKIH POŽARA MALIM DRONOVIMA

Radom [8] opisan je sistem za detekciju i praćenje šumskih požara korišćenjem infracrvenih kamera i kamera u vidljivom delu spektra. Osmišljen je tako da ima mogućnost upravljanja flotom različitih bespilotnih letelica na koordinisani način radi nadgledanja postojećeg požara kao i mogućnost obrade podataka sa letelica u realnom vremenu kako bi se izvršila procena širenja vatre.

Sačinjavaju ga dva glavna sistema – *sistem percepcije* i *sistem odlučivanja*. Sistem percepcije vrši integraciju svih informacija dobijenih sa senzora bespilotnih letelica, dok sistem odlučivanja vrši planiranje zadatka, alociranje i koordinisanje rada svih letelica flote.

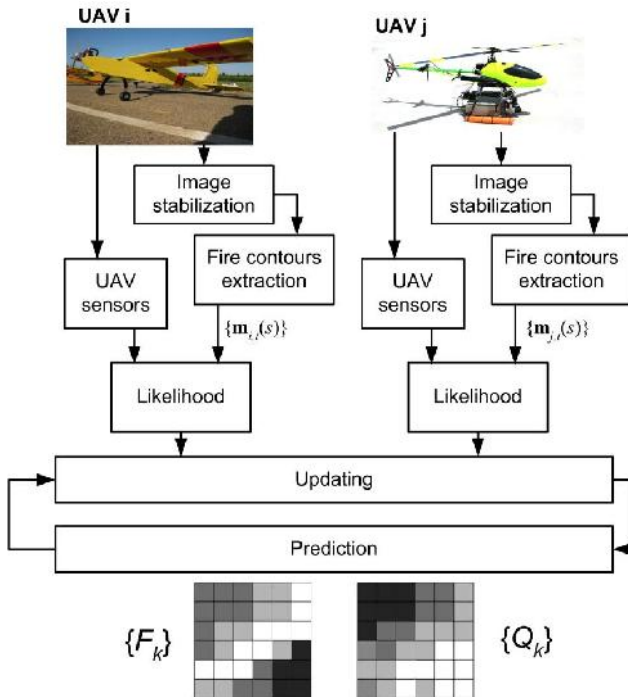
Operativni zahtevi letelica su sledeći:

- *Operativna autonomija* – da budu u stanju autonomnog leta po zadatim koordinatama i da mogu da pokriju oblast od interesa;
- *Lokalizacija* – da imaju mogućnost lokalizacije u istom referentnom okviru;
- *Korisna nosivost* – da imaju mogućnost nošenja infracrvenih ili optičkih RGB kamera.

Flota letelica testiranog sistema realizovana je od dva helikoptera i jednog balona. Sve letelice su opremljene GPS uređajima i inercijalnim mernim sistemima koji im omogućavaju da se lokalizuju u istom referentnom okviru. Takođe su sve letelice opremljene infracrvenim i optičkim RGB kamerama, a neke od njih su opremljene i pan/tilt uređajima. Pre leta vrši je kalibracija svih kamera. Sve letelice su opremljene komunikacionim uređajima pomoću kojih primaju komande sa zemaljskih stanica, a istovremeno i vraćaju korisne podatke ka njima.

*Sistem percepcije* obrađuje informacije prikupljene sa letelica i vrši procenu širenja požara primenjujući tehnike fuzije podataka. U sistemu prikazanim slikom 5. vidi se da svaka od letelica vrši obradu svoje slike i donosi procenu o širenju požara. U konkretnom slučaju vrši se procena verovatnoće nastanka požara kao i procena o

gorivu u svakoj od ćelija iz dve mreže. Sve informacije se šalju centralnoj stanici gde se vrši finalna procena uzimajući u obzir podatke sa svih letelica flote.



Slika 5.

Sistem odlučivanja – vrši četiri glavne funkcije:

- *Alokaciju (raspoređivanje) letelica*, - svaka od letelica treba da ima mogućnost izvršenja zadataka na osnovu specifičnog zahteva. Jedan od problema je određivanje koja od letelica treba da se pošalje na specifičnu lokaciju radi nadgledanja požara. Ova odluka može biti naročito zahtevna kada je svakoj od letelica već dodeljen određeni – prioritetni zadatak;
- *Planiranje zadataka* - glavni problem sistema odlučivanja. Osnovni cilj je definisati niz osnovnih zadataka koji se trebaju obaviti na takav način da se zadata misija realizuje na visokom nivou;
- *Koordinaciju* - predstavlja proces koji se javlja unutar sistema u kome se zahteva rad više različitih komponenti istovremeno. Konkretno u ovom slučaju, neophodnost obezbeđivanja dovoljnog prostora svakoj od letelica da izvrši bezbedno svoj plan leta u odnosu na planove leta ostalih letelica. Na primer, kod misija nadgledanja požara zahteva se kompletna pokrivenost zahvaćenog područja. Području kome je neophodno nadgledanje dodeljuju se dostupne letelice koje imaju optimalne mogućnosti u datom momentu (maksimalnu brzinu, autonomiju, vidno polje kamera itd.);
- *Nadzor* – bavi se upravljanjem (kontrolom) izvršenja zadataka.

## 7. PREDNOSTI I NEDOSTACI KORIŠĆENJA MALIH DRONOVA ZA REALIZACIJU MONITORINGA ŠUMSKIH EKOSISTEMA

Prema [1, 9] definišu se neke od prednosti i mana korišćenja dronova za realizaciju monitoringa šumskih ekosistema.

Prednosti korišćenja malih dronova su:

- *Ekstremno visoka prostorna rezolucija* - operativna visina korišćenja malih dronova kreće se između 50 i 300 metara koja omogućava dobijanje fotografija ekstremno visoke prostorne rezolucije (reda nekoliko santimetara po pikselu). Na ovaj način se povećava vizuelna analiza fotografija i značajno unapređuje monitoring. Na ovim rezolucijama specifična stabla i krošnje drveća se mogu jednostavno identifikovati i nadgledati;
- *Neosetljivost na pojavu oblačnosti* - mali dronovi tipično lete na visinama od 50 do 100 metara, što znači ispod visine oblaka omogućavajući na taj način značajnu prednost u odnosu na ostale konvencionalne daljinske platforme za nadgledanje;
- *Potencijal korišćenja 3D modela slika* - mali dronovi se sve češće koriste za dobijanje 3D modela površine zemlje. Ovakvi modeli značajno doprinose poboljšanju strategije monitoringa šumskih ekosistema – detekciju i kvantifikaciju šumskih degradacija kao i stanja procesa ponovnog rasta šuma. Takođe, mogućnost izrade veoma preciznih šumskih 3D modela pomaže u pronalaženju šumskih strukturalnih parametara kao što su visina, bazalna površina i gustina stabala. Na ovaj način se može proceniti ukupna šumska biomasa;
- *Relativno niska cena fotografija* - cena kupovine, operativnog rada i održavanja malih dronova je češće mnogo niža u odnosu na cenu iznajmljivanja komercijalnih pilotiranih letelica ili cene fotografija visoke rezolucije sa nekih od dostupnih satelitskih sistema kao što su IKONOS, QuickBird, RapidEye i sl;
- *Poboljšan monitoring ilegalnih aktivnosti* - ilegalna aktivnost kao što je npr. ilegalna seča šume može biti nadgledana ne samo upoređivanjem ranije snimljenih sa aktuelnim fotografijama, već i otkrivanjem tragova-staza koje vode ka lokacijama gde se seča odvija;
- *Lakši pristup teško pristupačnim oblastima (terenima)* - teško pristupačne oblasti kao što su udaljena područja, strme padine, kameniti tereni, močvare itd. mogu biti nadgledane malim dronovima. Ovo je korisno za nadgledanje šumskih zajednica manje gustine koje se prostiru na velikoj površini.

Nedostaci korišćenja malih dronova su:

- *Mala nosivost* - mali dronovi su u velikoj meri ograničeni količinom, težinom i veličinom korisnog tereta;
- *Lošije geometrijske i radiometrijske performanse* - obzirom da su mali dronovi mnogo lakši i da su manjih dimenzija nego senzorske platforme kao što su sateliti ili avioni, podložniji su uticaju raznih distorzija što može vrlo negativno da utiče na preciznost georeferenciranja. Češće korišćenje jeftinijih digitalnih kamera umesto profesionalnih senzora vodi do toga da loša geometrija fotografije proizvede netačne podatke. Ovakvi problemi mogu da utiču na konačan rezultat, a naročito su izraženi ako se zahteva visoka preciznost;
- *Osetljivost na atmosferske uslove* - mada mali dronovi mogu da lete dovoljno nisko da oblaci nemaju uticaja na njihov rad, ostali atmosferski uslovi kao što su magla, jaka kiša ili jak vetar promenljivog pravca mogu značajno



da utiču. Za dobijanje fotografija najboljeg kvaliteta brzina vetra treba da bude što je moguće manja i u zavisnosti od specifičnih modela dronova ne treba biti veća od 15-25 km/h;

- *Kratko trajanje leta* – ovo je potencijalno najznačajnije ograničenje obzirom da mala težina drona ograničava veličinu i težinu baterije koju dron može da nosi. Ipak, ne bi trebalo da bude glavno ograničenje za primenu monitoringa šuma, osim ukoliko nadgledana teritorija nije mnogo velika;

- *Mogućnost sudara* - mali dronovi obično nisu opremljeni sistemima za izbegavanje sudara, tako da je moguće doći do sudara tokom leta ukoliko ulazne koordinate nisu pravilno unete u sistem;

- *Reparacija i održavanje* - angažovanje stručne osobe za održavanje dronova ili pak slanje dronova ovlašćenom servisu u slučaju oštećenja može značajno povećati cenu leta drona. Ovo se može izbeći tehničkim poboljšanjima letelica ili osposobljavanjem lica koja će vršiti reparacije u slučajevima nezgoda.

- *Bezbedonosno-sigurnosni problemi* - upravljanje malim dronovima na potencijalno opasnim teritorijama odnosno teritorijama gde se odvija ilegalna seča šume, ilegalan lov ili naka druga ilegalna aktivnost može predstavljati bezbedonosni problem za operatora drona ili osoba koje vrše monitoring šuma.

## 8. POTENCIJALI KORIŠĆENJA MALIH DRONOVA U ŠUMARSTVU I ZAŠTIĆENIM PODRUČJIMA SRBIJE

Priroda Srbije odlikuje se izuzetno visokom raznovrsnošću biljnog i životinjskog sveta. Njeni najreprezentativniji delovi su i zakonom zaštićeni. Pod zaštitom se nalazi prema [10] 461 područje – 5 nacionalnih parkova, 18 parkova prirode, 20 predela izuzetnih odlika, 68 rezervata prirode, 3 zaštićena staništa, 310 spomenika prirode, 38 područja od izuzetnog kulturnog i istorijskog značaja. Većina ovih područja su izuzetno bogata šumama tako da je potencijal korišćenja malih dronova u cilju monitoringa i zaštite veliki.

Pravilnikom o bespilotnim vazduhoplovima [11] definisano je pod kakvim uslovima i na kojim lokacijama je moguće bezbedno upravljati bespilotnim vazduhoplovima na teritoriji Republike Srbije. Područje Nacionalnog parka Đerdap, izuzetno bogatog šumama predstavlja veliki potencijal za primenu ovakvih bespilotnih sistema.

## 9. ZAKLJUČAK

Poslednjih godina svedoci smo čestih i brojnih šumskih požara koji nastaju kako zbog klimatskih promena, tako i zbog ljudske nemarnosti. Korišćenje malih dronova radi nadgledanja šuma zahvaćenih požarima može imati neprocenljivu ulogu u smanjenju šteta koje tom prilikom nastaju. Takođe, mali dronovi imaju značajnu primenu i u turizmu, proceni i zaštiti životne sredine, očuvanju biodiverziteta ptica i drugih životinja, mapiranju vodotokova, ekoloških klasifikacija zemljišta, izradi modela zagađenosti sredine i mnogim drugim oblastima.

## LITERATURA

[1] Jaime Paneque-Gálvez, Michael K. McCall, Brian M. Napoletano, Serge A. Wich and Lian Pin Koh – „*Small Drones for Community-Based Forest Monitoring: An Assessment of Their Feasibility and Potential in Tropical Areas*“, *Forests* 2014, 5, 1481-1507; doi:10.3390/f5061481

[2] DHL Customer Solutions & Innovation Represented by Matthias Heutger, Senior Vice President Strategy, Marketing & Development, DHL CSI 53844 Troisdorf, Germany – „*Unmanned Aerial Vehicles In Logistics*“, A DHL perspective on implications and use cases for the logistics industry – 2014

[3] Lina Tang, „*Drone remote sensing for forestry research and practices*“ - *Journal of Forestry Research* - June 2015

[4] Esther Salamí, Cristina Barrado and Enric Pastor – „*UAV Flight Experiments Applied to the Remote Sensing of Vegetated Areas*“, *Remote Sens.* 2014, 6, 11051-11081; doi:10.3390/rs6111051

[5] <https://www.lidarusa.com/50-applications-for-lidar.html> [pristupljeno 09.01.2018.]

[6] Luis Antonio Esquivel Bustamante „*Forest Monitoring with Drones: Application Strategies for Protected Riverine Forest Ecosystems in the Atlantic Forest of Rio de Janeiro, Brazil*“, A thesis submitted in fulfillment of the requirements for the degree of Master of Science at the Institute for Technology and Resources Management in the Tropics and Subtropics, TH Köln – 2015

[7] L. O.Wallace, A. Lucieer and C. S.Watson – „*Assessing The Feasibility of UAV-Based LiDAR for High Resolution Forest Change Detection*“ - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XXXIX-B7, 2012 XXII ISPRS Congress, 25 August – 01 September 2012, Melbourne, Australia

[8] Luis Merino, Fernando Caballero, J. Ramiro Martínez-de-Dios, I. Maza and Aníbal Ollero – „*Automatic Forest Fire Monitoring and Measurement using Unmanned Aerial Vehicles*“ - VI International Conference on Forest Fire Research D. X. Viegas (Ed.), 2010

[9] <https://forestsnews.cifor.org/26586/unmanned-drones-forest-monitoring-redd?fnl=en> [pristupljeno 11.01.2018.]

[10] [http://www.zzps.rs/novo/index.php?jezik=sr&strana=zastita\\_prirode\\_osnovni\\_podaci](http://www.zzps.rs/novo/index.php?jezik=sr&strana=zastita_prirode_osnovni_podaci) [pristupljeno 17.01.2018.]

[11] [http://www.cad.gov.rs/docs/regulativa/Pravilnik%20o%20bespilotnim%20vazduhoplovima%20\(S1%20glasnik%20RS,%20broj%20108-15\).pdf](http://www.cad.gov.rs/docs/regulativa/Pravilnik%20o%20bespilotnim%20vazduhoplovima%20(S1%20glasnik%20RS,%20broj%20108-15).pdf) [pristupljeno 25.01.2018.]

# UPRAVLJANJE PROMENAMA U DINAMIČNOM OKRUŽENJU MANAGING CHANGES IN A DYNAMIC ENVIRONMENT

Miroslav Stefanović, Sanja Maksimović  
*Uprava za trezor*

**Sadržaj** – IT industrija je jedna od najmlađih. Kako vreme ide okruženje postaje sve dinamičnije. Tehnologije se brzo menjaju kao i podrška partnera, informacione tehnologije su sve zastupljenije u svim aspektima naših života, velika je fluktuacija ljudi. Sada imamo najviše informacija i najviše izazova.

Da bismo išli u korak sa promenama potrebno je da znamo šta želimo da ostvarimo ili koji cilj da postignemo. Što smo više svesni situacije u kojoj se nalazimo, resursa i znanja sa kojim raspoložemo definišemo korake za ostvarenje željenog rezultata. U tome nam pomaže iskustvo, preporuke iz oblasti ITIL®-a i dobro planiranje. U ovom radu predstavimo iskustvo Sektora za informacione tehnologije Uprave za trezor u sučeljavanju sa promenama.

**Abstract** - IT industry is one of the youngest. With time, our environment becomes more and more dynamic. Technologies are rapidly changing as well as partner support, information technology is increasingly represented in all aspects of our lives, the fluctuation of people is high. Now we have the most information and the most challenges.

In order to keep up with the changes, we need to know what we want to accomplish or what goal we want to achieve. The more we are aware of the situation we are in, resources and knowledge we possess, we define the steps for achieving the desired result. Our experience, guidelines from ITIL® publications and good planning are means to achieve this. Today, we will present what the IT Department of Treasury has done on this subject in the previous period.

## 1. UVOD

Uprava za trezor je deo Ministarstva finansija zadužena za poslove upravljanja gotovinskim sredstvima Republike, kontrole potrošnje budžetskih sredstava, budžetsko računovodstvo i izveštavanje, obrade ličnih primanja zaposlenih kod korisnika budžeta Republike i dr. Organizaciona struktura Uprave za trezor obuhvata osam sektora smeštenih u Centrali u Beogradu, 34 filijale i 109 ekspozitura širom Srbije. Sektor za informacione tehnologije je zadužen za pružanje usluga zaposlenima Uprave za trezor i ostalim korisnicima budžetskih sredstava.

## 2. PROMENE

Svakodnevno smo svedoci promena u našem okruženju. Ići u korak sa promenama predstavlja veliki izazov, kako za kompaniju, tako i za pojedinca. Primera ima dosta...



Slika 1. Uticaj klimatskih promena  
Promene klime su dovele do povećanja temperature i smanjenom obimu padavina tokom zime čime je snežni prekrivač dosta smanjen – što se može videti na slici.



Slika 2. Usklađenost sa klimatskim promenama  
Na slici možemo videti stazu prekrivenu snegom kao rezultat prilagođavanja klimatskim promenama – odnosno rad topova koji su napravili veštački sneg.

Primer iz ličnog iskustva:

Tehnika mi je od malih nogu bila zanimljiva. Sa pojavom računara otvorio mi se jedan svet koji se vremenom povećavao. Završio sam gimnaziju programerskog usmerenja, a kasnije Mašinski fakultet. Tokom školovanja sam dosta vremena provodio uz računar najviše kroz igrice. Prvi posao mi je bio u fabrici zupčanika. Posle 10 meseci sam prešao u IT struku.

Interesovanja koja imamo, odnosno ona bitna definišu naše živote i kreiraju nas. Za mene je to IT.

## 3. ORGANIZACIONE PROMENE

Razvojni put IT sektora Uprave za trezor je imao više faza. Posle primene mainframe-a prešli smo na Microsoft platformu. Naši developer-i su razvijali aplikacije. Broj korisničkih aplikacija je naglo porastao, odnosno, broj servisa koji se pružaju korisnicima. Funkcionalni zahtevi

klijenata su bili zadovoljeni, međutim, kvalitet rada i pružanja servisa je bio vrednovan na osnovu ličnih uverenja. Stekli smo utisak da nismo imali adekvatnu meru kvaliteta rada. Mislili smo da dobro radimo, ali nismo imali odgovarajuće parametre da to i potvrdimo. Shvatili smo da je potrebno nešto promeniti.

Unapređenje smo inicirali sa znanjem koje smo tada imali i koje se uglavnom svodilo na tehničko znanje. Optimizovali smo određene sistema i time smanjili vreme administracije. Kao rezultat pomenutih aktivnosti imali smo više vremena na raspolaganju. Organizovali smo edukacije za zaposlene.

Struktura SIT-a je tada bila većinom fakultetski obrazovnog kadra iz tehničkog usmerenja. Svi rukovodioci su prošli razvojni put od programera ili sistem inženjera do rukovodećih pozicija. Odnosno, nismo prošli edukacije za upravljanje.

Kada je organizacija rada IT-ja u pitanju, veoma su zastupljene preporuke iz prakse – ITIL® (Information Technology Infrastructure Library). Suština ITIL®-a je usaglašavanje usluga koje pruža IT sa potrebama biznisa. ITIL® prati celokupni životni ciklus IT usluge, od strategije, dizajna, tranzicije, operativnog funkcionisanja do kontinualnog unapređenja. U odnosu na hijerarhijsku organizaciju, kroz ITIL® preporuke uvode se dodatni aspekti merenja i upravljanja kroz procese. Istovremeno, ove smernice su primenljive za različite tipove organizacija. Daju nam preporuke na koji način ostvariti ciljeve, zadovoljiti standarde...

#### 4. PRIMENA ITIL-A

Primeri dobre prakse iz ITIL®-a delovali su logično, tako da smo odlučili da odslušamo Foundation trening, osnovni nivo u okviru ITIL® sertifikacije. Nekako se u našem radu u organizacionom smislu videlo da tu ima još nešto. Videli smo da to može bolje ali nismo znali šta i kako. U početku su nam sami procesi bili dosta apstraktni, ali kako je priča tekla polako se sve uklapalo. Otvorio nam se jedan svet koji je dao čitavu paletu mogućnosti.

Hronološki, promene koje su pratile IT sektor Uprave za trezor, kao rezultat primene ITIL® prakse su:

2014. godine:

- Urađena GAP analiza kojom smo definisali trenutni i željeni nivo razvoja IT procesa

Preporuke dobijene na osnovu analize:

- Organizovati obuke za zaposlene
- Definirati uloge i nadležnosti:
  - Security officer (nadležan za bezbednost informacija)
  - CSI (Continual Service Improvement) manager - nadležan za kontinualno unapređenja servisa
  - Service desk manager - nadležan za Servis desk

- Project manager - rukovodilac projekta, za projekat "Unapređenje IT sektora kroz primenu ITIL® preporuka"

- Oformljen je Servis Desk, implementiran ITSM (IT Service Management) alat

- Uvedeni procesi Upravljanje incidentima (Incident Management) i Rešavanje zahteva (Request fulfilment)

- Formirana grupa za harmonizaciju projekata i poslove logistike.

2015. godine:

- Započeti koraci na unapređenju procesa Upravljanje servisnim dobrima (Asset Management)

- Kroz dijalog sa klijentima formiran je Katalog usluga i definisan SLA

- Razvijena je Strategija Sektora za informacione tehnologije.

2016.godine:

- Definisan proces Upravljanje katalogom usluga (Catalog Management) i implementiran u ITSM alatu

2017. godine:

- Upravljanje servisnim dobrima implementirano u ITSM alat

2018. godine:

- Planirano uvođenje procesa Upravljanje znanjem (Knowledge Management) i Upravljanje događajima (Event Management). Radi se na unapređenju procesa Upravljanje kontinuitetom poslovanja i Finansijsko planiranje. Takođe, planirana je integracija alata za potrebe automatskog ažuriranje asset-a.

Paralelno smo radili na razvoju veština komunikacije.

Rezultati koje smo uočili tokom vremena:

Definisane su osobe koje će dati odgovore na pitanja:

- Da li smo bezbedni?
- Kako da se poboljšamo?
- Koliko efikasno pružamo usluge?
- Koliko uspešno vodimo projekte?

Definisane su IT usluge i nivo podrške koji se pruža korisnicima. Kroz Servis Desk je uvedena jedinstvena tačka kontakta za korisnike IT usluga u Upravi za trezor. Korisnici sada znaju kome treba da se obrate za usluge IT-ja i da se informišu u kojoj je fazi rešavanje incidenta ili zahteva koji su podneli.

Uspostavljeni su procesi koji mere i unapređuju kvalitet pružanja usluga. IT ima definisan način rada, jasno je određen put rešavanja incidenata i zahteva. Zaposleni su svesni strategije i dogovorenih ciljeva i samim tim jasno shvataju svoju ulogu.

Podrška rukovodstva Uprave za trezor, Direktora, Pomoćnika direktora koordinatora i Pomoćnika za Sektor za informacione tehnologije za uvođenje servisne

organizacije i obezbeđenje resursa za realizaciju navedenih aktivnosti je bila od presudnog značaja. Uvođenje Servis Desk-a je izneo Aleksandar Tošić. Konstantnu podršku smo imali od strane konsultanta Saše Antića.

## 5. LJUDSKI FAKTOR

Zadovoljstvo klijenta i korisnika zavisi od njihovog subjektivnog osećaja prilikom korišćenja usluge, gde se posebno ističu:

- Vizuelni prikaz usluge,
- Odnos IT podrške prema korisnicima,
- Jasno definisan okvir pružanja podrške.

Podrška korisnicima se pruža kroz rad Servis Desk operatera koji predstavljaju prvi nivo podrške. Viši nivoi podrške obuhvataju ceo IT sektor, uključujući i partnere.

Kvalitet rada servisa direktno zavisi od svih nivoa podrške - inženjera, tehničara i ostalih zaposlenih na tehničkim IT sistemima koji omogućavaju rad servisa.

Sve što smo do sada uradili, uvođenje servisne organizacije (ITIL®), veština komunikacije i drugo uticalo je da zaposleni imaju dodatne poglede na svet oko sebe. Samim tim postaju svesniji značaja svojih aktivnosti u operativnom radu i kroz saradnju sa kolegama. Ima puno faktora koji utiču na rad:

- Tehničko znanje je neophodno,
- Jasan cilj,
- Stanje osobe...

Svaki posao koji obavimo posledica je naše zamisli. Svakoj osobi dnevno prođe na hiljade misli, šta radimo, kako radimo, kada radimo... Većina misli nam se ponavlja iz dana u dan. Misli nam daju osobine, definišu našu ličnost i na osnovu njih funkcionišemo. Mogu biti podržavajuće ili u suprotnosti. Podržavajuće nam daju veću šansu za ostvarivanje cilja, a kada su u suprotnosti stvaraju konflikt.

Tim IT-a ima pred sobom više ciljeva. Ostvarivanje cilja se postiže angažovanjem pojedinaca koji razumeju šta oni treba da ostvare u datom okviru. Svaka aktivnost ima više aspekata, šta radimo, kada radimo, kako utiče... Tim ima kulturu ponašanja, ljudi znanje i specifične veštine. Koliko su vrednosti, uverenja i njihovi ciljevi usklađeni sa vrednostima i ciljevima IT tima direktno utiču na rezultate i atmosferu u kolektivu.

Ukoliko definišemo adekvatan cilj, uskladimo ga sa učesnicima možemo očekivati da se taj cilj i ostvari.

## 6. ZAKLJUČAK

Danas, u martu 2018. svedoci smo velikih pomena u našem okruženju. IT industrija kao jedna od mlađih industrija je nosilac promena. Tehnologija se konstantno razvija. Komunikacija nam sada omogućava da budemo u kontaktu sa ljudima širom sveta putem telefona, društvenih mreža...

Imamo puno informacija na raspolaganju. Na nama je izbor šta raditi.

Model ponašanja, rada ne moramo menjati. Pri tome se borimo da zadržimo trenutnu situaciju. Energiju trošimo suprotstavljajući se promenama, napretku, razvoju. Na taj način postajemo sve udaljeniji od ostatka koji se u svakom trenutku menja.

Model ponašanja ljudi kroz istoriju se menjao. Danas da bismo ispratili promene oko nas potrebno je da se i mi sami menjamo, prilagođavamo, budemo nosioci promena. Na taj način postajemo deo tima koji unapređuje našu sredinu, ima pozitivnu energiju, spreman je da pruži podršku. Stvarajući, kroz saradnju generišemo pozitivnu energiju koja nosi promene, život.

Kada nema promena, nema života. Život je promena.

Izbor je na svima nama.

# Kvantifikovanje relevantnosti prediktora, prediktivnog modela održavanja avionskog motora

## Quantifying importance of predictor for the predictive maintenance model for aircraft engine

Olivera Janković<sup>1</sup>, Đorđe Babić<sup>2</sup>  
ORAO a.d.<sup>1</sup>  
RAF<sup>2</sup>

**Sadržaj** – Sa porastom broja atributa seta podataka mašinskog učenja, raste i potreba za analizom njihovog odnosa, veze sa ishodom, odnosno potreba za mjerenje relevantnosti prediktivne moći atributa, vodi ka rangiranju, filterovanju prediktora. Kvantifikovanje mjere relevantnosti prediktora za potrebe izgradnje efikasnog prediktivnog modela binarne klasifikacije, modela prediktivnog održavanja, korištenjem multivarijantnog filter pristupa, generički ReliefF algoritam, biće prikazano u okviru ovoga rada.

**Abstract** - With the increasing number of attributes of the machine learning data set, there is a growing need for analyzing their relationship, a relationship with the outcome, or the need to measure the relevance of the predictive attribute power, leading to ranking, filtering predictors. The quantification of the predictable relevance measures for the purpose of building an efficient predictive model of binary classification, predictive maintenance model, using a multivariate filter approach, generic ReliefF algorithm, will be presented in this paper.

### 1. UVOD

Sinergija napretka i dostupnosti računarskog hardvera, raspoloživosti velikih količina podataka različitih izvora, i razvoj različitih algoritama mašinskog učenja vodi ka mogućnosti kreiranja prediktivnih modela. Podaci, model i predikcija predstavljaju osnovne aspekte, koje je, u kontekstu problema sa kojim se radi, neophodno analizirati i povezati, prilikom postupka izgradnje prediktivnog modela primjenom mašinskog učenja. Potrebno je dakle, primjenom algoritama, koji se koriste na raspoloživim podacima uzoraka, izgraditi model koji se kasnije može koristiti za donošenje predikcije, odnosno moći koristiti obučeni model na novim podacima.

Prediktivno održavanje je aktuelan domen koji nije dovoljno istražen u kontekstu domena primjene tehnika mašinskog učenja. Potvrdu tome daje [1], u kome se, na preko šezdeset radova u prethodećih pet godina, fokusira na korištene pristupe za rješavanje problema vezanih za otkrivanje kvarova i probleme prediktivnog održavanja, korištenjem pristupa mašinskog učenja. Generalno, stoji stav autora da mnogi važni koraci, koji utiču na odabir odgovarajućeg pristupa mašinskog učenja i u krajnjem doprinose i utiču na performanse, nisu istraženi u dovoljnoj mjeri. Naglasak je, pored ostalog, o oblastima procesa inženjeringa karakteristika, kao što su selekcija karakteristika i ekstrakcije karakteristika na primjer.

U scenariju primjene mašinskog učenja u oblasti prediktivnog održavanja u principu se koriste različite tehnike, sa vlastitim za i protiv, postoje i prisutne su i određene tendencije upotrebe, ali trenutno nije dostupan analitički postupak odlučivanja za njihov odabir, što pored prethodno pomenutog, otvara i zatijeva dodatan prostor za nova eksperimentisanja i istraživanja.

Prije nego se krene u izradu prediktivnih modela, poželjno je imati detaljno razumjevanje prediktora i ishoda za svaki set podataka. Prediktori (*predictors*), nezavisne varijable (*independent variables*), atributi (*attributes*), ili deskriptori (*descriptors*) su podaci koji se koriste kao ulazi u prediktivnu jednačinu, a ishod, rezultat (*outcome*), zavisne varijable (*dependent variables*), cilj (*target*), klasa (*classes*) ili odgovor (*response*), se odnose na događaje ili količinu koja se predviđa. Nedostatak razumjevanja može voditi ka računskim poteškoćama u izračunavanju i manjom od optimalne performanse. Nadalje, mnogi setovi podataka će zahtjevati neki stepen predprocesiranja kako bi se proširio prostor mogućih prediktivnih modela i da bi se optimizovale performanse svakog modela.

Sa namjerom da se odredi relevantnost prediktora u kontekstu date problematike, izgradnje prediktivnog modela održavanja avionskog motora putem binarne klasifikacije, biće prikazano kvantifikovanje mjere relevantnosti prediktora, korištenjem multivarijantnog filter pristupa, generičkog ReliefF algoritma. Kako bi se ustanovio doprinos kvantifikovanja relevantnosti prediktora, na efikasnost klasifikatora prediktivnog modela, isti su trenirani i testirani, na redukovanim trening i testnim setovima, nastalim na temelju rezultata relevantnosti prediktora, rangiranjem.

### 2. IZGRADNJA PREDIKTIVNOG MODELA

Problem izgradnje prediktivnog modela u okviru ovog rada baziran je na modelu koji je temeljen na podacima (*data-driven model*) koji koristi pristup i tehnike mašinskog učenja. Ovi modeli su u većoj mjeri generički, a u kontekstu pripadajućeg IoT doba, predstavljaju aktuelan, logičan ali i izazovan odabir. Domen istraživanja ovog problema, je po prirodi stvari široko aspektiran, a sam postupak sastoji se od nekoliko samostalno istraživačkih oblasti.

#### A. Prikupljanje podataka

Pristup prediktivnog održavanja počinje sa dijelom za prikupljanje podataka (*data acquisition*) [2], a odluka o



tehničari za prikupljanje podataka i postignuti rezultati utiče na korake radnog toka analize i prognoze realnog sistema (važan i u kontekstu razumjevanja implementacije u online radnom okruženju na primjer). U kontekstu prediktivnog održavanja pominju se akvizicione tehnike podataka: tehnika prikupljanja podataka u realnom vremenu, interval sistem za prikupljanje podataka, događajima vođen [3]. Dva najvažnija tipa podataka za detekciju kvara i prediktivno održavanje su podaci prikupljeni sa senzora [4], (vrijedonosni tip, talasni oblik, multidimenzionalni tip) i podaci prikupljeni log fajlovima (deskripcija aktivnosti održavanja, kvara ili greške,...).

#### B. Inženjering karakteristika

Inženjering karakteristika (*Feature Engineering*) je tematika [5] koja nije dovoljno obrađivana. U tom kontekstu naglasak je na postupcima područja ekstrakcije atributa (*feature extraction*) i selekcije atributa (*feature selection*). Cijeni se da su ova područja od velikog značaja za uspjeh mašinskog učenja, odnosno da je veliki dio uspjeha mašinskog učenja zapravo uspješnost u inženjeringu karakteristika [6]. U suštini, ponekad je neophodno da se redukuje broj karakteristika i poveća informacioni sadržaj (*information content*) karakteristika, kako bi se povećala tačnost i smanjili računarski napori pristupa mašinskog učenja za detekciju kvara i prediktivno održavanje. Ekstrakcija karakteristika i/ili selekcija karakteristika mogu pomoći u ostvarivanju ovoga cilja. Selekcija karakteristika selektuje podskup najreprezentativnijih karakteristika, dok ekstrakcija karakteristika transformiše prvobitni/originalni prostor karakteristika i dobija nove informacije kombinovanjem karakteristika. Ekstrakcija karakteristika može biti nelinearni proces pa stoga rezultati nisu samoobjašnjivi, a prednost ekstrakcije karakteristika nad odabirom karakteristika je da prostor karakteristika može biti smanjen u mnogo većem obimu [7]. Generalno posmatrano, potrebne su takve karakteristike koje opisuju strukture svojstvene korištenim podacima, koje je u biti potrebno manuelno kreirati (moderne metode dubinskog učenja (*deep learning*) postižu određeni uspjeh u području automatske identifikacije i korištenja karakteristika na sirovim podacima; npr. korištenjem restriktivne Bolcmanove mašine [8]).

#### C. Označavanje podatka

Označavanje podatka (*Data Labeling*) [9] je neophodan korak da bi pristup, temeljen na podacima, mogao analizirati podatke iz realnog sistema i tako naučio relevantne odnose datog ulaza i očekivanog izlaza. Ovo se obično vrši analizom i obilježavanjem istorijskih podataka, npr. tehnika označavanja podataka stanjem vođena, koja označava istorijske podatke u različita stanja pri čemu može da postoji različit broj stanja koji dijele životni vijek a koje pristup pokušava da klasifikuje. Odluka o odabiru tehnike označavanja podataka važna je za pronalaženje odgovarajuće tehnike mašinskog učenja.

#### D. Prozor predviđanja

Prozor predviđanja (*Prediction window*) određuje vrijeme prije nego što sistem otkaze, a pristup prediktivnog održavanja može ili treba znati da sistem otkazuje. To može biti vrijeme potrebno da se popravka zakaže ili da se definiše u kontekstu mogućnosti prepoznavanja kvara sistema. Prema [10] poželjno vrijeme za izdavanje

upozorenja je između 2 i 25 sedmice prije pojave kvara. Manje od toga, znači da operaciju zamjene možda nije moguće zakazati. Duže, znači da su troškovi visoki za prediktivno održavanje, jer je komponenta i dalje funkcionalna (postoji matrica troškova), pri čemu je, pogrešna klasifikacija nebezbednog/nesigurnog stanja kao bezbednog/sigurnog stanja mnogo teža nego pogrešno klasifikovanje bezbednog stanja u nebezbedno stanje.

#### E. Pristupi mašinskog učenja

Pristupi mašinskog učenja (*Machine learning approaches*), odnosno mašinsko učenje [11] predstavlja ključnu tehnologiju u scenariju posmatranog prediktivnog održavanja avionskog motora. U poslednjih nekoliko godina, mašinsko učenje postaje sve važnije u računarskoj nauci, jer se podaci mogu prikupljati i pohranjivati mnogo lakše. U takvom scenariju, tehnika mašinskog učenja igra ključnu ulogu [12]. Drugi razlog, za rastuću popularnost mašinskog učenja, je smanjenje troškova računanja. S evolucijom hardvera u posljednjih nekoliko godina, upotreba pristupa mašinskog učenja postalo je efektivno u smislu vremena i novca, posebno za otkrivanje tipa kvara i prediktivno održavanje [13]. Odabir tehnika i algoritama mašinskog učenja vođen iz perspektive scenarija prediktivnog održavanja dat je, kroz primjere korištenih algoritama, u radovima [Yang,14], [Zarei et al,14], [Yang et al,13]; (već je pomenuto da nije dostupan postupak odluke za odabir tehnika mašinskog učenja).

#### F. Evaluaciona strategija

Evaluaciona strategija, odnosno metrike evaluacije za ocenjivanje tehnika mašinskog učenja, koje se najčešće primjenjuju, dostupne jano u široj literaturi, nisu uvijek pogodne za kvantifikovanje performansi ovih tehnika u kontekstu prediktivnog održavanja, zbog toga je potrebno intenzivno istražiti, predstaviti i odabrati za korištenje, tehničke evaluacije koje su bolje prilagođene za procjenu rezultata i koje ukazuju na moguće nedostatke u scenariju prediktivnog održavanja.

#### G. Zahtjev vezan za podatke

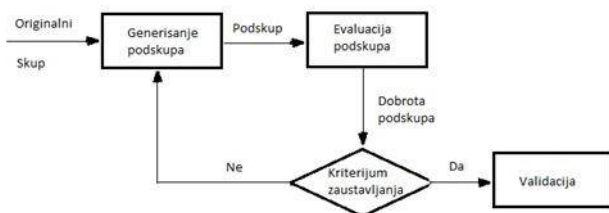
Karakteristika pristupa prediktivnog održavanja temeljenog na podacima (*data-driven*) [8] je da pored kvaliteta i veličine uzorka podataka, zahtijevaju progresiju greške/kvara, odnosno zahtijevaju dovoljno primjeraka koji su se izvršavali do kvara (*run-to-failure*), pri čemu upravo ovaj zahtjev predstavlja najveći izazov u prognozama temeljenim na podacima. Razlozi su jasno je objektivne prirode. Naime, obzirom na posljedice koje se usled ispunjenja traženog zahtjeva mogu pojaviti, to ne mogu da podrže/dozvole sebi, niti industrijski sistemi niti avioindustrija sa neupitnim zahtjevom na sigurnost. Stoga, najčešće se koriste dostupni setovi podataka iz javno dostupnih repozitorijuma.

U okviru NASA Ames repozitorija podataka [17] za predikciju, na raspolaganju su kompleti skupova podataka prognostičkih podataka, koji se sastoje od podataka vremenskih serija koji prikazuju slučajeve radom do otkaza. „Turbofan Engine Degradation Simulation Dataset“, koji će kao polazna osnova biti korišten u okviru eksperimentalne postavke ovoga rada, javno je dostupan skup pomenutog repozitorija i predstavlja simulaciju degradacije avionskog motora (sam postupak simulacije i detaljan opis atributa skupa dat je, od strane vlasnika skupova, u [18]).

### 3. RANGIRANJE PREDIKTORA

Često je potrebno, iz praktičnih razloga, kvantifikovati snaga odnosa, veze između prediktora i ishoda. Kako broj atributa postaje veći istraživačka analiza svih prediktora može biti neizbježna i usredotočavanje na one koji imaju jake odnose sa krajnjim ishodom može biti efikasna strategija obuke. Rangiranje prediktora na ovaj način može biti veoma korisno kada se radi sa velikim količinama podataka.

Jedan od osnovnih razloga za mjerenje jačine ili relevantnosti prediktora je filtriranje koje bi trebalo da se koristi kao ulaz u model. Ova nadgledana selekcija atributa (*supervised feature selection*) može biti vođena podacima kojima se raspolaže. Rezultat ovog procesa filterovanja, zajedno sa ekspertizom predmetne teme, može biti kritičan korak u kreiranju efikasnog prediktivnog modela. Mnogi algoritmi selekcije karakteristika, (tipični koraci selekcije atributa dati na Sl.1) se oslanjaju na kvantitativni značaj rezultata filterovanja.



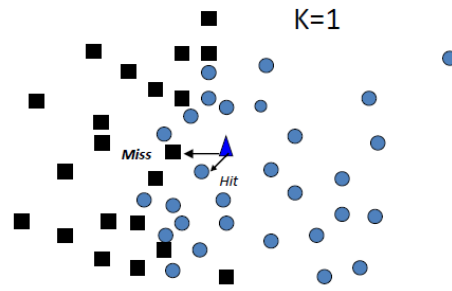
Slika 1. Koraci za selekciju atributa

Ukoliko se kod selekcije dobrog podskupa atributa (općenito mnogi zadaci vezani za selekciju atributa spadaju u klasu NP-teških (NP-hard) problema) koristi pristup da se napravi neka nezavisna procjena bazirana na generalnim karakteristikama podataka, onda se radi o tzv. filter pristupu (rangiranju) jer je set atributa filterovan da bi proizveo najviše obećavajući podskup podataka prije nego učenje počne [19]. (Druga opcija je da se evaluira podskup koristeći algoritam mašinskog učenja koji će na kraju biti korišten za učenje, tzv. wrapper pristup.) Individualno rangiranje atributa može se izvesti korištenjem evaluatora koji, na primjer, vrše evaluaciju na osnovu: informacijskog dobitka (Information Gain (IG)), omjera dobitka (Gain Ratio (GR)) ili dosta korištenog Hi-kvadrat (Chi-Squared (CS)) metoda na primjer.

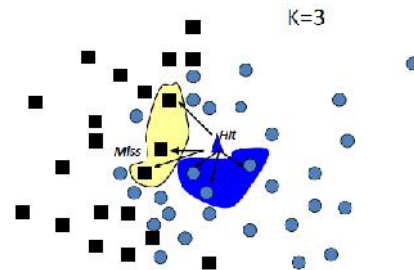
Za razliku od većine drugih metoda rangiranja karakteristika ili selekcije atributa koje pojedinačno uzimaju u obzir attribute, Relief algoritmi mogu da uhvate interakcije atributa jer je globalna mjera udaljenosti koja definiše blizinu uzorka multivarijantna funkcija.

#### A. ReliefF algoritam

ReliefF algoritam [20] predstavlja proširenje Relief algoritma, originalno razvijen za klasifikacione probleme sa dvije klase, (Kirra&Rendel,1992) za potrebe rješavanje podataka koji su bučni, nepotpuni i koji imaju više od dvije klase. Originalni Relief algoritam, koristi 2 susjedna uzorka (1 bliski pogodak – „hit“ i 1 bliski promašaj – „miss“; prikazano na Sl.2.) tokom svake iteracije, dok



Slika 2. Relief algoritam, K=1



Slika 3. ReliefF algoritam, K=3 (višeklasni problemi)

ReliefF koristi 2k susjedne uzorke (k najbližih primjeraka/bliskih pogodaka iste klase i k najbližih primjeraka/bliskih pogodaka suprotne klase), i prosjek njihova doprinosa da ažurira težinu atributa [21]. Princip pri određivanju težine varijabli je da bi primjeri koji pripadaju istoj klasi trebali biti bliže nego li primjeri različite klase. U nastavku, u okviru date eksperimentalne postavke, biće korištena ReliefF Weka implementacija - evaluator atributa ReliefFAttributeEval i Ranker metoda pretraživanja.

### 4. EKSPERIMENTALNE POSTAVKE I DISKUSIJA REZULTATA

#### A. Ulazni set podataka prediktivnog modela za održavanje avionskih motora

Za potrebe okvira ovoga rada, kao polazna osnova, biće korišten jedan od četiri dostupna trening i testna seta, Train\_FD003.txt i Test\_FD003.txt sa atributima (nazivi semantički prilagođeni): oznaka motora i tri različita setovanja za svaki motor, višestruke multivarijantne vremenske serije, ciklusom kao vremenskom jedinicom zajedno sa očitanim vrijednostima 21 senzora za svaki ciklus. To zajedno čini 26 atributa (označeno kao sirovi atributi na Sl.1.), za 24720 instanci trening seta (Testni set sadrži 16596 instanci i 26 atributa).

Pored sirovih atributa, kreirani su agregirani atributi (SI1), koji u osnovi sažimaju istorijske aktivnosti za posmatranu problematiku vezanu za avionski motor, dva tipa agregiranih karakteristika: kretanje prosječne vrijednosti sa senzora i standardnu devijaciju senzorskih vrijednosti u prethodnim ciklusima (parametar vremenskog prozora W, za koji se vrši agregiranje iznosi 7, sve sa ciljem da se za potrebe kreiranja prediktivnog modela postigne više sa podacima koji su na raspolaganju. U biti, radi se o procesu poznatom kao proces inženjeringa karakteristika [22], kako bi se kreirali trening podaci tako da posjeduju karakteristike koje imaju prediktivnu snagu za ciljnu predikciju.



Kako trening set (niti testni set) izvorno ne sadrži oznaku klase, da bi se izvršila predikcija putem binarne klasifikacije, u kontekstu prirode izabranog seta podataka predviđanje kvara avionskog motora u opsegu određenog broja ciklusa, neophodno je označavanje klase [23]. Obzirom da je predikcija rađena za opseg od 30 ciklusa, oznaka klase, (Klasa {0,1} na S1.4) je urađena uzimajući 30 poslednjih instanci koje su označene sa 1, dok su sve ostale za vrijednost oznake imale nulu, što respektivno polazi od i ukazuje na blizinu i odsustvo kvara.

Zbirno, kao što se može vidjeti sa prikaza korištenog .ARFF fajla na S1.4 (određeni atributi u nizu su izostavljeni zbog veličine prikaza), računajući i atribut klase, radi se o ukupno 69 atributa trening seta koji će biti korišteni u okviru eksperimentalne postavke.

```

% Vremenske serije turbo gasnih motora avion
% trening skup (klasifikacija w7 avg std)

@relation Serije
@attribute ID motora numeric
@attribute Ciklus numeric
@attribute Setovanje1 numeric
@attribute Setovanje2 numeric
@attribute Setovanje3 numeric
@attribute Senzor1 numeric
@attribute Senzor2 numeric
@attribute Senzor3 numeric
@attribute Senzor4 numeric
@attribute Senzor5 numeric
@attribute Senzor6 numeric
...
@attribute Senzor16 numeric
@attribute Senzor17 numeric
@attribute Senzor18 numeric
@attribute Senzor19 numeric
@attribute Senzor20 numeric
@attribute Senzor21 numeric
@attribute SSenzor1 numeric
@attribute SSenzor2 numeric
@attribute SSenzor3 numeric
@attribute SSenzor4 numeric
@attribute SSenzor5 numeric
@attribute SSenzor6 numeric
...
@attribute SSenzor16 numeric
@attribute SSenzor17 numeric
@attribute SSenzor18 numeric
@attribute SSenzor19 numeric
@attribute SSenzor20 numeric
@attribute SSenzor21 numeric
@attribute SSSenzor1 numeric
@attribute SSSenzor2 numeric
@attribute SSSenzor3 numeric
@attribute SSSenzor4 numeric
@attribute SSSenzor5 numeric
@attribute SSSenzor6 numeric
...
@attribute SSSenzor16 numeric
@attribute SSSenzor17 numeric
@attribute SSSenzor18 numeric
@attribute SSSenzor19 numeric
@attribute SSSenzor20 numeric
@attribute SSSenzor21 numeric
@attribute Klasa {0,1}

```

Slika 4. Prikaz ulaznog seta podataka

### B. Korišteni klasifikatori

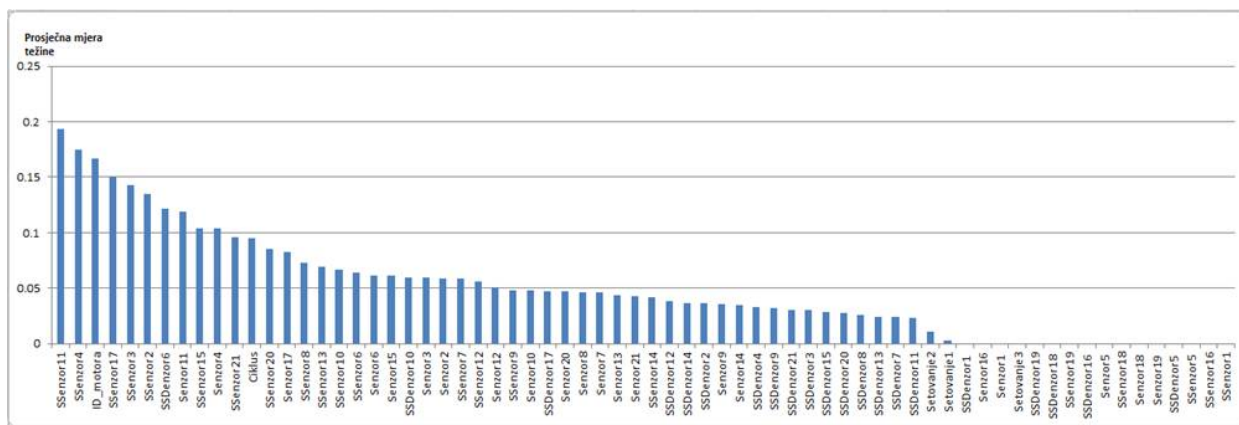
Za potrebe izgradnje i poređenja rezultata prediktivnih modela biće korišteno šest različitih klasifikatora:

- algoritam logističke regresije (Logistic Regression), jedan od najpopularnijih algoritama mašinskog učenja za binarne klasifikacije, u osnovi koje leži logistička funkcija – poznata i kao sigmoid funkcija;
- algoritam slučajna šuma (Random Forest), algoritam stabla odlučivanja (kreira veći broj klasifikatora u obliku stabla odlučivanja);
- algoritam stabla odlučivanja J48, baziran na C4.5 algoritmu koji generiše stablo odlučivanja;
- algoritam k-najbližeg susjeda IBk, primjer lijernih (lazy) klasifikacijsko-prediktivskih postupaka (k=7);
- implementacija algoritma vektora podrške (SMO) i
- višeslojni perceptron (MLP, Multilayer Perceptron) najistaknutiji tip vještačke neuronske mreže.

### C. Rezultati i diskusija

Za određivanje relevantnosti prediktora ulaznog seta podataka u kontekstu date problematike, izgradnje prediktivnog modela održavanja avionskog motora putem binarne klasifikacije, izvedeno je kvantifikovanje mjere relevantnosti prediktora korištenjem multivarijantnog filter pristupa, generičkog ReliefF algoritma. Rezultati primjene, rangiranje prediktora ulaznog seta u opadajućem redoslijedu relevantnosti, putem evaluatora atributa ReliefFAttributeEval i Ranker metode pretraživanja, grafički su dati na S1.5 (korištena je 10-struka unakrsna validacija).

Sa ciljem praćenja i u krajnjem eliminisanja, negativnog uticaja irelevantnih atributa na performanse binarne klasifikacije (postizanja veće klasifikacione tačnosti na primjer), izvršena je redukcija obima ulaznog seta podataka – polazni skup podataka je redukovan za 13 poslednjih atributa, prikazanih na S1.5, u skladu sa rezultatima postignutim procjenom od strane ReliefF algoritma. Korištenjem gore navedenih klasifikatora dobijeni su prediktivni modeli: obučeni na kompletnom i modeli obučeni na redukovanom setu; evaluacija performansi modela je izvršena korištenjem kompletnog, odnosno redukovanog testnog seta respektivno.

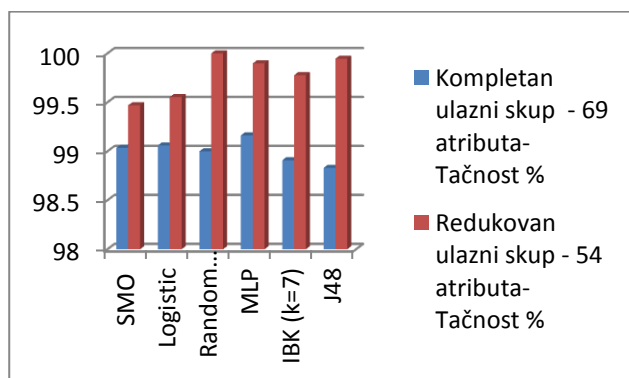


Slika 5. Rezultati rangiranja prediktora, korištenjem ReliefF algoritma, u skladu sa prosječnim težinama

**Tabela 1.** Tačnost klasifikacije za originalni i redukovani set podataka, nastao selekcijom atributa – multivarijantne filter metode ReliefF, u skladu sa rangiranjem, na ulaznom setu podataka

	<b>Kompletan ulazni skup - 69 atributa-</b>	<b>Redukovan ulazni skup - 53 atributa-</b>
	Tačnost %	Tačnost %
SMO	99.0359 (160)	99.4698 (88)
Logistic	99.06 (156)	99.5541 (74)
Random Forest	98.9998 (166)	<b>100.00 0</b>
MLP	99.1624 (139)	99.8976 (17)
IBK (k=7)	98.9094 (181)	99.7771 (37)
J48	98.831 (194)	99.9458 (9)

Rezultati tako nastalih prediktivnih modela, putem klasifikacione tačnosti (pored svake vrijednosti tačnosti u zagradama se nalazi i pripadajući broj netačno klasifikovanih instanci (od ukupno 16596)), na kompletnom skupu i na skupu sa redukovanim brojem atributa dati su u Tabeli 1, kako bi se vidjelo u kojoj je mjeri primjena rezultata predloženog kvantifikovanja relevantnosti prediktora doprinijela efikasnosti prediktivnih modela, korištenih klasifikatora binarne klasifikacije. Grafičko pređenje rezultata klasifikatora, ilustracija efekta redukovanja broja prediktora korištenjem ReliefF multivarijantnog filter pristupa, dati su na Sl.6.



Slika 6. Grafički prikaz tačnosti korištenih klasifikatora prije i nakon primjene rangiranja i redukcije prediktora

Na osnovu obavljenih eksperimenata, dobijenih i prikazanih rezultata (Tabela 1) može se zaključiti da je:

- svaki od klasifikatora postigao bolje rezultate, veću klasifikacionu tačnost, na redukovanom setu podataka u odnosu na kompletan/originalni skup podataka, odnosno, svaki od klasifikatora je imao koristi od primjenjenog postupka kvantifikovanja temeljem kojeg je izvršena redukcija.
- postignuti rezultati su značajni, obzirom na uvećanje vrijednost klasifikacione tačnosti, za svaki od klasifikatora, pri čemu je najveću korist od primjenjenog postupka imao algoritam stabla odlučivanja J48.
- najbolji rezultat, najveću klasifikacionu tačnost postigao je algoritam slučajna šuma, rekordnih 100 procenata.

## ZAKLJUČAK

U radu je prikazan jedan, eksperimentalnim rezultatima pokazano, efikasan način kvantifikovanja relevantnosti prediktora, temeljem rezultata kojeg je izvršena selekcija i redukcije atributa prediktivnog modela održavanja avionskog motora. Dakle, može se konstatovati da se metod filtriranja korištenjem multivarijantnog pristupa, primjenom ReliefF algoritma, pokazao koristan za procjenu, rangiranje relevantnosti prediktora, odnosno eliminisanje negativnog uticaja irelevantnih atributa na performanse klasifikacije.

## LITERATURA

- [1] Jahnke, P. "Machine Learning Approaches for Failure Type Detection and Predictive Maintenance," Master Thesis, 2015.
- [2] Jardine, A.K.S., Lin D. and Dragan Banjevic, "A review on machinery diagnostics and prognostics implementing condition-based maintenance", Mechanical systems and signal processing, Vol.20, No. 7, pp 483–1510, 2006.
- [3] Baldoni, R. Contenti, M. and A. Virgillito, „The evolution of publish/subscribe communication systems. In Future Directions in Distributed Computing“, Vol. 2584 of Lecture Notes in Computer Science, pp 137–141. Springer Berlin Heidelberg, 2003.
- [4] Aggarwal, C.C. „Managing and mining sensor data“, Springer Science & Business Media, 2013.
- [5] Boire, R. „Feature Engineering within the Predictive Analytics Process — Part One“, Dostupno: <http://www.predictiveanalyticsworld.com/patimes/feature-engineering-within-the-predictive-analytics-process-part-one/7657/2016>.
- [6] Heaton, "An empirical analysis of feature engineering for predictive modeling", SoutheastCon 2016, pp 1- 6, 2016.
- [7] Liu, T. Chen, Z. Zhang, B. Ma, W.Y. and G. Wu, „Improving text classification using local latent semantic indexing“, In IEEE International Conference on Data Mining (ICDM), pp 162–169, 2004.
- [8] Salakhutdinov, R and G. Hinton, „Deep Boltzmann Machines“, Appearing in Proceedings of the 12th International Conference on Artificial Intelligence and Statistics (AISTATS) 2009, Clearwater Beach, Florida, USA. Vol. 5 of JMLR: W&CP 5. [Online]. Dostupno: <http://www.utstat.toronto.edu/~rsalakhu/papers/dbm.pdf>
- [9] Hu, C. Youn, B.D. Wang, P. and J.T. Yoon, „Ensemble of Data-Driven Prognostic Algorithms for Robust Prediction of Remaining Useful Life“, Reliability Engineering and System Safety, 2012.
- [10] Mehta, P. Werner, A. and L. Mears, „Condition based maintenance-systems integration and intelligence using bayesian classification and sensor fusion“, Journal of Intelligent Manufacturing, pp 1–16, 2013.

- [11] Domingos, P. "A Few Useful Things to Know about Machine Learning", Magazine Communications of the ACM, Vol. 55 No. 10, pp 78-87, October 2012.
- [12] Witten, I. H. and E. Frank, Data Mining Practical Machine Learning Tools and Techniques, Elsevier, 2011.
- [13] Susto, G.A. Schirru, A. Pampuri, S. McLoone, S. and A. Begh, „Machine Learning for Predictive Maintenance: A Multiple Classifier Approach“, Published in: IEEE Transactions on Industrial Informatics, Vol. 11, No. 3, June 2015.
- [14] Yang, W-A. „Simultaneous monitoring of mean vector and covariance matrix shifts in bivariate manufacturing processes using hybrid ensemble learning-based model“, Journal of Intelligent Manufacturing, pp 1–30, 2014.
- [15] Zarei, J. Tajeddini, M.A. and H. R. Karimi, „Vibration analysis for bearing fault detection and classification using an intelligent filter“, Mechatronics, Vol. 24, No 2, pp151–157, 2014.
- [16] Yang W-A. and W. Zhou, „Autoregressive coefficient-invariant control chart pattern recognition in autocorrelated manufacturing processes using neural network ensemble“, Journal of Intelligent Manufacturing, pp 1–20, 2013.
- [17] NASA Ames Research Center, A. Saxena and K. Goebel "Turbofan Engine Degradation Simulation Data Set", NASA Ames Prognostics Data Repository, 2008. ([Online]. Dostupno: <http://ti.arc.nasa.gov/project/prognostic-data-repository>), Moffett Field, CA, 2008.
- [18] Saxena, A. Goebel, K. Simon, D. and N. Eklund, "Damage Propagation Modeling for Aircraft Engine Run-to-Failure", in the Proceedings of the 1st International Conference on Prognostics and Health Management (PHM08), Denver CO, Oct 2008. [Online]. Available <https://www.researchgate.net>
- [19] Janković, O. „Data Mining: Implikacije filterovanja rangiranjem na performanse klasifikacionog modela“, ETRAN 2016, Zbornik 60. konferencije za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku ETRAN 2016, , str. RT5.5.1-6, Zlatibor, 2016.
- [20] Robnik-Šikonja, M. and I. Kononenko, „Theoretical and empirical analysis of ReliefF and RreliefF MachineLearning“, Vol. 53, pp 23-69, 2003.
- [21] Kononenko I. „Estimating attributes: analysis and extensions of RELIEF“; Proceedings of the European conference on machine learning on Machine Learning; Catania, Springer-Verlag New York, Inc.: pp. 171–182, 1994.
- [22] Janković, O. „Inženjering karakteristika u kontekstu predikcije korištenjem binarne klasifikacije“, XXIII naučna i biznis konferencija YU INFO 2017, Zbornik radova, str.46-51, Kopaonik, 2017.
- [23] Janković, O. „Implementacija modela prediktivnog održavanja korištenjem binarne klasifikacije“, XVI Međunarodni naučno-stručni simpozijum INFOTEH Jahorina 2017, Vol. 16, str.576-581, 2017.

# IDENTIFIKACIONI SISTEM ZA PREOZNAVANJE DUŽICE OKA ZASNOVAN NA UPOTREBI VistaFA2 BioCAM

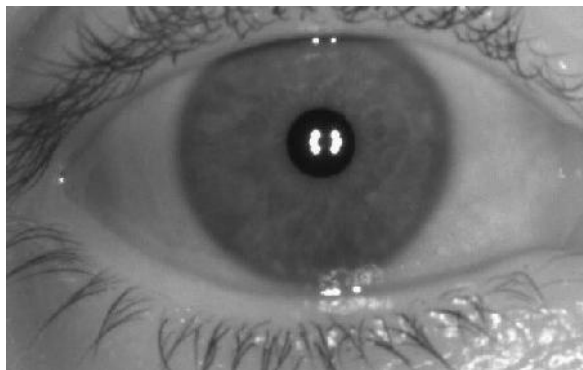
## IRIS RECOGNITION IDENTIFICATION SYSTEM BASED ON USING VistaFA2 BioCAM

Nedeljko Lekić

*Elektrotehnički fakultet, Univerzitet Crne Gore*

**Sadržaj** – U ovom radu predstavljen je identifikacioni sistema za prepoznavanje dužice oka. Kao skener dužice upotrijebljena je kamera VistaFA2 BioCam. Sistem omogućuje jednostavno upisivanje i identifikaciju korisnika. Upisivanje i identifikacija se mogu obaviti na dva načina: upotrebom Vista FA2 kamere i korištenjem već raspoložive slike dužice. Podaci se čuvaju unutar MySQL baze podataka.

**Abstract** –The iris recognition identification system based on using VistaFA2 Single Iris & Face Camera is presented in this paper. The system ensures easy enrollment and identification in two ways: with VistaFA2 Camera and using already available iris image. The all system data are stored into MySQL database.



Slika 1. Slika oka dobijena upotrebom VistaFA2 BioCam.

### 1. UVOD

Dužica je tanka, kružna struktura u oku, odgovorna za kontrolu prečnika, odnosno veličine zjenice, a time i za količinu svjetlosti koja dopire do mrežnjače. Dužica se počinje formirati u trećem mjesecu trudnoće. Njena struktura se kompletira do osmog mjeseca, mada se pigmentno srastanje može nastaviti i prve postnatalne godine [1]. Struktura dužice je različita za svako oko, kako kod očiju jednojajčanih blizanaca tako i kod lijevog i desnog oka iste osobe. Dužica je dobro zaštićena od uticaja spoljašnje sredine. Njena struktura ostaje nepromijenjen tokom vremena.

Struktura dužice je kompleksna i sačinjena od pjega, brazdi, kriпти, prstenova, grebena, korona, lucnih ligamenta, zavojitih ogrlica, itd. Tako bogata struktura, sa slučajnim varijacijama, izuzetno je pogodna za biometrijsku identifikaciju. Prilikom slikanja, koristi se infracrveno spektralno područje, gdje čak i naizgled tamne i jednolične dužice otkrivaju svoju bogatu teksturu. Na Slici 1 prikazana je slika oka dobijena upotrebom VistaFA2 BioCAM.

U teksturi dužice postoji više od 266 stepena slobode, odnosno strukturnih karakteristika koje nezavisno variraju, kod različitih očiju. Ovo doprinosi da se odluka o prepoznavanju donese brzo i sa visokom pouzdanošću i omogućuje brzo pretraživanje velikih, nacionalnih, baza podataka. Tehnologija prepoznavanje dužice pokazuje najbolje performanse za rad u 1:n modu pretraživanja.

U poređenju sa drugim biometrijskim karakteristikama dužica je u prednosti po više osnova.

Dužica je dobro zaštićena iza kapaka, rožnjače i očne vodice što je čini manje osjetljivom na oštećenja. Mogućnost zaprljanja ili ogrebotina kod drugih biometrijskih karakteristika, kao što je otisak prsta, je vrlo prisutan problem. Upotreba načara ili kontaktnih sočiva nema bitnog uticaja na očitavanje strukture dužice. U poređenju sa licem kao biometrijskim identifikatorom dužica je u prednosti zbog nepromjenljivosti s vremenom i puno izraženije jedinstvenosti.

Fiziološka reakcija dužice na svjetlo može se iskoristiti kao prirodan test za detekciju falsifikata. Takvu karakteristiku ne posjeduje nijedna druga biometrijska identifikaciona metoda.

Ipak tehnologija prepoznavanja dužice se sučava i sa njoj svojstvenim poteškoćama. Prečnik dužice je svega oko 1cm pa je za njeno skeniranje potrebna posvećenija saradnja korisnika. S druge strane, skeniranje dužice otežava djelimična prekrivenost očnim kopcima, kao i povremeno spuštanje kapaka.

Mogućnost da se dužica oka koristi za identifikaciju prvi je sugerisao Dr. Frank Burch 1939. godine. Prvi algoritmi za prepoznavanje dužice razvijeni su na Univerzitetu Cambridge, od strane Dr John Dougman-a [2-5]. Danas mnoge kompanije koriste i dalje razvijaju ove algoritme u cilju kreiranja različitih proizvoda i servisa. Neke od njih su BAYOMETRIC [6], IrisGuard [7], NEUROTechnology [8], CMITECH [9], IRISYS [10], itd.

Glavne primjene ove tehnologije su: zamjena za pasoše u automatizovanim graničnoj kontroli, ubrzanje sigurnosnih provjera na aerodromima, kontrolu pristupa zaštićenim prostorima, identifikacije u školama i bolnicama (npr.



uparivanje majke i novorođečeta), pristup bazama podataka, identifikaciju zatvorenika, praćenje sumljivih osoba, itd.

Najranija veća primjena tehnologije prepoznavanja dužice desila se 2001. godine u Ujedinjenim Arapskim Emiratima (UAE). U UAE se svaki dan, kroz pretraživanja baza u realnom vremenu, obavi više od 12 milijardi poređenja dužica. Putnici koji ulaze u UAE na svih 35 vazdušnih, zemaljsih i morskih pristupa, skenirju dužice i dobijeni kod se poredi sa raspoloživim kodovima dužica u bazi podataka [11]. Joše veća primjena u kojoj se kod dužice smješta u ID kartici, realizovana u indijskoj državi Andhra Pradesh [12].

Prognoza je da će tehnologija prepoznavanja dužice naći primjenu i u širokom spektru drugih aplikacija, u kojima identitet osobe treba biti pouzdanije utvrđen nego samo na osnovu posjedovanja uobičajenih dokumenata.

U ovom radu predstavljen je identifikacioni sistem za prepoznavanje dužice, u kojem je kao skener dužice upotrijebljena VistaFA2 Single Iris & Face Camera [13]. U okviru razvijene PC aplikacije, omogućeno je upisivanje korisnika u sistem, idenifikacija korisnika, kao i izvještavanje o izvršenim identifikacijama. Sastavni dio sistema je MySQL baza podataka u kojoj se čuvaju podaci o korisnicima sistema, kao i podaci o izvršenim identifikacijama.

Rad je organizovan na sljedeći način. U poglavlju 2 date su osnovne informacije o tehnologiji prepoznavanja dužice. U poglavlju 3 date su osnovne karakteristike upotrijebljenog skenera dužice. Detaljniji opis predloženog ID sistema dat je u poglavlju 4. Zaključak je dat u poglavlju 5.

## 2. TEHNOLOGIJA PREPOZNAVANJA DUŽICE

Tehnologija prepoznavanja dužice kombiuje kompjutersku viziju, prepoznavanje oblika, statističko zaključivanje i optiku. Njen cilj je da matematičkom analizom slike teksture dužice, u realnom vremenu omogući utvrđivanje identiteta osobe. Identifikacija se obavlja bez kontakta korisnika i skenera, sa odgovarajuće udaljenosti između njih.

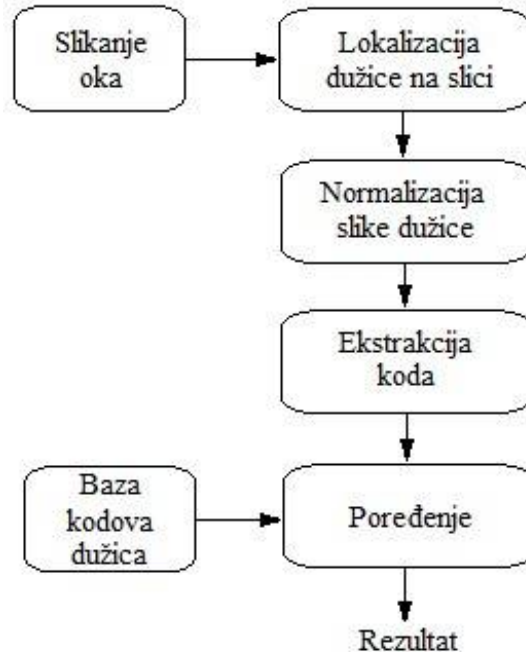
U postupku prepoznavanje dužice oka mogu se uočiti sljedeće faze:

- slikanje oka,
- lokalizacija dužice,
- normalizacija dužice,
- ekstrakcija karakteristika i
- poređenje
- 

Na Slici 2 prikazan je blok dijagram postupka prepoznavanja dužice, u kome svaki blok predstavlja jednu fazu postupka.

Slikanje dužice predstavlja početnu fazu postupka prepoznavanja. Slika mora obilovati teksturom dužice, biti što veće rezolucije i bolje jasnoće. Uspjeh ostalih faza neposredno zavisi od kvaliteta dobijene slike. Prilikom slikanja korisnik se postavlja ispred kamere u odgovarajuć

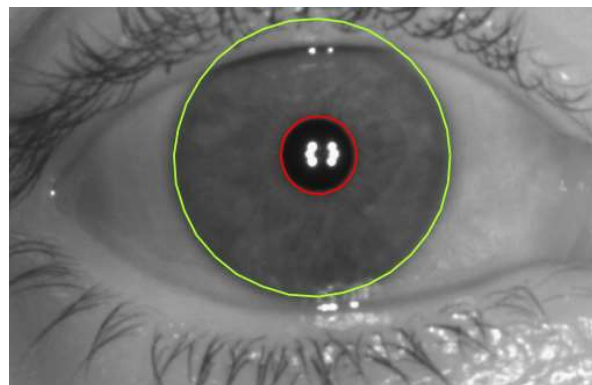
položaj, u čemu mu pomažu indikatori na kameri. Za slikanje se koristi infracrveno spektralno područje, čime se umanjuje refleksija sa područja dužice. Osim toga, u slučaju vidljive svjetlosti, dobija se slab kontrast između tamne dužice i zjenice, pa je u kasnijim fazama teško izdvojiti region dužice [14].



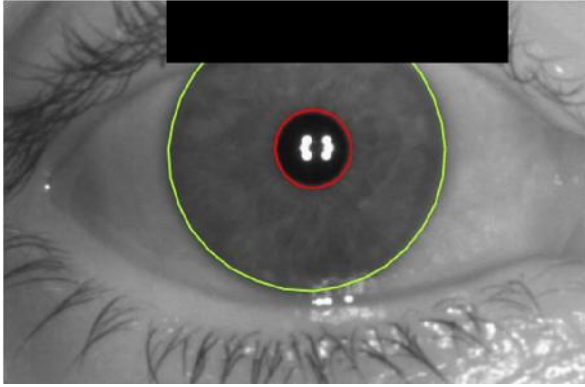
Slika 2. Faze u postupku prepoznavanja dužice.

Glavni cilj u fazi lokalizacije dužice je određivanje unutrašnje i spoljašnje granice dužice, u digitalnoj slici. Unutrašnja granica predstavlja granicu između dužice i zjenice, dok spoljašnja predstavlja granicu između dužice i beonjače. Osim određivanja navedenih granica, u ovoj fazi se, u podgručju dužice, lokalizuju očni kapci, trepavice i odsjaj [15][16].

Na Slici 3 predstavljena je slika oka dobijena upotrebom VistaFA2 BioCAM, sa lokalizovanim unutrašnjim i spoljašnjim granicama dužice, dok je na Slici 4 predstavljena ista slika, sa lokalizovanom granicom između dužice i trepavica.



Slika 3. Slika oka sa lokalizovanim unutrašnjim i spoljašnjim granicama dužice



Slika 4. Lokalizovana granica između dužice i trepavica

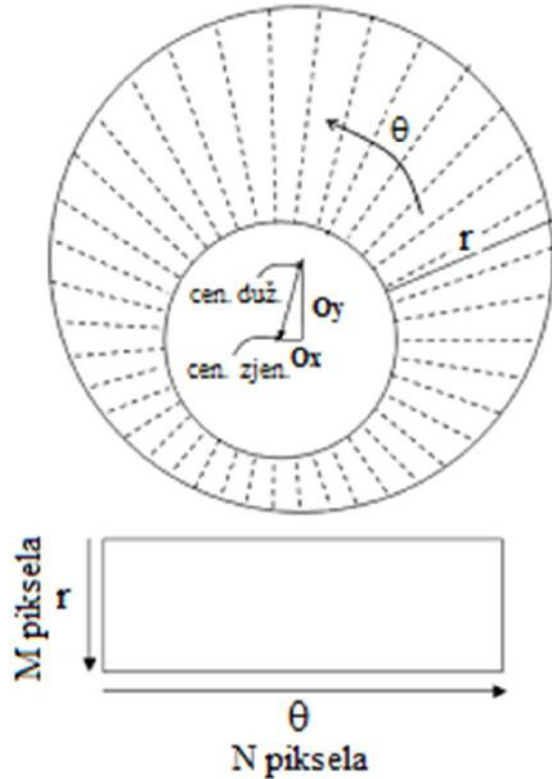
Nakon lociranja dužice, sljedeća faza je normalizacija. Normalizacija ima za cilj obezbjeđivanje fiksnih dimenzija regiona dužice. Veličina dužice na slici, pozicija zjenice unutar dužice, kao i orijentacija dužice mijenjaju se od osobe do osobe, odnosno od snimka do snimka. Da bi se bilo u stanju efikasno porediti kodove dužica, neophodno je predstavljanje regiona dužice učiniti istim i istih dimenzija, u svim slučajevima. U fazi normalizacije, region dužice se transformiše u njegov polarni ekvivalent. Takva transformacija se može izvesti upotrebom Daugman Rubber sheet modela [4]. Kao referentna tačka uzima se centar zjenice. Radijalni vektori presijecaju region dužice. Isti broj tačaka podataka se uzima po svakoj radijalnoj liniji. Time se definiše radijalna rezolucija normalizovanog regiona dužice. Broj radijalnih linija određuje ugaonu rezoluciju normalizovanog regiona dužice. Normalizacijom se dobija dvodimanzionalni niz, u kome horizontalnu dimenziju određuje ugaona rezolucija a vertikalnu dimenziju radijalna rezolucija (Slika 5) [5].

Ekstrakcija je završna faza u generisanju koda dužice. U ovoj fazi se izdvajaju najizraženiji obrasci iz normalizovane predstave regiona dužice. U postupku ekstrakcije, upotrebom banke kompleksnih 2D Gabor wavelet-a, struktura dužice se predstavlja nizom fazora (vektora u kompleksnoj ravni). Kvantizovanjem ugla fazora određuje se kvadrant kompleksne ravni u kojoj se fazor nalazi. Kod dužice se formira tako što se informacija o kvadrantu kompleksne ravni svakog fazora predstavlja sa 2 bita [4][5].

Informacija o amplitudi fazora se ne koristi jer nije u dovoljnoj mjeri diskriminujuća i zavisi od mnogih faktora, kao što su oštrina slike, osvjetljenje, pojačanje kamere, itd.

Za upoređivanje kodova dužica, u skladu sa Dougman-ovom metodom, u uporebi je test statističke nezavisnosti [2]. Test statističke nezavisnosti se primjenjuje jednostavno upotrebom  $\otimes$ -ili operatora bulove algebre i izračunavanjem hamingove distance (HD) između kodova dvaju dužica, prema formuli:

$$HD = \frac{\|(kodA \otimes kodB) \cap maskaA \cap maskaB\|}{\|maskaA \cap maskaB\|} \quad (1)$$



Slika 5. Normalizacija regiona dužice

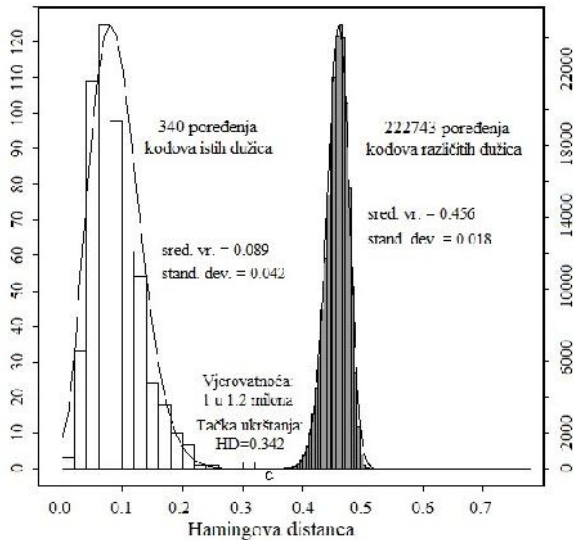
U (1) su sa  $kodA$  i  $kodB$  predstavljeni kodovi dužica koji se porede, dok su sa  $maskaA$  i  $maskaB$  predstavljene maske kodova dužica. Maske osiguravaju da na rezultat poređenja neće uticati smetnje u kodovima, koje su posljedica trepavica, kapaka, zranaste refleksije i dr. Iz (1) se vidi da  $HD$  zapravo predstavlja frakcionu mjeru različitosti dvaju kodova dužica.  $HD=0$  označava savršeno podudaranje kodova dužica. Za kodove različitih dužica  $HD$  će biti približno jednaka 0.5, jer statističke nezavisnot podrazumijeva slučajnu vrijednost bita u kodovima, te je i vjerovatnoća da bitovi budu isti, odnosno različiti, približno ista [4][5].

Na Slici 6 je dat uporedni prikaz vrijednosti  $HD$  za slučaj poređenja kodova različitih dužica, i  $HD$  za slučaj poređenja kodova dobijenih iz različitih slika istih dužica [17]. Iz Slike 6 se uočava da se  $HD$ -e u ova dva slučaja značajno razlikuju. Tačka ukrštanja nalazi na  $HD=0.342$ , čije je vjerovatnoća pojavljivanja prilično mala i iznosi 1 prema 1.2 miliona.

### 3. VISTAFA2 BIOCAM

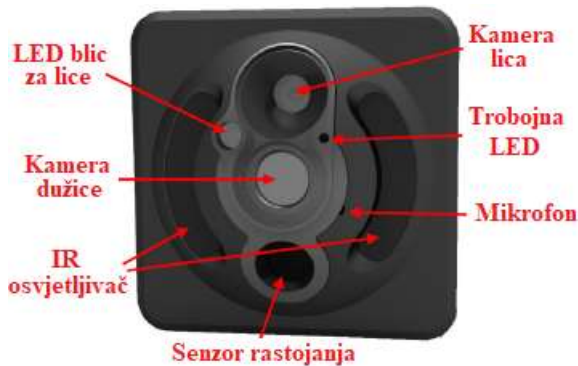
U identifikacionom sistemu za prepoznavanje dužice oka, koji je predstavljen u ovom radu, za slikanje dužice upotrijebljena je VistaFA2 Single Iris & Face Camera [13].

VistaFA2 je kompletna multimodalna biometrijska periferija, koja se može koristiti za Windows CE, XP, Vista, Windows 7 i 10, kao i za Linux OS platforme.



Slika 6. Hamingova distanca kodova različitih dužica, i kodova dobijenih iz različitih slika istih dužica

VistaFA2 sadrži CMOS kameru za dužicu, ogledalo, infracrveni (IR) osvjetljivač, trobojnu LED, senzor za rastojanje, kameru za lice, LED bic za lice i mikrofon (Slika 7).



Slika 7. VistaFA2 Single Iris & Face Camera

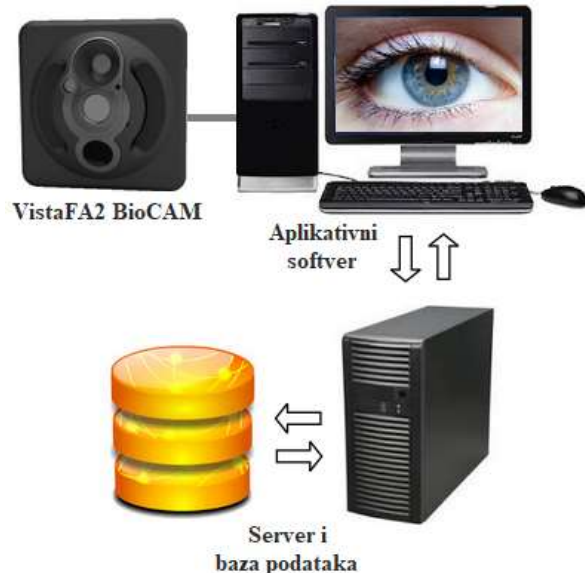
Nominalno rastojanje oka od VistaFA2 kamere je oko 25cm. Da bi se korisniku omogućilo jednostavno pozicioniranje prilikom slikanja, kamera dužice je postavljena iza ogledala. Akustični senzor rastojanja omogućuje korisniku da jednostavno odredi odgovarajuće rastojanje od kamere. Trobojna RGB LED signalizira korisniku na kakvom je odstojanju od kamere. Plava boja označava da je predaleko, crvena da je preblizu, a zelena da je na pravom odstojanju. Za povezivanje sa računarom ili drugim procesorskim uređajem kamera raspolaže standardnim USB 2.0 Female Type B priključkom.

#### 4. OPIS IDENTIFIKACIONOG SISTEMA

Osnovni sastavni dijelovi predloženog identifikacionog sistema su:

- VistaFA2 Single Iris & Face Camera
- PC aplikacija i
- baza podataka.

Na Slici 8 prikazana je blok šema sistema.



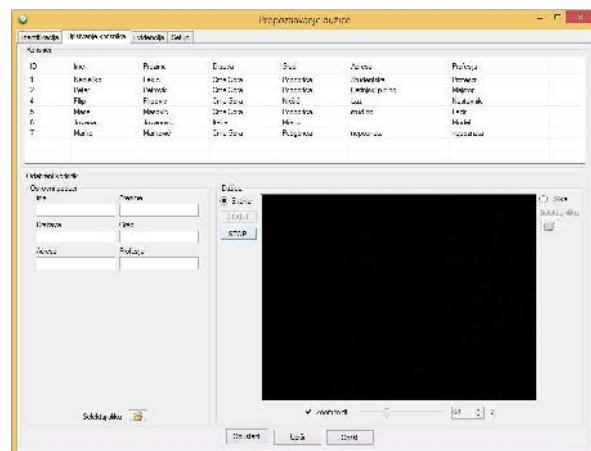
Slika 8. Blok šema identifikacionog sistema

Aplikacija može da radi u dva osnovna režima i to:

- upisivanje korisnika i
- identifikacija

U razvoju aplikacije, korišten je Biometric VeryEye 10.0 Software Development Kit, proizvod kompanije NEUROtechnology [8].

Na Slici 9 prikazan je izgled aplikacije kada ona radi u režimu upisivanja korisnika.



Slika 9. Aplikacija u režimu upisivanja korisnika

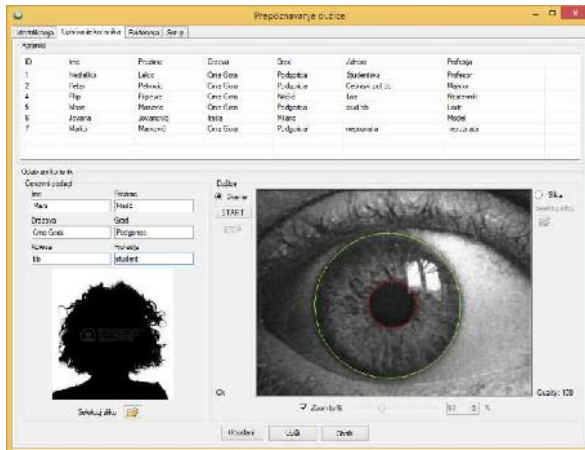
U gornjem dijelu forme nalazi se lista u kojoj su prikazani osnovni podaci korisnika sistema. Donji dio forme služi za unos novih korisnika, kao i za ažuriranje podataka već postojećih korisnika.

Prilikom upisivanja novih korisnika, osim osnovnih podataka, unosi se slika korisnika, slika njegove dužice, kao i digitalni kod dužice. Svi podaci o korisniku smještaju se u tabelu MySQL baze podataka. Za smještanje slike



korisnika, slike dužice i koda dužice korišten je LONGBLOB tip podataka.

Podaci dužice mogu se obezbijediti na dva načina. Prvi način je skeniranjem dužice upotrebom VistaFA2 Single Iris & Face kamere. Ova opcija se pokreće selekcijom radio dugmeta Skener i klikom na komandno dugme START. Klikom na dugme STOP moguće je prekinuti proces skeniranja dužice (Slika 9). Kada se skeniranje završi, na formi se prikazuje slika dužice i generiše njen kod. Kroz odgovarajuće labele na formi, izvještava se o rezultatu skeniranja i kvalitetu dobijene slike (koda) dužice. (Slika 10).



Slika 10. Izgled aplikacije nakon uspješnog skeniranja dužice

Drugi način upisivanja podataka dužice je upotrebom već postojeće slike dužice, osobe koju se želi upisati u sistem. Opcija se pokreće tako što se selektuje radio dugme Slika. Zatim se, upotrebom OpenFileDialog komponente, iz odgovarajućeg foldera, odabere slika dužice. Odmah po odabiranju slike generiše se njen kod. Kroz odgovarajuće labele na formi izvještava se o kvalitetu odabrane slike, odnosno dobijenog koda dužice (Slika 11).

Nakon obazbjedivanja slike i koda dužice i unosa ostalih potrebnih podataka, klikom na komandno dugme Upiši, korisnik se upisuje u sistem.

U cilju ažuriranja podataka već postojećih korisnika, potrebno ih je najprije selektovati, klikom na odgovarajući zapis u listi korisnika.

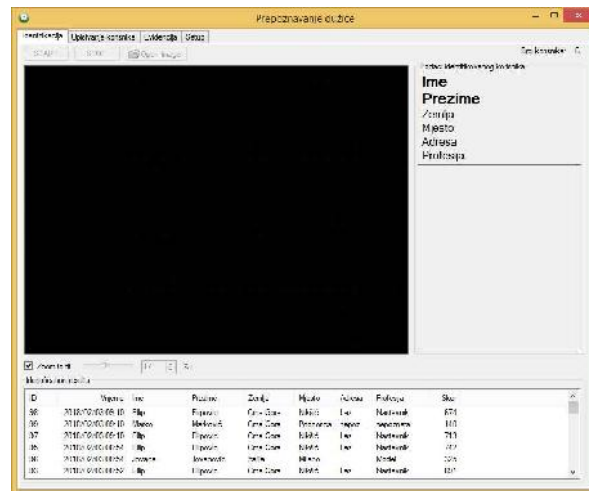
Na Slici 12 prikazan je izgled aplikacije kada ona radi u režimu identifikacije korisnika.

Slično kao i u režimu upisivanja, i u ovom slučaju moguća su dva načina dobijanja podataka dužice. Prvi način je identifikacija upotrebom VistaFA2 kamere. Ovo je primarni način, u kojem korisnik, u cilju obazbjedivanja podataka dužice, zauzima odgovarajući položaj prema kameri. Po dobijanju slike i koda dužice započinje proces poređenja sa već raspoloživim podacima u bazi. U slučaju uspješne identifikacije, na formi aplikacije se prikazuju osnovni podaci i slika prepoznatog korisnika (Slika 13). U

odgovarajuću tabelu baze podataka upisuju se podaci o tekućem vremenu, prepoznatom korisniku i stepenu podudarnosti kodova dužica. Podaci o obavljenim identifikacijama u toku tekućeg dana, prikazani su u listi u donjem dijelu forme aplikacije (Slika 13). Podaci o prepoznatom korisniku se na formi aplikacije zadržavaju predefinisano vrijeme, nakon čega ona ponovo poprima izgled prikazan na slici 12.



Slika 11. Izgled aplikacije nakon selektovanja slike dužice



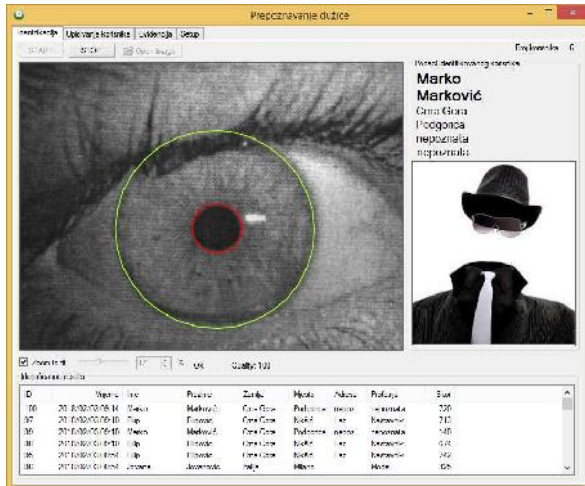
Slika 12. Aplikacija u režimu identifikacije korisnika

Drugi način identifikacije obavlja se upotrebom već postojeće slike dužice. Ova opcija se pokreće klikom na komandno dugme STOP i selekcijom slike.

Osim upisivanja korisnika i identifikacije, aplikacija omogućuje izvještavanje o izvršenim identifikacijama. Moguće je, u zadatom periodu vremena, dobiti zbirne i pojedinačne izvještaje o izvršenim identifikacijama pojedinog ili grupe korisnika

U dijelu podešavanja parametara sistema, moguće je podesiti željeni FAR (False Accept Rate), minimalni potrebni stepen podudarnosti, period zadržavanja podatka prepoznatog korisnika na formi aplikacije, parametre servera i baze podataka i dr.

Opisani identifikacioni sistem se može prilagoditi različitim primjenama. Može poslužiti kao kontrola pristupa zaštićenim prostorima, kao kontrola pristupa računarima i serverima, za identifikacije u obrazovnim i zdravstvenim ustanovama, na graničnim prelazima, aerodromima, itd.



Slika 13. Aplikacija u režimu identifikacije pomoću VistaFA2 kamere

## 5. ZAKLJUČAK

U radu je predstavljen identifikacioni sistem za prepoznavanje dužice oka. Sistem se sastoji od VistaFA2 Single Iris & Face kamere, PC aplikacije i servera sa bazom podataka. Sistem može da radi u dva režima: režimu upisivanja korisnika i režimu identifikacije. Pokazano je da se upisivanje korisnika u sistem i identifikacija mogu obaviti na dva načina: pomoću VistaFA2 kamere ili korištenjem raspoložive slike dužice. Sistem omogućuje izvještavanje o obavljanim identifikacijama. Moguće ga je prilagoditi različitim primjenama.

Osim opisa sistema, u radu su date su osnovne informacije o dužici kao biometrijskom identifikatoru. Dat je pregled tehnologije prepoznavanja dužice, kao i informacije o upotrijebljenoj biometrijskoj VistaFA2 kameri.

## LITERATURA

[1] Kronfeld, P. "Gross anatomy and embryology of the eye", H. Davson, Ed. London, U.K. Academic, 1962.

[2] Daugman, J., "High confidence visual recognition of persons by a test of statistical independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 5, pp 1148-1161, 1993.

[3] Daugman J and C. Downing, "Epigenetic randomness, complexity, and singularity of human iris patterns." Proceedings of the Royal Society, Biological Sciences, pp 1737 – 1740, 2001.

[4] Daugman, J., "How iris recognition works". IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 21–30, 2004.

[5] Daugman, J., "Information Theory and the IrisCode", IEEE Trans. Info.Foren.Sec, Vol. 11, No. 2, pp 400-409, 2015.

[6] [www.bayometric.com](http://www.bayometric.com)

[7] [www.irisguard.com](http://www.irisguard.com)

[8] [www.neurotechnology.com](http://www.neurotechnology.com)

[9] [www.cmi-tech.com](http://www.cmi-tech.com)

[10] [www.irisys.net](http://www.irisys.net)

[11] Daugman, J. And Malhas, I., "Iris recognition border-crossing system in the UAE", Reproduced from International Airport Review, Issue 2, 2004

[12] "Indian state selects iris based identity management solution by IriTech". BiometricUpdate. Retrieved 2015-11-02.

[13] [http://www.vistaimaging.com/FA2\\_product.html](http://www.vistaimaging.com/FA2_product.html)

[14] "CASIA Iris Image Database", Chinese Academy of Sciences Institute of Automation, <http://www.sinobiometrics.com>

[15] Boles, W.W. and Boashah, B., "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Transaction on Signal Processing, Vol. 46, pp 1185-1188.

[16] T. Chen, C. Amd Liang Chung, K., "An Efficient Randomized Algorithm for Detecting Circles", Computer Vision and Image Understanding, Vol. 83, pp 172-191, 2001.

[17] <http://www.cl.cam.ac.uk/~jgd1000/decidability.html>

# METOD MERENJA FAKTORA SNAGE IMPLEMENTIRAN U VATMETRU VISOKE KLASNE TAČNOSTI POWER FACTOR MEASUREMENT METHOD IMPLEMENTED IN THE HIGH-ACCURACY WATTMETER

Ljubiša Jovanović  
Institut Mihajlo Pupin Beograd

**Sadržaj** – U radu je predstavljeno rešenje za merenje faktora snage integrisano u okviru razvijenog vatmetra visoke klase tačnosti. Rešenje je bazirano na definiciji faktora snage i koristi vrednosti izmerene aktivne snage i vrednosti efektivnih vrednosti napona i struje. Potrebna izračunavanja obavlja ugrađeni mikrokontroler, a pridodato jednostavno elektronsko kolo određuje da li je opterećenje induktivno ili kapacitivno. Merna nesigurnost je u okviru  $\pm 10 \times 10^{-5}$ .

**Abstract** - The paper presents a solution for measuring the power factor integrated within developed high-accuracy wattmeter. The solution is based on the definition of the power factor and uses the value of the active power and the effective values of the voltage and current measured within the wattmeter. The required calculations are performed by a built-in microcontroller, and the added simple electronic circuit determines the load type. Measurement uncertainty is within  $\pm 10 \times 10^{-5}$ .

## 1. UVOD

Faktor snage je veličina koja ima veliki značaj u energetici i usko je vezana za elektroenergetski sistem i za prenos električne energije. U naizmeničnom električnom sistemu faktor snage PF definisan je kao odnos aktivne snage P prema prividnoj snazi S

$$PF = P/S, \quad (1)$$

kreće se u uskom opsegu od -1 do +1 i predstavlja veličinu bez dimenzije (nema mernu jedinicu). Aktivna snaga je realna snaga koju potrošač uzima iz mreže, dok je prividna snaga jednaka proizvodu efektivnih vrednosti napona i struje

$$S = U_{\text{eff}} \cdot I_{\text{eff}} \quad (2)$$

i uvek je veća ili jednaka aktivnoj snazi. U slučaju čistog otpornog opterećenja aktivna snaga jednaka je prividnoj snazi pa je u tom slučaju faktor snage jednak jedinici. U slučaju da opterećenje ima i reaktivnu komponentu (induktivnu ili kapacitivnu) tada je aktivna snaga manja od prividne snage pa je i faktor snage manji od jedan. U elektroenergetskom sistemu potrošači sa manjim faktorom snage vuku iz mreže veću struju nego potrošači sa velikim faktorom snage pri istoj aktivnoj snazi i tako stvaraju veće gubitke u prenosnoj elektroenergetskoj mreži (na prenosnim vodovima). Da bi se ovi gubici smanjili u elektroenergetskoj mreži se vrše razne vrste kompenzacija reaktivnog opterećenja kako bi se faktor snage povećao, pri čemu je od velikog značaja precizno merenje faktora snage. Pri čisto sinusoidalnim oblicima

električnih signala aktivna snaga P jednaka je proizvodu prividne snage S i kosinusa faznog ugla  $\varphi$  između naponskog i strujnog sinusoidalnog signala

$$P = S \cos \varphi, \quad (3)$$

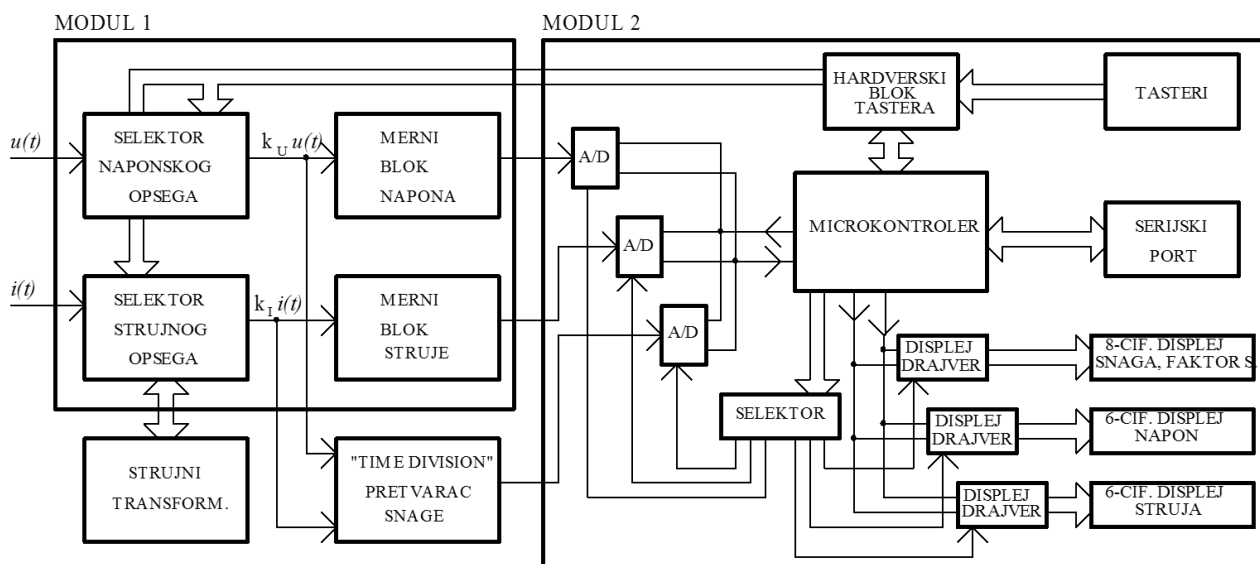
pa je u tom slučaju faktor snage PF jednak  $\cos \varphi$

$$PF = \cos \varphi. \quad (4)$$

Metode merenja faktora snage mogu biti zasnovane na dva osnovna principa. Prvi, koji koristi osnovnu definiciju pa se do rezultata dolazi merenjem prividne i aktivne snage i drugi, koji je zasnovan na merenju faznog pomeraja između naponskog i strujnog signala, pri čemu je ovaj drugi metod primenljiv samo u slučaju kada su signali napona i struje čisto sinusoidalni. Jedan od mernih uređaja koji je zasnovan na drugoj metodi predstavljen je u [1]. U ovom radu predstavljeno je praktično rešenje za merenje faktora snage, zasnovano na metodi merenja aktivne i prividne snage, a implementirano je u okviru novog razvijenog vatmetra visoke klase tačnosti [2].

## 2. IMPLEMENTACIJA REŠENJA U OKVIRU NOVOG UREĐAJA

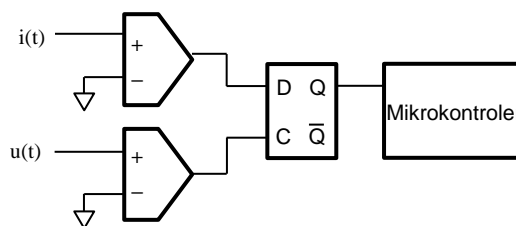
Za merenje aktivne električne snage u mnogim nacionalnim laboratorijama kao sekundarni etalon električne snage koristi se precizni merni pretvarač snage MSB-001[3] razvijen u Institutu Mihajlo Pupin u Beogradu. Ovaj merni uređaj se koristi i kao prenosni etalon za interkomparaciju nacionalnih etalona električne snage [4]. Informaciju o izmerenoj snazi ovaj merni pretvarač daje u vidu jednosmernog naponskog signala nominalne vrednosti od 10 V DC sa tačnošću od  $\pm 50 \times 10^{-6}$ . U uobičajenim laboratorijskim uslovima ovaj napon se meri preciznim digitalnim voltmetrom visoke klase tačnosti pri čemu se u procesu merenja i tačnost voltmetra uzima u obzir. U razvoj novog uređaja [2] se krenulo sa idejom da se korišćenjem modula pretvarača MSB-001 napravi precizni vatmetar tako što bi se postojećem pretvaraču dodao odgovarajući hardver koji bi merio izlazni napon i na ugrađenom displeju prikazivao vrednost izmerene snage. Pri tom, osnovni zahtev koji je novi uređaj trebalo da zadovolji bio je da njegova tačnost merenja ostane na nivou postojeće tačnosti pretvarača, odnosno  $\pm 50 \times 10^{-6}$ . Ostali postavljeni zahtevi bili su da novi vatmetar ima četiri naponska i četiri stujna opsega, i da ima još dva dodatna displeja za prikaz vrednosti napona i struje bez zahtevane tačnosti za ova merenja. Princip rada novog uređaja kao i njegove značajne merne karakteristike prikazane su u [2] ali samo u pogledu merenja snage. U toku razvoja ovoga uređaja uz određeno



Slika 1. Strukturna blok šema vatmetra

proširenje softvera i jednostavno hardversko proširenje dodatno je impementirana i funkcija merenja faktora snage. Strukturna blok šema celog uređaja prikazana je na Sl. 1. Kao što se vidi sa slike uređaj se sastoji iz tri modula. Kao najvažniji u pogledu osnovne funkcije uređaja izdvaja se modul pretvarača snage baziran na analognim elektronskim kolima i na "time-division" množaču [3]. Na njegove ulaze dovode se naponski signal i strujni signal koji su prošli kroz određene blokove za izbor i prilagođenje mernih opsega, a na njegovom izlazu generiše se jednosmerni napon proporcionalan aktivnoj električnoj snazi. Na modulu 1 (Sl. 1) nalaze se relejni blokovi za selktovanje mernih opsega kao i elektronska kola za merenje naizmeničnih signala struje i napona koja na izlazu generišu jednosmerne naponske signale proporcionalne izmerenim efektivnim vrednostima. Na modulu 2 nalaze se tri identična A/D konvertora koji mere izlazne napone pretvarača snage i naponskog i stujnog bloka, zatim odgovarajući LED displeji sa svojim drajverskim čipovima, tasteri za izbor opsega i načina rada uređaja i mikrokontroler koji očitava izbor postavljenih mernih opsega, očitava izmerene vrednosti na odgovarajućim A/D konvertorima na osnovu tih vrednosti izračunava izmerene vrednosti za snagu, napon i struju i preko odgovarajućih drajverskih kola prikazuje ih na odgovarajućim posebnim displejima. Mikrokontroler komunicira sa A/D konvertorima i sa drajverskim kolima LED displeja serijskom vezom. Upotrebljeni su 22-bitni sigma-delta A/D konvertori LTC1966. Na dva 6-cifarna manja LED displeja prikazuju se izmerene vrednosti napona i struje. Na glavnom, većem 8-cifarnom LED displeju prikazuje se vrednost izmerene snage ( u vatima ili u procentima od nominalne vrednosti selektovanih mernih opsega) ili izmerena vrednost faktora snage, što zavisi od izabranog načina rada preko odgovarajućih tastera. U slučaju da je selektovan mod merenja faktora snage, mikrokontroler na osnovu izmerenih vrednosti aktivne snage efektivne vrednosti napona i struje izračunava vrednost faktora snage prema jednakostima (1) i (2) i prikazuje ih na glavnom displeju, pri čemu ispred brojne vrednosti ispiše slovo L ili C u zavisnosti da li je

opterećenje induktivno ili kapacitivno, odnosno da li struja kasni ili prednjači u odnosu na napon. Iz očitanih vrednosti sa A/D konvertora ne može se odrediti da li struja kasni ili prednjači pa je bilo neophodno na modulu 1 ugraditi jednostavno kolo prikazano na Sl. 2 tako da softver mikrokontrolera očitavanjem stanja D flip flopa detektuje koji signal prednjači a koji kasni. U uređaju je upotrebljen



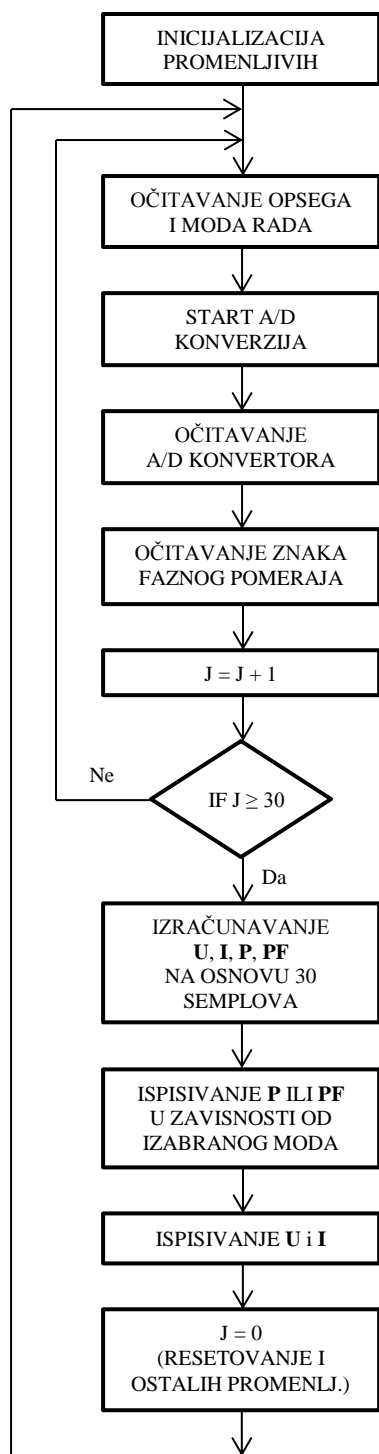
Slika 2. Kolo za detekciju znaka faznog pomeraja

Mikrokontroler PIC 18F252. Jedna odznačajnijih karakteristika mikrokontrolera serije PIC 18FXXX je mogućnost hardverskog množenja dva bajta u jednom instrukcijskom ciklusu tako da ovde brzina obavljanja potrebnih izračunavanja nije kritična.

### 3. STRUKTURA SOFTVERA

Strukturalni blok dijagram softvera prikazan je na Sl. 3. Kao što se vidi sa slike softver se sve vreme vrti u unutrašnjoj petlji u okviru koje na početku očitava selektovane merne opsege i način rada. Zatim startuje konverziju na sva tri A/D konvertora, čeka oko 80 ms koliko traje A/D konverzija i posle toga vrši očitavanje vrednosti A/D konvertora i njih dodaje sadržajima odgovarajućih registara napona struje i snage i očitava znak faznog pomeraja struje u odnosu na napon. Posle toga inkrementira promenljivu brojača J i proverava da li je obavljeno 30 uzastopnih konverzija i ako nije vraća se na početak petlje, a ako jeste, onda prema selektovanom modu rada obavlja odgovarajuća izračunavanja i prikazuje na glavnom displeju vrednost snage u vatima ili

procentima ili faktor snage sa oznakom da li se radi o induktivnom ili kapacitivnom opterećenju, a na manjim displejima prikazuje vrednosti napona i struje. Na kraju resetuje promenljivu brojača J i druge odgovarajuće promeljive i vraća se na početak petlje.



Slika 3. Strukturni blok dijagram softvera

Dakle vrednosti koje se prikazuju na ekranu su usrednjene vrednosti na osnovu 30 uzastopnih vrednosti očitanih sa odgovarajućih A/D konvertora. Ovo usrednjavanje se vrši za sve merene veličine. Kako je trajanje konverzije oko 80 ms, tako se osvežavanje displeja novim vrednostima vrši za nešto manje od 3 s. Na Sl. 4 prikazana je prednja

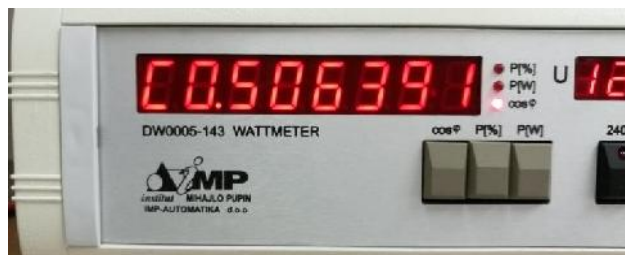
strana uređaja. Na Sl. 5 i Sl. 6 prikazan je izgled glavnog displeja pri merenju faktora snage i to pri induktivnom i pri kapacitivnom opterećenju.



Slika 4. Izgled prednje strane uređaja



Slika 5. Merenje faktora snage – induktivno opterećenje



Slika 6. Merenje faktora snage – kapacitivno opterećenje

#### 4. ZAKLJUČAK

Proširenjem softvera i dodavanjem jednostavnog elektronskog kola u vatmetru visoke klase tačnosti ( $\pm 50 \times 10^{-6}$ ) implementirana je funkcija merenja faktora snage po metodi baziranoj na definiciji. Ostvarena je tačnost od  $\pm 50 \times 10^{-5}$ . Ova tačnost je za red veličine manja od tačnosti merenja snage, meduim i pored toga ovim je značajno proširena mogućnost primene uređaja

#### LITERATURA

- [1] Jovanović, Lj. “ Precizni pretvarač faznog pomeraja strujnog signala u odnosu na naponski signal u elektroenergetskoj mreži“, Zbornik radova, YU INFO, Kopaonik, 2013.
- [2] Jovanović, Lj. “A Novel TDM-Based High-Precision Wattmeter“, IEEE Transactions on instrumentation and measurement, Vol. 66, No. 6, June 2017.
- [3] Miljanić, P., Stojanović, B. and Bošnjaković, P. “The Development of High-Precision Time-Division Power Meter“, Conference Digest, CPEM, pp. 67-68, Aug. 1984.

- [4] Moore, W., So E., Oldham, N., Miljanić, P. and Bergeest, R. “An international comparison of power meter calibrations conducted in 1987,” IEEE Transactions on Instrumentation and Measurement, Vol. 38, pp. 395-401, April 1989.



# RIZICI KORIŠĆENJA ANDROID APLIKACIJA ANDROID APPLICATIONS RISK

Mirko Kosanović<sup>1</sup>, Miloš Kosanović<sup>1</sup>, Vesna Kosanović<sup>2</sup>

<sup>1</sup> *Visoka tehnička škola strukovnih studija u Nišu*

<sup>2</sup> *Ekonomska škola u Nišu*

**Sadržaj** – Veliki napredak bežičnih komunikacionih tehnologija kao i sve veća računarska snaga kao i gabaritno smanjivanje računarskih komponenti, doprinele su do masovne primene mobilnih uređaja. Oni su danas postali gotovo sastavni deo ljudskog življenja ali su i svojom računarskom snagom gotovo u potpunosti zamenili standardne desktop računare ili laptopove. Brojni mobilni uređaji, kao što su BlackBerries, iPhones i uređaji koji rade pod Android operativnim sistemom, koji se izborio kao vodeći operativni sistem, naparavili su pravu revoluciju na svetskom tržištu. U ovom radu ukazano je na neke od opasnosti koje vrebaju kod korišćenja ovog operativnog sistema. Na nekoliko primera prikazano je kako je moguće neovlašćeno pristupiti nekom mobilnom uređaju pod Android operativnim sistemom i zloupotrebiti njegove mogućnosti.

**Abstract** - *The great advancement of wireless communication technologies, as well as the increasing computing power, as well as the downsizing of computing components, have contributed to the massive use of mobile devices. Today they have become almost an integral part of human life, but with their computer power almost completely replaced standard desktop computers or laptops. Numerous mobile devices, such as BlackBerries, iPhones and devices operating under the Android operating system, which fought as the leading operating system, have made a real revolution in the world market. This paper presents some of the dangers that lurk when using this operating system. A few examples show how it is possible to unauthorized access to a mobile device under the Android operating system and abuse its capabilities*

## 1. UVOD

Svedoci smo sve većeg prodora mobilnih uređaja koji postaju sastavni deo naših života. Oni su preuzeli primat u odnosu na gotove sve ostale uređaje kojima smo se do sada služili tj. komunicirali sa svetom ili pamtili važne podatke. Ubrzani razvoj Interneta kao i mogućnost da se na njega povežemo gotovo na svakoj tački zemljine kugle, promenili su način na koji ljudi međusobno komuniciraju i rešavaju svoje probleme, informišu se o raznim događajima, kupuju ili plaćaju različite račune, putuju do nepoznatih mesta ili se zabavljaju. Gabaritno jako mali, pouzdani i jednostavni za rukovanje omogućili su da gotovo trenutno dođemo do ogromne količine podataka. Samim tim možemo slobodno da kažemo da su danas mobilni uređaji postali gotovo neizostavni deo našeg življenja. Oni se koriste 24 h dnevno i 365 dana u godini, kako u svakodnevnom životu, tako i u poslovnim primenama. Ono što još više uzbuđuje to je da velikom

brzinom raste i broj drugih pametnih uređaja poput automobila, satova, TV uređaja, frižidera, šporeta i td., kojima možemo pristupiti putem Internet veze. Nismo daleko od vizije mnogih naučnika koji su predviđali da će u budućnosti gotovo svaki uređaj biti adresibilan i dostupan putem Internet veze – *Internet things*. Time se ostvaruje proročanstvo mnogih naučnika krajem XX veka a to je da osnovni zahtev klijent-server arhitekture 3A: **Any one** (bilo ko), **Any place** (bilo gde) i **Any time** (bilo kada), duplira i preraste u 6A: **Any thing** (bilo šta), **Any path/network** (na bilo koji način) i **Any service** (bilo koji dostupan servis) [1]. Prema istraživanju koja je uradila američka kompanija “A10 Networks” poslovne i lične aplikacije na mobilnim uređajima su postale sastavni i svakodnevni deo naših života na globalnom nivou tako da mnogi veruju da je nemoguće živeti i funkcionisati bez njih. Savremena poslovna komunikacija gotovo da se ne može ni zamisliti bez mobilnih uređaja. Oni se mogu koristiti i kao pomoćna sredstva za proveru identiteta (autentifikacija korisnika), kao sredstvo za plaćanje, sredstvo za lociranje i navigaciju, pristup različitim lokacijski baziranim uslugama uz pomoć GPS (*Global Position System*). Mnogi su mišljenja da su oni postali naša životna potreba bez koje više ne možemo da živimo i upoređuju ih sa osnovnim potrebama ljudi kao što su voda, hrana, disanje ili druženje sa prijateljima [2].

Međutim, zbog masovne upotrebe mobilnih uređaja postavljaju se i razna pitanja koja su vezana za integritet i stepen pouzdanosti kako podataka tako i korisnika ovih uređaja. Nemaran stav prema mobilnom uređaju i njegovom korišćenju, može dovesti do katastrofalnih posledica u vidu narušavanja privatnosti vlasnika, krađom njegovog identiteta, gubitkom intelektualne svojine, materijalnih gubitaka ili raznih drugih neprijatnosti. Kako je zavisnost od mobilnih uređaja veća to je i rizik od neke neprijatnosti veći. Svedoci smo da svakog dana nivo mnogobrojnih bezbednosnih pretnji za ove uređaje i njihove aplikacije gotovo eksponencijalnom brzinom raste. Zato je neophodno da se kontinuirano prati i povećava potreba uvođenja većeg nivoa zaštite integriteta informacija koje se razmenjuju i smeštaju u ovim uređajima. Neželjeni faktori koji utiču na bezbednost komunikacionog kanala manje su izraženi u uređajima koji koriste neki od korisnički orjentisanih operativnih sistema. Brojniji napadi na bezbednosni sistem kod *smart* telefona i veća učestalost napada dešava se prilikom prihvatanja, preuzimanja i slanja podataka odobrenih od strane korisnika [3]. Međutim, činjenica je da mnoštvo napada u ovim sistemima nije ni primećeno, niti registrovano od strane korisnika, a posledice mogu biti značajne. Tako recimo može doći do usporenog rada mobilnog uređaja, odnosno operativnog sistema (*OS*), do gubitka bitnih podataka ili otkrivanja važnih informacija i



lokacija. Zato je proučavanje sigurnosnih mehanizama u mobilnim uređajima od primarnog značaja jer može dovesti do razvoja svesti korisnika o povećanju sigurnosti podataka u njima, jer su sami korisnici svojom nepažnjom u najvećem broju slučajeva indirektni inicijatori napada.

U ovom radu nakon uvoda u problem u poglavlju 2, biće ukratko prikazani kakvi sve napadi prete mobilnim uređajima i izvršice se njihova klasifikacija. U poglavlju 3 razmatrani su sigurnosni mehanizmi jednog od najpopularnijih operativnih sistema Android. U poglavlju 4 dat je pregled dostupnih programskih paketa preko kojih je moguće zloupotrebiti sadržaje koji se nalaze na mobilnim uređajima ("hakerisati" mobilni uređaj). U poglavlju 5 prikazan je jedan od tih mnogobrojnih programa i prikazano je kako na jedan vrlo jednostavan način možete zloupotrebiti tuđi mobilni uređaj. Poglavlje 6 zaključuje ovaj rad i daje neke preporuke kojih se treba držati kod korišćenja mobilnih uređaja.

## 2. VRSTE NAPADA NA MOBILNI UREĐAJ

Svedoci smo da mobilni uređaji velikom brzinom preuzimaju primat u odnosu na ostale klasične vidove komunikacije preko računara ili fiksnog telefona. Popularnost mobilnih uređaja i aplikacija, kao njihova svakodnevna upotreba, su u stalnom porastu. Svakog dana raste broj mobilnih aplikacija koje pristupaju mnogim podacima koji se nalaze na našim telefonima a da pri tome ne nude nikakvo obaveštenje niti o razlogu pristupanja niti o načinu na koji će se ti preuzeti podaci kasnije koristiti. Kako pokazuju nedavno objavljeni rezultati istraživanja u ovoj oblasti, zaštita privatnosti korisnika nije prioritet većine autora mobilnih aplikacija. Prema istraživanju koje je sproveo Kanadski komeserijat za privatnost (*Office of the Privacy Commissioner of Canada*), 85% analiziranih mobilnih aplikacija ne obaveštava korisnika na jasan način kojim podacima o ličnosti se pristupa a svega 15% jasno obaveštava korisnika o svom odnosu prema njegovoj privatnosti[4]. Ako uzmemo u obzir da se danas u telefonima nalazi veoma velika količina privatnih podataka kao što su: telefonski imenik, fotografije, informacije o pozivima (Call detail), kalendar sa događajima, E-mail, SMS/MMS, slike, audio i video zapisi, Internet History, dokumenta preuzeta sa interneta, GPS lokacije i td., jako je bitno da se posveti posebna pažnja na sigurnost i bezbednost svih tih podataka tj. naših mobilnih uređaja.

Dodatan problem i još veću opasnost po bezbednost mobilnih uređaja donela je pojava pametnih telefona (smartphones). Mnoge razvojne kompanije, kao i mrežni operateri, nastoje da razviju nove multimedijalne aplikacije koje mogu iskoristiti prednosti novih moćnih mobilnih uređaja koji sve više objedinjuju funkcije tradicionalnog mobilnog telefona i PC računara u jednom uređaju. Već duži niz godina telefoni nisu samo uređaji kojima se samo vrši glasovna komunikacija. Danas, oni podržavaju razmenu tekstualnih i multimedijalnih poruka, slanje email-ova, web surfovanje, audio i video transmisijske, i mnogo drugih aplikacija. Sa ovim transformacijama i novim funkcionalnostima pojavila se potreba za sofisticiranijim mobilnim operativnim sistemima. Oni su omogućili i korišćenje velikog broja

besplatnih programa koje se mogu preuzeti i koristiti sa mnogih sajtova na Internetu. Omogućavaju pokretanje više programa istovremeno (multitasking) i kao takvi predstavljaju prave male računare, smeštene u minijaturno kućište. Zadnjih godina na tržištu su se, između ostalih, posebno istakli "Android", "IOS" i "Microsoft" operativni sistemi. U poslednjih godinu-godinu i po dana, Android uređaji (mobilni telefoni pre svega, a u skorije vreme i tableti) su preplavili domaće tržište. Otvorenost, veliki izbor aplikacija i mogućnosti koje pruža Android je ono što ga je učinilo toliko popularnim. Ovako brza ekspanzija je dovela do toga da mnogi novi korisnici nisu svesni svih aspekata korišćenja Android mobilnih uređaja, uglavnom zbog nedostatka potrebe za određenim funkcionalnostima. Na žalost, bezbednost spada u tu kategoriju, i to uglavnom kod korisnika kojima tehnika "nije jača strana". Operativni sistemi omogućavaju instaliranje velikog broja aplikacija za komunikaciju koje ne koriste standardnu GSM mrežu, kao što su Skype, Viber i sl. Pored toga, omogućavaju korišćenje mesendžer programa za slanje i primanje kratkih poruka koji mogu da koriste i neke druge izvore Internet saobraćaja kao što je WiFi i sl. Takav način komunikacije uveliko ugrožava sigurnost i bezbednost podataka koji se u komunikacijama razmenjuju.

Postoji jako veliki broj potencijalnih pretnji koje mogu da ugroze kako sigurnost i bezbednost podataka tako i sam hardver mobilnih uređaja. Broj tih pretnji raste svakog dana tako da se sa pravom postavlja pitanje koliko je komunikacija između mobilnih uređaja sigurna? Sve napade, odnosno potencijalne pretnje na komunikacioni kanal mobilnih uređaja, možemo prema strukturi tih napada tj. kako se taj napad izvodi i šta se napada podeliti u tri velike grupe i to[5]:

1. **Hardverski orijentisani napadi** – podrazumevaju jedan širi opseg napada na bezbednost mobilnih uređaja koji modifikuju postojeći hardver mobilnih uređaja i na osnovu toga omogućavaju ili onemogućavaju neke skrivene radnje nad njim. Kako zahtevaju fizički pristup hardveru mobilnog uređaja ove napade nije jednostavno sprovesti jer zahtevaju fizičko posedovanje mobilnog uređaja. U neke od poznatijih napada ove vrste spadaju upotreba TurboSIM kartice kojom se vrši dekodiranje mobilnih telefona ili korišćenje JTAG ( Joint Test-Action Group) interfejsa koji se koristi kod digitalne forenzike mobilnih uređaja pre svega memorije i SIM kartice mobilnih uređaja [6]
2. **Tipski nezavisni napadi** - spadaju u napade kojima je osnovni cilj da direktno naruše sistem zaštite mobilnih uređaja i da na taj način omogućе neku zloupotrebu tj. krađu nekih podataka. Ovi napadi koriste pojedine slabosti u softveru koji se izvršava na mobilnom uređaju i umeću svoj programski kod poznat pod imenom Back door. Back door je program koji omogućava trećim osobama nesmetan i neovlašćen pristup mobilnom uređaju koristeći slabosti OS ili nekog drugog programa. Potencijalni napadač uz pomoć odgovarajuće opreme prisluškuje komunikacioni kanal između dva korisnika, detektuje pojedinačne slabosti, ubacuje se u kanal i ima neometanu mogućnost modifikovanja, tj. narušavanja integriteta podataka. Ovakvi napadi ne zavise od tipa ili vrste uređaja.

**3. Korisnički orijentisani napadi** - koriste slabosti samih korisnika mobilnih uređaja koji ili neznaju ili pogrešno koriste mehanizme zaštite svojih uređaja. Postoje mnogi maliciozni programi za mobilne uređaje koji koriste sigurnosne propuste koji nisu tehničke, tj. programske prirode. Svojim pokretanjem izvršavaju niz korisničkih neovlašćenih procesa. Zbog svoje prirode zaobilaze sigurnosne mehanizme čime povećavaju nivo ranjivosti operativnog sistema. Softverskih napada ima više vrsta. Dešavaju se izvršavanjem malicioznih programa, ili krađom identiteta mobilnog pretplatnika (špijunaža). Ovi napadi najčešće mogu biti finansijski motivisani. Moguće ih je realizovati preko botnet mreža ili uz pomoć DoS napada na mobilne uređaje. Botnet mreža predstavlja skup međusobno povezanih računara kojima upravlja jedna osoba, ili više njih, u cilju zlonamernog delovanja na komandnu datoteku koja služi za lakše prisvajanje kontrole nad uređajem, kao i njegovim uključivanjem u botnet mrežu. Napadi se mogu izvršiti i preko određenih servisa mobilne telefonije kao što su SMS, MMS, EMS, GPRS, preko mobilnog Internet pretraživača, korisnički instaliranog zlonamernog softvera kao i antivirusnog sistema za zaštitu. Ciljevi ovih napada svode se na: prisluškivanje mobilnih uređaja, onemogućavanje korišćenja mobilnih uređaja blokiranjem komunikacije, narušavanje privatnosti tj. zlonamerno korišćenje tuđeg ID mobilnog uređaja u cilju lažnog predstavljanja i smanjivanja vlastitih finansijskih troškova.

### 3. ANDROID BEZBEDNOSNI PROBLEMI

Jedna od manje poznatih oblasti kada je Android operativni sistem u pitanju je njegova arhitektura zaštite. Često se sa razlogom postavlja pitanje kako i koliko ovaj operativni sistem štiti aplikacije, podatke i korisnike od napada, ili eventualnih sopstvenih grešaka. Da bi postao jedan od najsigurnijih mobilnih operativnih sistema, Android teži da redefiniše nivo sigurnosnih kontrola koje koriste tradicionalni operativni sistemi. U cilju zaštite korisničkih podataka, sistemskih resursa (uključujući i mrežne resurse) uključeni su sledeći bazični sigurnosni mehanizmi [7]:

- veoma jaka zaštita na nivou operativnog sistema, putem Linux kernela;
- obavezna izolacija pri pokretanju svih aplikacija (Sandbox);
- sigurna komunikacija između aktivnih procesa, pri čemu je definisana dozvola od strane korisnika ili same aplikacije.

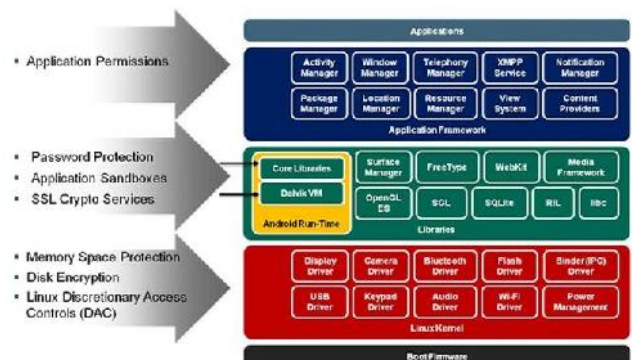
Kao osnove na kojima se Android uređaji baziraju mogu se navesti Linux kernel, sistemske biblioteke u sloju iznad njega, Android runtime u okviru kojeg se izvršavaju Delvik virtualna mašina i na kraju Application Framework komponente u Java programskom jeziku namenjene programerima u razvoju aplikacija. Pored činjenice da se u velikoj meri oslanja na procesorsku snagu, Android koristi i bezbednosne mogućnosti koje su usko vezane za hardver kao što je ARM v6 eXecute-Never9. Svim dostupnim hardverskim resursima (kamera, GPS, Bluetooth i dr.) pristupa se isključivo putem

operativnog sistema u čijoj se osnovi nalazi Linux kernel zadužen za upravljanje hardverskim komponentama, uređajima, memorijom i procesima.

Na Android sistemima zastupljene su dve vrste aplikacija: one koje dolaze uz Android (core) i one koje korisnici sami instaliraju. Android aplikacije su pisane u Java programskom jeziku i startuju se uz pomoć Dalvik virtualne mašine. Ova virtualna mašina predstavlja specifično okruženje koje je namenjenog izvršavanju Java aplikacija na Androidu. Veliki broj aplikacija, uključujući i servise koji raspolazu resursima sistema, predstavljaju samostalne Android aplikacije. Dalvik virtualna mašina zajedno sa Android aplikacijama radi u istom bezbednosnom okruženju. Aplikacijama se pridružuje njihov (privatni) deo fajl sistema kojim mogu da upravljaju i upisuju privatne podatke.

Jedan od uslova za uspešno implementirano rešenje bezbednog modela ogleđa se i u njegovoj jednostavnosti upotrebe. Osnovni zadatak dobro projektovanog rešenja je da krajnji korisnici u radu što manje osećaju prisustvo kriptografskog sistema. To podrazumeva jednostavnost posla koji obavljaju, statičnost postojećih funkcija i minimum vremenskog perioda potrebnog za obavljanje konkretnog poslovnog zadatka. Model implementacije bezbedonosnog rešenja komunikacionog kanala obezbeđuje odličan metod za zaštitu osetljivih podataka koji se prenose od predajne do prijemne strane. Uslovljavanjem modela dolazi do pada nivoa performansi i do otežavanja konkretne upotrebe predloženog sigurnosnog rešenja.

Princip izolacije je jedan od zaštitnih mehanizama na kojima počiva Android. Svi vitalni segmenti sistema su međusobno odvojeni iz sigurnosnih razloga, što je vidljivo iz priloženog prikaza arhitekture sistema prikazane na Slici 1. Izolacija kao izuzetno efikasna forma zaštite nadovezuje se na osnovni bezbednosni princip koji predstavlja sam Linux kernel. Godinama unazad Linux kernel se koristi u velikom broju "osetljivih" okruženja. Kroz svoju istoriju konstantno istraživan, napadan i "krpljen" od strane velikog broja programera, Linux je postao izuzetno stabilan i siguran kernel kome poverenje pružaju mnogi značajni sistemi.



Slika 1. Arhitektura zaštite Android OS [8]

Svaka aplikacija za Android operativni sistem je upakovana u .apk arhivu, datoteka koja je slična .jar arhivi. Android aplikacije su pisane u Java programskom jeziku i bazirane su na API funkcijama koje su implementirane u SDK (Software Development Kit) u Android razvojnom okruženju. Nekoliko bezbednosnih

mehanizama su takođe sastavni delovi Android radnog područja koji mogu biti klasifikovani u tri glavne grupe. To su: Linux mehanizmi, razvojno okruženje i Android specifični sigurnosni mehanizmi (Tabela 1.) [9].

Ključne osobine zaštite koje Linux kernel obezbeđuje Android platformi su sledeće:

1. sistem dozvola za korisnike na sistemu;
2. pomenutu izolaciju procesa;
3. proširivi mehanizam za bezbednu komunikaciju između procesa;
4. mogućnost da sam obriše nepotrebne ili potencijalno nesigurne delove kernela.

Kako Android predstavlja višekorisnički operativni sistem, osnovna ideja je da se jedan korisnik, njegov prostor kao i podaci i aplikacije u potpunosti izoluju od drugog korisnika na sistemu. Ova logika isključuje korišćenje podataka koji pripadaju drugom korisniku i potencijalno narušavanje tuđeg radnog memorijskog prostora. Memorija za rad i deo procesorskog vremena su takođe rezervisani za sve trenutne konkurentne korisnike, tako da i kod korišćenja ostalih resursa postoji potpuna izolacija. Treba napomenuti i da su particije na Android sistemu podešene kao read-only, tako da kada korisnik podigne sistem u safe modu dostupne su mu samo core (ugrađene) aplikacije.

Tabela 1. Android sigurnosni mehanizmi

Mehanizam	Opis	Bezbednosni problem
<b>LINUX MEHANIZMI</b>		
<b>POSI korisnici</b>	Svaka aplikacija pristupa sa različitim ključevima.	Osigurava jedinstvenost upotrebe aplikacije
<b>Pristup podacima</b>	Direktorijum instalirane aplikacije je dostupan samo toj aplikaciji.	Osigurava pravo pristupa podacima.
<b>RAZVOJNO OKRUŽENJE</b>		
<b>Upravljanje memorijom</b>	Svaki proces je pokrenut u vlastitom prostoru.	Izvršavanje dozvola i otkrivanje informacija.
<b>Tip sigurnosti</b>	Izvršavanje u skladu s određenim formatom.	Kontrola punjenja memorij. bafera.
<b>Bezbednosne funkcije mob.operatera</b>	Upotreba SIM kartice za proveru autentifikacije.	Smanjenje krađe telefon. poziva.
<b>ANDROID SIGURNOSNI MEHANIZMI</b>		
<b>Korisničke dozvole</b>	Svaka aplikacija izjašnjava se dozvolom za izvršenje procesa.	Manja mogućnost izvršenjamalicioznih programa
<b>Izvršavanje komponenti</b>	Svaka komponenta u aplikaciji poseduje određeni nivo vidljivosti koji određuje pravo pristupa druge aplikacije	Ograničava upotrebu jedne aplikacije od strane druge i pristup određenim komponentama.
<b>Potpisivanje aplikacija</b>	APK datoteke su programski potpisane i overene.	Proverava da li dve aplikacije imaju istog vlasnika.
<b>Dalvik VM</b>	Svaka aplikacija se pokreće u vlastitom virtuelnom procesu.	Kontroliše mem. bafer, izvršavanje koda i gašenja procesa.

#### 4. PROGRAMI ZA NAPAD NA ANDROID

Sa porastom upotrebe mobilnih uređaja rasli su zahtevi koji su se pred njima postavljali. To je sa jedne strane doprinelo ogromnom razvoju velikog broja aplikacija za mobilne uređaje tako da prema izvoru [10] na Google Play marketu (najpopularniji sajt za preuzimanje Android aplikacija) trenutno je dostupno preko 3 500 000 (3,633,232 na dan 03.02.2018 god.) različitih aplikacija koje se mogu preuzeti. Ali zbog velikog broja potencijalno opasnih aplikacija, samo u toku 2017. godine, Google je iz Play Store-a uklonio preko 700.000 aplikacija, kao deo inicijative da se zaštite Android korisnici. Google je na svom blogu objavilo da su uklonjene aplikacije koje su ugrožavale Google Play polisu i uslove korišćenja, a uklonjeno je 70 procenata više aplikacija nego što je to bio slučaj tokom 2016. godine. U pitanju je ogromna količina, posebno kada se zna da je tokom 2012. godine ukupan broj aplikacija na Google Play Store-u bio nešto preko 700.000 [11]. Interesantan je i podatak da je Google 99% aplikacija sa malicioznim ili napadnim sadržajem identifikovao i odbio pre nego što ih je bilo ko instalirao. Koliko Goole polaže na bezbednost i sigurnost svojih aplikacija govori i podatak da je on razvio novi metod detekcije i tehnike koje mogu da identifikuju one koji učestalo krše polise, kao i developere koji postavljaju uvredljiv sadržaj. Ovo je rezultiralo time da je tokom prošle godine sa servisa skinuto preko 100.000 loših developera [11].

Međutim pored ovih potencijalno opasnih aplikacija na Internetu se mogu pronaći i veoma velik broj različitih programa preko kojih se može narušiti privatnost mobilnih uređaja i zloupotrebiti njihovo korišćenje. U daljem tekstu ovog rada navešćemo samo neke od tih programa jer njihov broj stalno raste tako da je nemoguće izvršiti neki detaljniji pregled i prikaz svih dostupnih aplikacija. Generalno sve te aplikacije možemo podeliti u tri velike grupe i to su:

1. Aplikacije koje se koriste za špijuniranje tj. hakovanje tuđih razgovora – one nose jedinstven naziv *SpyApps* i one daju sve podatke koji su vezani za razgovore ili poruke koje potiču sa mobilnog uređaja na kome se ove aplikacije izvršavaju. Među ovim aplikacijama ističu se: The TruthSpy, mSpy, SpyEra, Copy9 i td.
2. Aplikacije koje služe za hakovanje Wi-Fi mreža – omogućavaju raspolaganje administratorskih prava nad nekom Wi-Fi mrežom tj. otkrivanje šifre za priključenje na mrežu i hakovanje ostalih korisnika u toj mreži. U programe koji nam to omogućavaju spadaju: dSploit, WiFi killer, Interceptor-ng, Droidsheep, FaceNiff, zANTI, Router Keygen i ostali.
3. Aplikacije za analiziranje saobraćaja – ovi programi imaju popularan naziv Packet sniffing i omogućavaju presretanje i uvid u kompletan saobraćaj koji se odvija između mobilnih uređaja u nadgledanoj mreži. Ove aplikacije se mogu koristiti za najrazličitije namene, od dijagnostike sigurnosnih problema pa sve do ometanja rada mreže. Kako su ovi programi dosta složeni za pravilnu primenu, pre svega zbog obilne dokumentacije i literature koju treba filtrirati i izdvojiti za ono što je

primenljivo na konkretnu/specifičnu mrežu, ova vrsta programa je namenjena računarskim profesionalcima. To se pre svega odnosi na mrežne administratore koji ove aplikacije primenjuju za posmatranje rada mreže kao i proveru sigurnosnih postavki u njoj. Pored omiljene aplikacije WireShark sve više se koristi i Interceptor-NG zbog svojih naprednih mogućnosti koje su prilagođene Android operativnom sistemu.

Navešćemo i neke od najpopularnijih aplikacija koje se koriste za "hakovanje" mobilnih uređaja, a koje je objavio sajt *Tech Viral* [12]:

- *Wps connect* – Android aplikacija namenjena root-ovanim telefonima. Omogućava da hakujemo bilo koju Wi-Fi mrežu, da se konektujemo na bilo koju lozinkom zaštićenu mrežu kao i da blokirati druge korisnike na istoj mreži.
- *Wi-Fi Wps Wpa Tester* – smatra se za najboljom aplikacijom za hakovanje Wi-Fi mreža. Omogućava povezivanje na određene osetljive/ranjive rutere u mreži.
- *Wi-Fi Kill* – omogućava blokiranje svih uređaja koji su trenutno povezani na istu Wi-Fi mrežu kao i blokiranje Interneta i korisnika koji žele da se zakače na tu mrežu.
- *Wi-Fi Inspect* – ova aplikacija je namenjena naprednim korisnicima i služi za nadgledanje Wi-Fi mreža i praćenje njihove bezbednosti. Ne može se koristiti za hakovanje.
- *Network Spoofer* – spada u bolje aplikacije koje omogućavaju testiranje i proveru bezbednosti na Android uređajima. Daje nam informacije o stepenu zaštite neke Wi-Fi mreže kao i podatke o tome koliko je lako hakovati neku Wi-Fi mrežu.

## 5. PRIMER BEZBEDONOSNOG NAPADA

Za potrebe ovog rada uradili smo jedan eksperiment kako bi se uverili kolika je stvarna bezbednost naših mobilnih uređaja. Kao primer nismo uzeli neku od dostupnih aplikacija koje se nude na tržištu već smo koristili Msfvenom, standardni alat koji se nalazi u Kali Linux-u. Ovaj alat je poznat kao alat koji se tipično koristi za napad na Android sisteme. On predstavlja kombinaciju Msfpayload i Msfencode alata, stavljajući oba ova alata u jednu okvirnu instancu. Ima širok spektar dostupnih opcija a osnovne prednosti su da je to sada jedan jedinstveni alat, ima standardizovane opcije iz komandne linije i povećana je brzina izvršavanja. Ranije se koristio napad pomoću METASPLOIT-a iz Kali Linux-a, ali je sada u potpunosti prevaziđen i zamenjen MSFvenom. Mi smo koristili Kali Linux ver. 2016.2 operativnog sistema, a napad je izvršen na mobilni telefon na kome je radio Android ver. 6.01. Važno je još da se napomene da se napad može izvesti samo pod uslovom da su napadač i žrtva korisnici jedne iste mreže.

Da bi se napad sproveo potrebne su nam IP adresa računara sa koga se napad sprovodi i IP adresa računara koji se napada. Nakon toga naredni korak je formiranje aplikacije koja će se instalirati na napadnuti računar i koja će omogućiti da preuzmemo kontrolu nad tim računarnom (back door program). U tu svrhu koristili smo sledeću komandu, kao što je prikazano na Slici 2.

```
msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.1.25 LPORT=555 R>/root/Desktop/
YUInfo.apk
```

Slika 2. Pravljenje Back door programa

Ovde se zadaje IP adresa računara sa koga se vrši napad, zatim adresa porta preko koga će se odvijati komunikacija i ime Back-door aplikacije kojoj smo mi dali ime YUInfo.apk. Nakon što smo uspešno kreirali .apk datoteku, moramo nabaviti odgovarajući sertifikat jer Android mobilni uređaji ne dozvoljavaju instaliranje nesertifikovanih aplikacija. Android uređaji instaliraju samo potpisane .apk datoteke. Da bi smo to uradili potrebno je prijaviti novo kreiranu .apk datoteku u Kali Linux koristeći sledeće alate: **keytool**, **jar signer** i **zipalign** (potrebno ga je naknadno instalirati u okviru Kali Linux-a). Taj postupak prikazan je na Slici 3:

```
keytool -genkey -v -keystore my-release-key.Keystore -
alias YUInfo -keyalg RSA -keysize 2048 -validity 10000
```

```
 jarsigner -verbose -sigalg SHA1withRSA -digestalg
SHA1 -keystore my-release-key.Keystore
/root/Desktop/YUInfo.apk YUInfo
```

```
 jarsigner -verify -verbose -certs
/root/Desktop/YUInfo.apk
```

```
 zipalign -v 4 /root/Desktop/YUInfo.apk
/root/Desktop/Android.apk
```

Slika 3. Sertifikovanje aplikacije YUInfo.apk

Naredni korak u izvođenju napada je detektovanje IP adrese žrtve napada. Takođe, u ovom koraku vrši se slanje sertifikovanog fajla za napad (Android.apk) na email adresu žrtve napada koja je prethodno pribavljena. IP adresu potencijalne žrtve napada dobićemo zadavanjem sledeće komande prikazane na Slici 4:

```
nmap -sP 192.168.0.0-255
```

Slika 4. Nabavljanje IP adrese potencijalne žrtve

Ova komanda daje listu IP adresa uređaja koji su trenutno povezani na dati mrežni opseg, tj. mrežu na kojoj se izvodi napad. Nakon što se ustanovi IP adresa uređaja koji želi da se napadne (odabrali smo da to bude uređaj sa adresom 192.168.1.50), potrebno je aplikaciju Android.apk pokrenuti na njemu. Najjednostavnije je da se fajl Android.apk pošalje na E-mail uređaja koji želi da se napadne. Kad žrtva dobije E-mail potrebno je da aktivira primljeni fajl. U međuvremenu je napadač je odradio podizanje metasploit framework konzole kucanjem komande **msfconsole**. Tako su startovani Msfconsole a samim tim i Metasploit, kao što je prikazano na Slici 5.



Slika 5. Pokretanje Metasploita



Zadnji korak je otvaranje i podešavanje **multi/handler-a**, odnosno ubacivanje parametara žrtve i napada kao što je prikazano na Slici 6.

```
msf > use multi/handler
msf exploit(handler) > set payload android/
meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.50
msf exploit(handler) > set RPORT 555
msf exploit(handler) > exploit
```

Slika 6. Podešavanje multi/handler-a

Payload Handler je pokrenut pod pretpostavkom da je žrtva ranije pokrenula aplikaciju za napad (MAIN ACTIVITY). U suprotnom napad (meterpreter session) će biti moguć tek kada žrtva otvori, odnosno pokrene aplikaciju koju je prethodno putem E-maila dobila. Kada se ta veza između Kali Linuxa i napadnutog mobilnog telefona uspostavi sledi prikaz raspoloživih komandi za napad. Moguće je komandom **help**, Slika 7., dobiti spisak komandi koje su nam na raspolaganju. Primeri napada koji se izvode mogu biti snimanje i slikanje sa web kamere žrtve, preuzimanje kontakata iz uređaja, zatim skidanje podataka iz memorije uređaja, sms poruka i sl.



Slika 7. Pregled raspoloživih opcija

Na Slici 8. prikazani su primeri preuzimanja svih SMS poruka i kontakata iz imenika pomoću komandi **dump\_sms** i **contacts\_dump**.



Slika 8. Preuzimanje poruka i kontakta

## 6. ZAKLJUČAK

Ovaj rad je pokušaj da se ustanovi koliko su naši mobilni uređaji, kao i podaci, koji rade pod Android operativnim sistemom stvarno bezbedni i sigurni. Putem jednog jednostavnog primera prikazano je kako se mogu neovlašćeno prikupiti podaci sa drugih telefona koji se kasnije mogu zloupotrebiti. Dat je i pregled dostupnih programa koji se mogu koristiti za "hakovanje" tuđih

telefona. Mnogi od ovih aplikaciju su besplatni ali postoje i komercijalne aplikacije koje se nude na tržištu. Izučavanjem ove problematike došli smo do zaključka da "hakovanje" tuđih telefona više nije samo u domenu profesionalaca već i običnih ljudi. Samim tim rizici korišćenja mobilnih uređaja svakog dana sve više rastu, pa se javlja potreba da se o bezbednosti mobilnih uređaja povede znatno veća pažnja. Nemar ili nezainteresovanost korisnika mobilnih uređaja da zaštite privatnost i dalje predstavljaju najveći izvor dostupnosti "hakovanja" uređaja. Pridržavanje samo nekoliko osnovnih pravila možemo podići bezbednost naših uređaja na znatno viši nivo. Navešćemo neka od osnovnih pravila kojih se treba pridržavati prilikom korišćenja mobilnih uređaja:

1. Uvek kada koristimo mobilni uređaj mora se voditi računa o njegovoj bezbednosti !
2. Instalirajte bezbednosno rešenje-antivirusni program.
3. Obavezno treba postaviti jaku lozinku.
4. Ne pokretati nepoznate aplikacije
5. Postavite anti-theft, rešenje protiv krađe.
6. Instalirajte najnovija ažuriranja OS
7. Nemojte instalirati aplikacije iz sumnjivih prodavnica
8. Nemojte da ulazite u "koren" (root) uređaja
8. Uključiti šifriranje podataka (data encryption)
9. Uvek se povežite samo sa bezbednom Secure Wi-Fi om
10. Čuvati samo one podatke koje nisu osetljive prirode

## LITERATURA:

[1] M.Kosanović, M.Kosanović, " Integracija bežičnih senzorskih mreža u *Cloud Computing-u*", XIX IT, Žabljak 24.02-28.02.2014, pp. 88-91.

[2] <https://www.a10networks.com/solutions/enterprise-delivery-security>, pos. 10.01.2018

[3] M. Veinović, M. Cajić, B. Brkić, "Tehnike i metode napada na komunikacioni kanal pri prenosu podataka u mobilnoj telefoniji", 10. Međunarodni naučni skup Sinergija, pp. 89-94, BiH, Bjeljina 2012.

[4] <https://www.priv.gc.ca/en/blog>, pos. 15.01.2018

[5] M.Kotadia, "Major smartphone worm by 2007", Gartner Study, 2005

[6] [http://www.amontec.com/pub/amt\\_ann004.pdf](http://www.amontec.com/pub/amt_ann004.pdf) , pos. 10.01.2018

[7] <https://singipedia.singidunum.ac.rs/izdanje/41244-zastita-podataka-i-sms-poruka-na-mobilnim-telefonima-sa-android-operativnim-sistemom>

[8] <https://source.android.com/security/>, pos. 10.01.2018

[9] M. Cajić, B. Brkić, "Sistem procjene bezbjednosti za Android operativni sistem", INFOTEH-JAHORINA, Vol. 10, Ref. F-1, pp. 902-906, BiH, Jahorina, March 2011.

[10] <http://www.appbrain.com/stats/number-of-android-apps> , pos. 03.02.2018

[11] <https://sensortower.com/blog/app-revenue-and-downloads-2017>, pos. 03.02.2018

[12] <https://techviral.net/hack-wifi-on-android-without-root/> , pos. 20.01.2018

# KORIŠĆENJE ARCGIS I HEC-RAS PROGRAMSKIH PAKETA ZA DEFINISANJE PLAVNIH ZONA APPLICATION OF ARCGIS AND HEC-RAS TOOLS IN DETERMINATION OF FLOODPLAIN AREAS

Boris Krunic<sup>1</sup>, Nevena Cvijanovic<sup>1</sup>  
Institut za vodoprivredu "Jaroslav Černi"<sup>1</sup>

**Sadržaj** – Problem plavljenja inudacionih prostora je oduvek bio aktualan na prostoru Srbije, s obzirom na veliki broj vodotoka koji se nalaze na ovom području. Poslednjih godina, usled katastrofalnih poplava koje su se desile, ova problematika je dodatno aktualizovana. Dodatni problem prilikom plavljenja predstavlja i činjenica da je u novijem periodu došlo da proširenja urbanih područja i da se veliki broj novih objekata sagradio u potencijalnim plavnim zonama vodotokova. Da bi se predvidele potencijalne štete i izbegli štetni uticaji izazvani izlivanjem reka, potrebno je definisati prostor koji je ugrožen poplavama. U ovom radu je prikazana primena softverskih programa ArcGIS i HEC-RAS, pomoću kojih se vrši formiranje digitalnog modela terena i određivanje plavnih zona.

**Abstract** – Problem with floods has always been important issue in Serbia, due to large amount of rivers on this territory. During last few years, due to catastrophic floods, this issue have been more actualized. Additional problem during these events became the fact that urban areas are spreading, and large number of objects have been constructed in the potential floodplain areas. In order to predict potential damage and avoid damages due to floods, it is necessary to determine floodplain area. This paper presents the application of ArcGIS i HEC-RAS software, in order to define digital terrain model and floodplain areas.

## 1. UVOD

Srbija je zemlja sa velikim brojem vodotokova različite veličine. Većina ovih vodotokova nije regulisana, i ne poseduje zaštitu od plavljenja. Izlivanja reka uzrokuju velike štete u naseljima, industriji i poljoprivrednom zemljištu koje se nalaze u dolinama vodotokova. Karakteristično za noviji period predstavlja širenje urbanih područja, pri čemu se jedan deo objekata gradi u inudacionim zonama reka, koje su ugrožene poplavama. Da bi se sagledali svi potencijalno ugroženi objekti, nepohodno je definisati plavnu zonu, uz morfološke i hidrauličke parametre reka, čime bi se definisao stepen ugroženosti razmatranog područja.

## 2. METODOLOGIJA DEFINISANJA PLAVNIH ZONA

Za određivanje plavnih zona, neophodno je sakupiti topografske i geodetske podloge analiziranog područja, na osnovu kojih se formira digitalni model terena (DMT). Na osnovu hidrološke analize, dobijaju se merodavne vrednosti velikih voda. Proticaji dobijeni hidrološkim proračunima se dalje koriste u hidrauličkom proračunu.

Rezultati hidrauličkog proračuna se zatim prikazuju na digitalnom modelu terena, gde se kao krajnji rezultat dobija granica plavne zone.

## 3. FORMIRANJE DIGITALNOG MODELA TERENA

### 3.1. Topografske i geodetske podloge

Za formiranje digitalnog modela, potrebni ulazni podaci su topografske podloge i geodetska snimanja razmatranog područja. Topografske podloge predstavljaju karte iscrtane u različitim razmerama. Da bi ove karte bile upotrebljive kao podloga u nekom od programskih paketa koji se bave analizom prostornih podataka, potrebno ih je digitalizovati. Digitalizacija karata je proces u kom se visinski podaci sa karata prevode u digitalni oblik, i na taj način postaju operativni za formiranje DMT.

Prilikom definisanja plavnih zona za određeni vodotok nepohodno je posedovanje geodetske podloge koja treba da obuhvati celokupan pojas na kom može da dođe do plavljenja. Prostor koji može biti obuhvaćen plavljenjem po pravilu obuhvata veliku teritoriju, naročito kod većih vodotokova gde se vrši analiza plavljenja na dugačkoj deonici.

S obzirom na veliku površinu koju treba obuhvatiti snimanjem, najčešće se kao osnovna podloga koriste digitalizovane topografske karte (slika 1).



Slika 1. Digitalizovana topografska karta razmere 1: 25.000 prikazana u ArcGIS okruženju



Digitalizovana topografska karta je relativno grube tačnosti, bez visinke predstave korita vodotoka, puteva i slično. Da bi se formirao precizan DMT, potrebno je osnovnu podlogu dopuniti geodetskim snimanjem. Kako je geodetsko snimanje tehnokonomske prirode, snimanje se obavlja u što manjem obimu, pri čemu je neophodno snimiti sve elemente nepohodne za formiranje DMT zadovoljavajuće tačnosti.

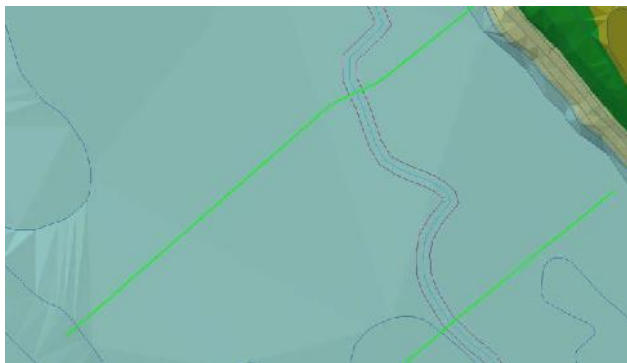
Pod geodetskim snimanjem se podrazumeva snimanje poprečnih profila rečnog korita na određenom rastojanju, objekata u samom koritu (mostova, pragova, kaskada itd.), kao i objekata uz korito (putevi, nasipi itd.).

### 3.2. Integrisanje raspoloživih podataka u DMT

Da bi se formirao digitalni model terena, potrebno je rezultate geodetskog snimanja integrisati sa topografskom podlogom. Postoji više različitih softvera u pomoću kojih je moguće formirati DMT. Za potrebe ovog rada, za izradu DMT je korišćen ArcGIS.

ArcGIS je geografski informacioni sistem, koji ima široku primenu u radu sa mapama i geografskim podacima. Koristi se za kreiranje mapa, povezivanje geografskih podataka kao i njihovo analiziranje [1].

Geodetskim snimanjem dobijaju se poprečni profili korita na određenom rastojanju duž vodotoka. Integrisanjem snimljenih poprečnih profila u DMT dobija se geometrija korita samo na mestima snimanja. Kako bi se napravila bolja prezentacija plavnih zona i dubina vode, potrebno je i između snimljenih profila formirati korito u okviru DMT. Ta operacija se može obaviti u okviru programskog paketa ArcGIS sa *bathymetry* dodatkom. Ovaj dodatak omogućava formiranje rečnog korita u DMT po zadatoj osi toka. Geometrija korita nastaje interpolacijom između susednih snimljenih poprečnih profila vodotoka (slike 2 i 3). Ova geometrija ne odgovara u potpunosti geometriji rečnog korita u prirodi, ali daje bolju predstavu terena i preglednije rezultate kada je u pitanju grafička prezentacija plavne zone i dubina vode na plavnom području.



Slika 2. DMT bez geometrije korita



Slika 3. DMT nakon integrisanog korita

## 4. HIDRAULIČKI PRORAČUN

DMT koji je formiran u okviru ArcGIS-a koristiti se za formiranje hidrauličkog modela. Ovaj postupak se obavlja uz pomoć HEC-GeoRAS dodatka za ArcGIS.

HEC-GeoRAS predstavlja set ArcGIS alata koji omogućuju integraciju prostornih podataka iz ArcGIS okruženja u HEC-RAS, kao integraciju rezultata hidrauličkog proračuna iz HEC-RAS-a u ArcGIS[2].

Softverski paket HEC-RAS (Hydrologic Engineering Centers River Analysis System) je razvijen od strane američkog vojnog inženjerstva (US Army Corps of Engineers), i koristi se za hidrauličku analizu rečnih tokova. Sam program podržava računicu za otvorene tokove nepravilne geometrije rečnog korita, pri čemu postoji mogućnost izbora velikog broja spoljašnjih i unutrašnjih graničnih uslova. Program računa liniju nivoa za merodavne protoke rešavanjem energetskih i jednačina kontinuiteta. Računicom može da se simulira ustaljeno ili neustaljeno tečenje [3].

Osnovna prednost HEC-GeoRAS-a je mogućnost pripreme svih geometrijskih podataka u okviru ArcGIS-a, koji su potrebni za hidraulički proračun u HEC-RAS-u. Formiranje geometrije pre svega podrazumeva definisanje linije ose toka reke, obala i pozicije poprečnih profila. Po potrebi moguće je definisati zone sa različitim vrednostima Manningovog koeficijenta rapavosti, zatim zone bez tečenja, položaje nasipa, mostova i raznih drugih prepreka u koritu i van njega. S obzirom na to da se navedeni parametri definišu u okviru ArcGIS okruženja, koje odlikuje prostorna preglednost, moguće je sa velikom tačnošću definisati navedene ulazne parametre, i formirati vrlo precizan model.

Ovako pripremljena podloga se integriše u HEC-RAS u kome se formira model za hidraulički proračun. Pored geometrije rečne doline, potrebno je definisati sve unutrašnje i spoljašnje granične uslove. Kao rezultat proračuna dobijaju se linije nivoa za merodavne vode, brzine toka, vučne sile, kao i veliki broj drugih parametara.

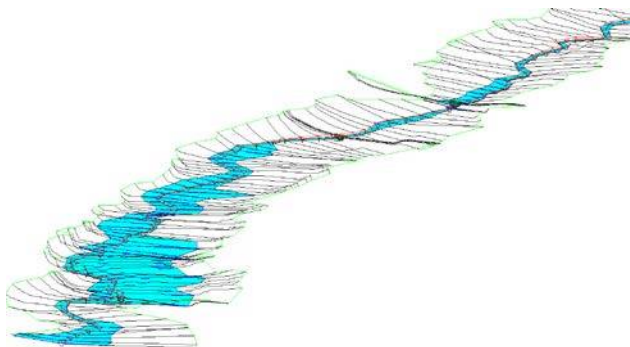
## 5. FORMIRANJE PLAVNIH ZONA

Dobijeni rezultati hidrauličkog proračuna (linije nivoa) integrišu se u ArcGIS. Integracijom se linija nivoa vezuje za prethodno definisane poprečne profile, koji su korišćeni u hidrauličkom proračunu. Na mestima profila se očitavaju vrednosti linije nivoa i na taj način se formira plavna zona u odnosu na DMT, pri čemu se ujedno dobijaju i dubine vode na plavnom području.

S obzirom da pregledan grafički prikaz plavne zone, posebno ako se kao podloga ubaci orto-foto snimak, moguće je vrlo lako odrediti pojas koji je ugrožen od plavljenja. Na ovaj način se može konstatovati koji su lokaliteti najugroženiji od poplava, kako prema širini plavne zone, tako i u odnosu na dubine koje se ostvaruju u okviru plavne zone. Karta plavnih zona definisana na ovaj način predstavlja osnovu za dalju analizu i izradu karata rizika od poplava.

## 6. REZULTATI

Prethodno opisana metodologija za određivanje plavnih zona na ugroženom području primenjena je na dolinu reke Ribnice u zapadnom delu Srbije. Na slici 4 je prikazan rezultat hidrauličkog proračuna neustaljenog tečenja na reci Ribnici, prikazan u vidu vodnog ogledala vodotoka u HEC-RAS okruženju.



Slika 4. Rezultat hidrauličke alalize neustaljenog tečenja na reci Ribnici

Rezultati hidrauličkog proračuna integrisani su u ArcGIS i na taj način definisane su plavne zone i dubine plavljenja u rečnoj dolini (slika 5).



Slika 5. Plavna zona sa prikazom dubina u dolini reke Ribnice

## 7. ZAKLJUČAK

ArcGIS je jako koristan programski paket sa velikim mogućnostima za formiranje i analizu prostornih podataka. Takođe, uz HEC-GeoRAS dodatak moguće je kreirati vrlo preciznu geometriju koja se na jednostavan način integriše u HEC-RAS koji se koristi za hidraulički proračuna. Rezultati proračuna se integrišu nazad u ArcGIS gde se formiraju plavne zone sa dubinama plavljenja koje se ostvaruju u okviru njih. Na osnovu ovih podataka moguće je utvrditi koja površina je ugrožena od poplava kao i stepen ugroženosti analiziranog područja.

## LITERATURA

- [1] University of Maryland Libraries U.S. Government Information, Maps & GIS Services - Introduction to GIS Using ArcGIS Desktop 10.1 , January 2013.
- [2] US Army Corps of Engineers, HEC-GeoRAS GIS Tools for Support of HEC-RAS using ArcGIS – User Manual Version 4.2, September 2009.
- [3] US Army Corps of Engineers, HEC-RAS River Analysis System - Hydraulic Reference Manual Version 5.0, February 2016.

# ADVANCED MEMORY PROFILING FOR DSP APPLICATIONS

Nives Kaprocki, Jelena Kovačević, Nenad Pekez  
Faculty of Technical Sciences, University of Novi Sad

**Abstract** - This paper presents profiling of access to internal and external memory spaces in an embedded system used for real-time audio processing. As consumer embedded devices must execute applications that demand extensive memory footprint, it is crucial for the early development phase to be aware of how each memory access affects processing performance. Memory management of a typical digital DSP system is introduced through an overview of its memory architecture and mapping of the present memory spaces onto the main buses. A detailed analysis of the measured access times enables us to design an optimized software architecture for complex applications such as audio coders or renderers.

## 1. INTRODUCTION

Embedded systems can be defined as information processing systems embedded into larger products such as cars, telecommunication equipment or consumer electronics [1]. In contrast to general-purpose systems, embedded systems are dedicated towards a certain applications and have to be efficient in fulfilling these specific requirements. Due to many constraints, most of the requirements are not functional but refer to the cost, performance, power consumption etc. [2].

As stated in [3,4], memory system contributes most to the performance of an embedded system and increases the manufacturing cost of the hardware. Specifically, in embedded systems based on digital signal processors used in audio consumer devices, memory organization and interfaces are a critical factor in performance assessment of the processor. In order to enable successful real-time processing of increasingly large amount of data, audio systems demand a high memory bandwidth.

There are several architectural solutions which can improve efficiency of memory handling. Instead of the classical Von Neumann architecture with shared data and code memory, these systems have an improved Harvard architecture which has two separate data memories and one code memory. Size of internal memory is often restricted by processor's physical size and its IO performance, hence external memory must also be used. Additional memory outside the processor is a paged dynamic memory (SDRAM), slower than a static RAM memory (SRAM) but also significantly smaller and cheaper. This additional memory is necessary in high-performance audio systems like Audio/Video receivers, Sound Bar systems and Set-top boxes.

The design of an audio system often starts from a software description of the system in C language [5]. This software code is not optimized in any manners, because it mainly serves the purpose of functional and conformance testing. Therefore, it has to be transformed into an efficient system with following steps: system architecture design,

hardware/software partitioning and software optimization [6]. These steps require detailed information about the performance of different parts of the application.

Before the beginning of the system architecture design phase, extensive profiling of memory requirements and MIPS (million instructions per second) consumption has to be done. As earlier generations of audio applications, such as multichannel audio coders MP3, Dolby Digital and DTS HD, handled smaller amount of data which could entirely fit into the processor's internal memory spaces, it was possible to do separate profiling of memory and processor time consumption. However, recent audio processing applications, e.g. object based audio coders Dolby Atmos and DTS X, are three to four times more demanding than their predecessors. Thus it is necessary to analyze the effect certain memory access has on both memory organization and processor performance.

This paper first gives an overview of the typical DSP for home and consumer audio systems, focusing on its memory organization, memory controllers and interfaces. Second part shows how memory is mapped onto the corresponding buses as well as arbitration for access to the slaves on the bus. Lastly, test procedure and test environment is described, which were used to measure internal and external memory access times.

## 2. TEST CASE STUDY

Memory access profiling will be described on the case study of a Cirrus Logic CS49844 DSP processor [7], a typical processor for home audio systems. This processor was chosen because it was designed with a large amount of on-chip program and data RAM. It also has all the necessary peripherals required to support the latest standards in consumer entertainment products, in particular the external SDRAM memory interface.

### A. Memory Architecture

Quad-core DSP processor used for high-performance audio processing consists of two DSP clusters. These two clusters are interconnected to the various peripherals and to each other via two AHBs (Advanced High-performance Buses) and two APBs (Advanced Peripheral Buses) [8] and various sideband signals.

Main components of each DSP cluster (Fig. 1) are:

- 32-bit fixed point DSP core
- DMA controller
- X, Y and P RAM
- Memory interface
- AHB arbiter and interface
- APB arbiter and interface

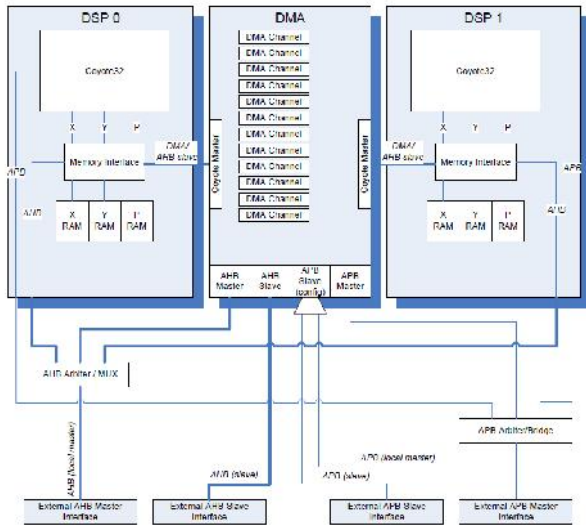


Fig. 1. Architecture of a DSP cluster

All DSP cores are based on an advanced Harvard architecture. They have two separate X and Y data memory spaces with the size of 60k Words and one code memory space with the same size, and employ independent buses for each memory space. The 32-bit DSP cores achieve the high performance of 300 MHz through an efficient instruction set and highly parallel architecture.

The DMA (Direct Memory Access) controller can transfer data between peripheral devices, internal and external memory spaces without processor interference, thus more resources can be spent on processing. Each of its twelve independent channels has a source and a destination, which can be any address in the DSP local address map (X, Y, and P), any address in the AHB space, or any address in the APB space. Channels of the DMA are mostly used to service repeated events like DAO (Digital Audio Out) services and DAI (Digital Audio In) accesses, and to send PCM (Pulse-code modulation) samples from one DSP core to another.

Memory interface handles X, Y and P memory requests from the DSP, and DMA requests. This interface does the arbitration and proper conversion to the memories. Memory interface also decodes the XYP DSP requests, which are mapped to the on-chip or the external memories. Requests to the on-chip memory go directly to the X, Y and P RAMS, while off-chip requests go to the AHB arbiter.

Both AHB and APB blocks arbiter between three potential masters: two DSP cores in the cluster and the local DMA. They are the interface between AHB/APB master in the DSP cluster and the corresponding AHB/APB bus. Data memory of the DSP is extended during runtime with SDRAM controller, which is a AHB peripheral. SDRAM controller provides two-port access to X, Y and P memory spaces, where one port is dedicated to the P memory space and the second port is shared by the X and Y memories.

## B. Memory Mapping

This study focuses on accessing data needed for runtime processing of input audio streams, which includes metadata extracted from the input stream inside the decoder, tables with coefficients needed for a variety of audio filters and tables used for classification of sound based on its features. As the aforementioned data is placed inside internal DSP memories and external SDRAM memory, this chapter will present memory mapping and arbitration of these memory spaces onto the AHB bus (Fig 2).

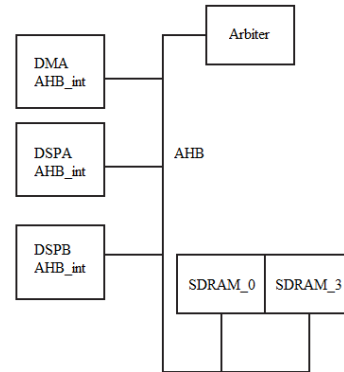


Fig. 2. AHB bus

When AHB masters need the bus to do transactions to slaves, they all need to send the request signal to the arbiter. The arbiter will grant the request by issuing a bus grant signal. As soon as the master gets a bus grant signal in a valid phase, it will pop out the address phase by issuing a signal which indicates the sequential transfer type and new address of transaction. During data phase where read or write signals are transferred, slaves have the right to extend a current data phase by pulling the ready signal low. This can also extend the address phase and the grant phase of the next transaction.

Total external memory size addressable in AHB space is 128 Mbytes. The number of pages required by the DSP to access external memory is 8K pages, which can be addressed using 13 bits. The X, Y, and P memory interface for each DSP will have a 13-bit page register to access external memory. All DSPs see an almost identical address map on the AHB bus, except from address 0x6200000 through 0x63ffff, Cluster 0 sees Cluster 1, and Cluster 1 sees Cluster 0, while from address 0x6400000 through 0x65ffff, Cluster 0 sees Cluster 0, and Cluster 1 sees Cluster 1. The SDRAM with the size of 64 MB is mapped to the address range from 0x0000000 to 0x3ffffff.

X Memory		Y Memory		P Memory	
Address	Size (kW)	Address	Size (kW)	Address	Size (kW)
0000- efff	60	0000- efff	60	0000- efff	60
f000- ffff	4	f000- ffff	4	f000- ffff	4

Table 1. Internal memory mapping

In each DSP, rather than have a different external decoder for every memory space, the maximum internal space is

used to decode the external memory accesses. Firmware requirements have determined that any DSP address smaller than 0xF000h is an access to internal memory, and any address higher or equal to 0xF000h is an access to external memory (Table 1). Thus, memory pages from the DSP point of view have a size of 4K Words.

### 3. TEST PROCEDURE

Test environment for measurement of the memory access times consists of the evaluation board CRD49844 [9] with a Cirrus Logic CS49844 DSP chosen as our case study, a sound card for sound reproduction and the PC with an Integrated Development Environment (IDE) for audio firmware development.

First step in the test procedure is development of a simple application which measures a number of cycles required to read data from an AHB slave or write data to the slave. DSPC core has been chosen as the bus master and DSPA, DSPB, DSPD and SDRAM have been chosen as bus slaves in our test procedure. However, it is possible to run the same application on any other DSP core with minor changes to memory mapping addresses.

Accessing AHB slaves' memory is achieved using the memory mapping method explained in the previous chapter. The appropriate external memory space is mapped to the top locations of DSPC core's internal memory by setting the page register value to the slave's AHB address. Table 2 shows which value has to be assigned to the page register in order to access a specific external memory space from the DSPC core.

Memory space	Address
DSPA X memory	0x06200000 – 0x0623bfff
DSPA Y memory	0x0623c000 – 0x06277fff
DSPB X memory	0x062b4000 – 0x062effff
DSPB Y memory	0x062f0000 – 0x0632bfff
DSPD X memory	0x064b4000 – 0x064effff
DSPD Y memory	0x064f0000 – 0x0652bfff
SDRAM memory	0x00000000 – 0x03ffffff

Table 2. AHB memory mapping from DSPC

External memory access cycle count is measured with the programmable timer block. The timer consists of a 32-bit downcounter, a 32-bit modulo register and associated control and interrupt logic. The DSP clock drives the 32-bit downcounter timer. When the timer reaches zero, it is reloaded with the value in the timer modulo register. Subtraction of timer value after the read/write operation from its value before the operation gives a number of cycles spent on this operation.

After the application is written and compiled, it has to be uploaded onto the processor and started by sending any audio stream into the audio input interface. The type and the sampling rate of the stream do not affect the measurements, as the APB bus and DMA controller are the ones responsible for transport of the audio samples and they do not interfere with the AHB bus.

### 4. RESULTS

The profiling of memory access is done on a four-core digital signal processor. The evaluation of memory read/write operations is presented through its memory access time and its processor time usage. Access time in a number of elapsed cycles per one read/written Word – 32 bit location, which is measured using the development environment, is converted into a number of seconds per one read/written Word using a following equation:

$$access\ time = \frac{cycle\_num}{clock}$$

In the equation, clock is the processor clock which equals 300MHz. Measured time of one read/written Word for different test cases is presented in Table 3. The first column shows which memory location the DSPC is accessing, while the second column shows whether the memory is being read or written to. The last column shows the number of seconds used for transferring of one Word to or from that location.

Memory location	Memory operation	Access time [ns]
Internal DSPC X/Y memory	read	3.3
Internal DSPC X/Y memory	write	3.3
DSPA/B/D X/Y memory	read	29.7
DSPA/B/D X/Y memory	write	19.8
SDRAM memory	read	59.4
SDRAM memory	write	42.9

Table 3. Measured time of read/write operations

Internal memory access can be achieved in one cycle, because DSP requests to the on-chip memory go directly to X and Y RAM. On the other hand, off-chip memory requests have to be handled through the AHB arbiter. Due to the initial communication between the AHB master and controller, and the duration of the data transfer, external memory operations spend more cycles. When accessing SDRAM memory, this number is even higher because each SDRAM interface is running at the SDRAM clock speed (up to 166MHz).

In order to receive a better understanding of how each memory access affects processor performance, a number of spent cycles on reading and writing of 4kW to different memory spaces is measured. This value is then converted



into million instructions per second with the following equation:

$$MIPS = \frac{cycle\_num * \frac{Fs}{BLOCK\_SIZE}}{1000000}$$

Parameter  $F_s$  is the sampling frequency, number of samples obtained in one second, which equals 48kHz in the project.  $BLOCK\_SIZE$  is the size of the processing block, which equals 256 samples.

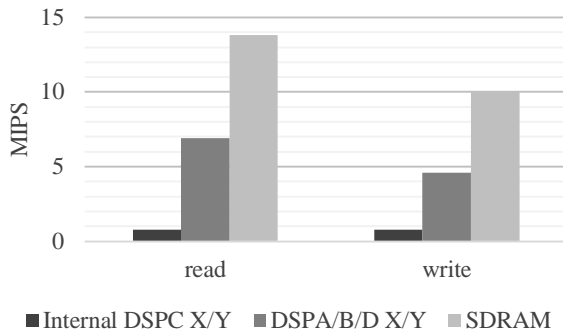


Fig. 3 Consumption of processor time for different memory operations

Fig. 3 shows how much processing time is spent on reading or writing of 4 kW of data into different memory spaces. Reading and writing to internal DSP memory spends only a small portion of 300 MIPS available for processing. However, frequent access to external memory significantly reduces the amount of processing time that can be spent on complex audio processing modules. For this reason, its usage has to be restricted. Situation when SDRAM is mostly used is when some data has to be shared among the DSP cores, such as the metadata which is extracted inside the decoder module and used throughout the whole processing. Furthermore, new sound algorithms based on neural networks demand classification and computing tables which require up to 35 kW of data. These tables are also stored on external memory spaces, as only some of their data is used periodically and they would occupy a high percentage of internal memory space.

## 5. CONCLUSION

This paper introduced a procedure for profiling of processor time consumption during external memory read and write operations in modern consumer audio systems. This procedure has been done on a case of a typical DSP used in home consumer devices, such as AV receivers and Sound Bars. As the new generation of audio applications requires more resources and has to access off chip memory,

profiling should combine memory and processor time consumption. With this additional information it is possible to make a precise memory organization outline.

Results have shown that accessing off chip memory locations is up to 18 times more demanding than accessing on chip memory and can have a significant impact on the processing performance. Thus, external memory is mostly used to store data which has to be shared or accessed periodically. Further improvements of the profiling procedure can include profiling of the audio input and output peripherals and DMA controller which are affected by the choice of external interfaces and input stream's sample rate.

## ACKNOWLEDGEMENT

This work was partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under Grant TR-32029.

## REFERENCES

- [1] P. Marwedel, *Embedded Systems Design*, Dordrecht: Springer, 2006.
- [2] W. Wolf, *Computers As Components: Principles of Embedded Computing System Design*, San Francisco: Morgan Kaufmann, 2005.
- [3] W. Wolf and M. Kandemir, "Memory System Optimization of Embedded Software," *Proceedings of the IEEE*, pp. 165-182, 2003.
- [4] L. Oliveira, J. C. B. Mattos and L. Brisolaro, "Survey of Memory Optimization Techniques for Embedded Systems," *2013 III Brazilian Symposium on Computing Systems Engineering*, Niteroi, 2013, pp. 65-70.
- [5] M. Djukic, N. Cetic, J. Kovacevic and M. Popovic, "A C compiler based methodology for implementing audio DSP applications on a class of embedded systems," *2008 IEEE International Symposium on Consumer Electronics*, Vilamoura, 2008, pp. 1-4.
- [6] H. Hubert, B. Stabernack and K. I. Wels, "Performance and Memory Profiling for Embedded System Design," *2007 International Symposium on Industrial Embedded Systems*, Lisbon, 2007, pp. 94-101.
- [7] Cirrus Logic Inc: CS49844 Data Sheet, May 2012.
- [8] AMBA Specification (Rev 2.0), ARM Limited, 1999.
- [9] Cirrus Logic Inc: CRD498X4 Board User's Manual, November 2015.

# KONFIGURABILNE ARITMETIČKO LOGIČKE JEDINICE REALIZOVANE KORIŠĆENJEM PROTOČNE OBRADE

## CONFIGURABLE PIPELINED ARITHMETIC LOGIC UNITS

Filip Hadžić<sup>1</sup>, Zaharije Radivojević<sup>1</sup>, Marko Mićović<sup>1</sup>, Uroš Radenković<sup>1</sup>

<sup>1</sup>Elektrotehnički fakultet Univerziteta u Beogradu

**Sadržaj** - U ovom radu je prikazan princip rada konfigurabilnih aritmetičko logičkih jedinica realizovanih tehnikom protočne obrade. Konfigurisanje aritmetičko logičke jedinice se zasniva na tablicama preslikavanja. Korišćenjem tablica preslikavanja postiže se mogućnost izvršavanja instrukcija koje realizuju bilo koju Bulovu funkciju. Prikazana je realizacija aritmetičko logičke jedinice koja je zasnovana na serijskom povezivanju tablica preslikavanja korišćenjem protočne obrade. Protočna obrada je razmatrana sa stanovišta protoka podataka i protoka instrukcija. Uz predloge organizacija aritmetičko logičkih jedinica prikazane su i optimizacije u vidu dodatne logike.

**Ključne reči** - aritmetičko logička jedinica, protočna obrada, tablica preslikavanja, logičko projektovanje

**Abstract** - This paper presents the configurable pipelined arithmetic logic units. Configuring the arithmetic logical unit is based on the lookup tables (LUT). Using the lookup tables, it is possible to execute instructions that implement any Boolean function. The presented arithmetic logical unit is based on the serial connection of the lookup tables using pipeline. Pipelining was considered from the point of view of data pipelining and instruction pipelining. With the proposals, the organization of arithmetic logical units also presents optimizations in the form of additional logic.

**Keywords** - ALU, pipeline, lookup table LUT, logic design

### 1. UVOD

Operacije instrukcija savremenih procesora mogu se podeliti u četiri grupe. U prvu grupu spadaju operacije koje obrađuju podatke procesora, u drugu grupu operacija spadaju operacije koje razmenjuju podatke procesora sa ostalim komponentama računarskog sistema, u treću grupu spadaju operacije koje vrše upravljanje toka programa, a u četvrtu grupu spadaju instrukcije podešavanja rada računarskog sistema.

U prvu grupu instrukcija spadaju aritmetičke, logičke i pomeračke instrukcije. Za izvršavanje prve grupe operacija pretežno se koristi aritmetičko logička jedinica. Aritmetičke instrukcije su instrukcije koje treba da izvrše operacije sabiranja, oduzimanja, inkrementiranja, dekrementiranja itd. Ove instrukcije mogu da obrađuju dva tipa podataka. Prvi tip podataka su celi brojevi, a drugi tip su decimalni brojevi. Logičke instrukcije su instrukcije koje treba da izvrše operacije logičkog

sabiranja, logičkog množenja, negiranja itd. Ove instrukcije nemaju poseban tip podataka, već svoje operande smatraju kao niz međusobno nezavisnih bitova.

Aritmetičko logičke instrukcije se mogu izvršavati koristeći aritmetičko logičke jedinice. Aritmetičko logičke jedinice realizuju skup Bulovih funkcija. Tablice preslikavanja su pogodno za predstavljanje bilo koje Bulove funkcije.

Prikazana je realizacija aritmetičko logičke jedinice koja je zasnovana na serijskom povezivanju tablica preslikavanja korišćenjem protočne obrade. Protočna obrada služi za povećanje paralelizacije u bilo kom sistemu [1]. Podelom procesa na više faza oslobađa se prostor za dodavanje više poslova u sistem, tako što kada jedan posao završi svoju fazu i pređe u narednu, trenutno posmatrana faza se oslobađa za sledeći posao. Protočnom obradom se povećava paralelizacija procesora čemu se povećavaju njegove performanse. Protočna obrada je razmatrana sa stanovišta protoka podataka i protoka instrukcija. Pokazano je da logika unutar protočne obrade kojom bi se obavljao protok podataka zahteva veći broj logičkih kola u odnosu na broj logičkih kola kojom se obavlja protok instrukcija.

Uz predloge organizacija aritmetičko logičkih jedinica prikazane su i optimizacije u vidu dodatne logike. Ove optimizacije obuhvataju način odabira podataka nad kojim se obavlja obrada i način računanja statusnih bitova. Prikazan je odabir podataka na osnovu maske umesto dekoderske logike.

Ostatak rada organizovan je na sledeći način. U drugoj glavi dat je pregled postojećih rešenja. U trećoj glavi je opisan problem i ograničenje. Četvrta glava opisuje implementacione detalje aritmetičko logičkih jedinica zasnovanih na korišćenju tablica preslikavanja. U petoj glavi prikazane dve realizacije aritmetičko logičke jedinice zasnovane na protočnoj obradi. U glavi šest dat je zaključak.

### 2. POSTOJEĆA REŠENJA

Aritmetičko logička jedinica kao ulaz ima dva (ili atipično više) podatka kao i zadatu operaciju koju treba da izvrši nad njima, a kao izlaz može biti jedan ili više podataka (obično postoje i statusni bitovi pomoću kojih se određuje da li je rezultat operacije negativan ( $N$  – negative bit), da li je rezultat operacije jednak nuli ( $Z$  – zero bit), da li je pri izvršavanju operacije bilo prekoračenja ( $V$  – overflow bit), kao i da li je bilo prenosa ( $C$  – carry bit)). Ulazni i

izlazni podaci koji se obrađuju mogu da budu širine jedan ili više bitova. Operacije koje se zadaju u aritmetičko logičkim jedinicama su aritmetičko sabiranje, aritmetičko oduzimanje, logičko sabiranje, logičko množenje, negiranje itd. Savremeni procesori imaju nekoliko aritmetičko logičkih jedinica u zavisnosti od mikroarhitekture proizvođača. Savremene mikroarhitekture imaju obično četiri aritmetičko logičke jedinice (*Intel Haswell* [2], *Intel Skylake* [3], *AMD Zen* [4]). Optimizacijom aritmetičko logičkih jedinica bi se potencijalno uticalo na performanse procesora.

### 3. OPIS PROBLEMA I OGRANIČENJA

Operacije koje se zadaju aritmetičko logičkoj jedinici predstavljaju jednoznačno preslikavanje, pa se ove jedinice realizuju kao kombinacione mreže i kao takve rezultat operacije računaju u istom taktu u kome se zadaje operacija. Kod ovakve realizacije mogu se uočiti dve mane.

Prva mana realizacije aritmetičko logičke jedinice kao kombinaciona mreža je ta što se pri operacijama aritmetičkog sabiranja i oduzimanja unosi veliko kašnjenje signala koji prolaze kroz potrebna logička kola. To je posledica same aritmetike, jer rezultat aritmetičke operacije jednog para bitova može da utiče na celokupni rezultat, tj. na sve starije bitove rezultata kod sabiranja ili na sve mlađe bitove rezultata kod oduzimanja. Samim tim se dobija zavisnost između veličine podatka nad kojim se vrši operacija i vremena izvršavanja operacije usled kašnjenja kroz kombinacionu mrežu. Aritmetičko logička jedinica može da ima uticaj na dužinu periode takta samog procesora, što može da bude problem kod obrade podataka velike širine. Različitim implementacijama načina sabiranja pokazalo se da je moguća trgovina vremena kašnjenja i broja logičkih elemenata u samoj jedinici, međutim za velike operande ova trgovina postaje dosta skupa. Da bi se razrešio prethodno opisani potencijalni problem, u ovom radu se razmatra uvođenje protočne obrade u izvršavanju operacija aritmetičko logičke jedinice.

Druga mana realizacije aritmetičko logičke jedinice kao kombinaciona mreža je ta što se u paraleli računaju rezultati svih realizovanih operacija, a na kraju se izabere samo jedan rezultat (na osnovu zadate operacije aritmetičko logičke jedinice). Ovo predstavlja neracionalno korišćenje resursa: vremena (neke operacije se brže završe od drugih, a ipak moraju da sačekaju izračunavanje sporije operacije), logičkih elemenata (paralelno se računaju operacije, a na kraju se ignoriše rezultat svih osim jedne) i povećane potrošnje struje (računanjem svih operacija koje nisu zahtevane, dolazi do velikog broja bespotrebnih promena napona u signalima, pa samim tim i stanjima u tranzistorima koji troše struju, a njihov rezultat će biti ignorisan). Da bi se razrešio prethodno opisani potencijalni problem, u ovom radu se razmatra uvođenje tablica preslikavanja u izvršavanju operacija aritmetičko logičke jedinice.

Problem koji se posmatra u ovom radu je ubrzanje aritmetičko logičkih jedinica pomoću protočne obrade koje imaju mogućnost rekonfiguracije. Osnovna

pretpostavka pod kojom se rešava problem je da aritmetička logička jedinica predstavlja najsporiji deo procesora. Operacije koje se mogu realizovati su raznolike i zavise od same arhitekture procesora. Kod aritmetičkih instrukcija bez smanjenja opštosti, smatraće se da su podaci celobrojne veličine. Razmatraju se sve logičke operacije, kao i aritmetičke operacije sabiranja, oduzimanje, inkrementiranje i dekrementiranje.

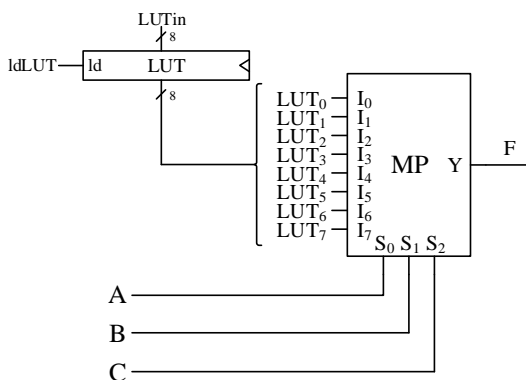
### 4. ARITMETIČKO LOGIČKE JEDINICE REALIZOVANE KORIŠĆENJEM TABLICA PRESLIKAVANJA

Tablice preslikavanja su rešenje pomoću kojeg se može na jednostavan način realizovati bilo koja Bulova funkcija. Fizički gledano, tablica preslikavanja se može predstaviti kao memorijski modul u kome se nalazi realizacija Bulove funkcije. Operandi Bulove funkcije formiraju adresu memorijskog modula, dok se rezultat Bulove funkcije može pročitati kao izlaz memorijskog modula. Širina adrese memorijskog modula je jednaka zbiru broja bitova operanada, dok memorijskih reči ima  $2^{\text{širina adrese}}$  širine jedan bit (rezultat Bulove funkcije može da bude logička jedinica ili logička nula). Međutim, ako je potrebno da se za isti ulazni vektor izračuna više operacija (rezultat operacije ima više bitova), nije potrebno praviti nove, odvojene tablice preslikavanja, već bi se realizacija svodila na jednu tablicu preslikavanja čija bi se reč memorijskog modula proširila na potreban broj bitova. Ovim postupkom bi se uštedela dekoderska logika unutar memorijskog modula. Memorijski modul može biti namenjen isključivo za čitanje (ROM) ili može biti modul iz kojeg je moguće i čitati i upisivati podatke (RAM). Na osnovu samog tipa memorije, postoje dve vrste tablica preslikavanja i to tablica preslikavanja sa fiksnom operacijom ili tablica preslikavanja sa konfigurabilnom operacijom.

Tablice preslikavanja sa fiksnom operacijom koje vrše preslikavanje jednog bita se ne koriste, jer je jeftinije i brže realizovati Bulove funkcije sa direktnim logičkim kolima. Međutim, kada je potrebno vršiti preslikavanje na više bitova, ovakav tip tablica je dosta koristan. Neke od primena ovih tablica se može naći u nekim jedinicama za množenje i deljenje ili za realizaciju nekih drugih složenijih matematičkih funkcija kao što su sinus, kosinus, tangens itd. Korišćenjem tablica ubrzava se izračunavanje Bulovih funkcija, jer se kompletno preslikavanje zasniva na čitanju iz memorije, čije kašnjenje se svodi na multiplektersku logiku.

Konfigurabilne tablice preslikavanja imaju široku primenu na FPGA (енг. *Field-Programmable Gate Array*) čipovima. Prednost ovakvih tablica je u tome što mogu da na jednom fizičkom delu čipa ili procesora izvršavaju više različitih operacija u različitim vremenskim trenucima. Potrebno je samo da se u memoriju učita nov način preslikavanja kada za to ima potrebe. Ovim postupkom ostavlja se mogućnost izvršavanja bilo koje logičke funkcije u vidu jednog preslikavanja. Na ovaj način moguće je smanjiti ukupan broj instrukcija za izvršavanje programskog bloka.

U nastavku rada korišćiće se tablice preslikavanja koje vrše preslikavanje jednog bita, dok će se memorijski modul predstaviti kao spoj registra i multipleksera. Aritmetičke operacije osim parova bitova koji učestvuju u operaciji imaju još jedan podatak, a to je prenos kod sabiranja ili pozajmica kod oduzimanja. To znači da je za računanje aritmetičkih operacija potrebno tri podatka, pa ako računanje svodimo na parove od po jedan bit, onda u svakom trenutku se koriste tri bita u operaciji. Na Slici 1, data je strukturna šema tablice preslikavanja sa tri jednobitna operanda koja će se često koristiti u daljem radu. Registar LUT ima mogućnost paralelnog upisa, kako bi mogao da učita novu konfiguraciju i time promenio način preslikavanja. Obzirom da je sa tri operanda moguće definisati osam različitih vektora, korišćiće se registar širine osam bita, kao i multiplekser sa osam jednobitnih kanala i jednim jednobitnim izlazom. Svaki razred registra LUT se povezuje na određene kanale multipleksera. Na osnovu bitova A, B i C preko multipleksera bira se odgovarajući bit registra LUT koji predstavlja rezultat Bulove funkcije.



Slika 1. - Strukturna šema tablice preslikavanja na osnovu tri bita

Za logičko sabiranje dva bita A i B, konfiguracija u LUT registru treba da ima učitane vrednosti 11000000<sub>2</sub>. Kod logičkog sabiranja dva bita nije nam od interesa podatak C. Ovo važi za sve binarne logičke operacije. Za računanje prenosa kod sabiranja dva bita A i B sa prenosom C, konfiguracija u LUT registru treba da ima učitane vrednosti 11101000<sub>2</sub>. Za sabiranje dva bita A i B sa prenosom C, konfiguracija u LUT registru treba da ima učitane vrednosti 10010110<sub>2</sub>. Za računanje prenosa kod sabiranja dva bita A i B sa prenosom C, konfiguracija u

LUT registru treba da ima učitane vrednosti 11101000<sub>2</sub>. Na ovaj način je pokazano kako je moguće izvršavanje logičkih i aritmetičkih operacija preko tablica preslikavanja.

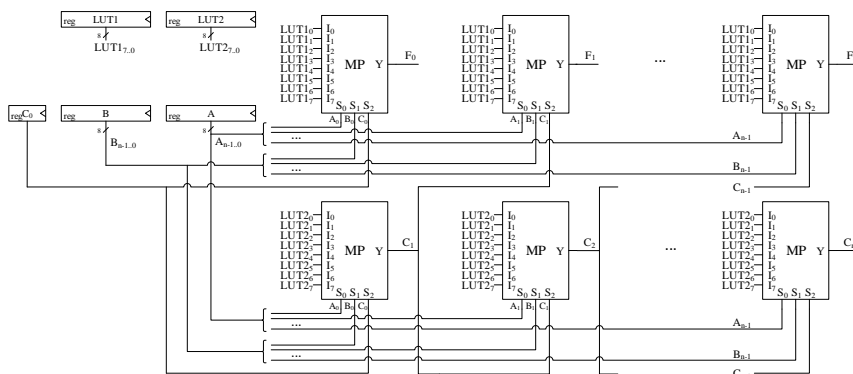
#### 4.1. Serijska realizacija sa računanjem na osnovu jednog bita

Kod logičkih operacija nad višebitnim operandima, svaki razred bita se zasebno računa i nema uticaj na izvršavanje operacije nad ostalim razredima. Kod aritmetičkih operacija to nije slučaj, jer postoji bit prenosa ili pozajmice, pa samim tim pri računanju nekog razreda operacije, potrebno je da postoji dve tablice preslikavanja. Prva tablica preslikavanja služi za računanje samog rezultata posmatranog razreda, dok druga tablica preslikavanja služi za računanje bita prenosa ili pozajmice za sledeći razred. Ove dve tablice preslikavanja su nezavisne (na istom razredu) pa mogu da se izvršavaju u paraleli.

Aritmetičko logičke jedinice operišu sa višebitnim operandima, pa je potrebno da se tablice preslikavanja međusobno povežu. Na Slici 2 data je strukturna šema koja predstavlja konfigurabilnu aritmetičko logičku jedinicu koja zasnovana na serijskom povezivanju trobitnih tablica preslikavanja.

Ako su operandi dužine  $n$ , onda je potrebno da se serijski poveže  $n$  tablica preslikavanja za računanje rezultata i  $n$  tablica za računanje bita prenosa ili pozajmice. Za računanje rezultata i prenosa, potrebna su dva registra (LUT1 i LUT2) u kome se čuvaju konfiguracije na osnovu kojih se izvršavaju preslikavanja. Svaki par bitova ulaznih podataka A i B se dovode na parove upravljačkih ulaza multipleksera. Bit rezultata operacije prenosa ili pozajmice se povezuje na upravljačke ulaze sledeća dva razreda multipleksera. Kod računanja prvog bita rezultata, za bit prenosa ili pozajmice uzima se ulazni bit aritmetičko logičke jedinice.

U dosadašnjim prikazima aritmetičko logičke jedinice gde se na osnovu koda bira jedan od više sračunatih rezultata, u ovoj realizaciji sve logičke komponente su u funkciji računanja rezultata. Još jedna razlika je u tome što kod realizacije aritmetičko logičke jedinice sa tablicama preslikavanja potrebno je dopremiti podatke koji predstavljaju način preslikavanja – LUT registar pre samog izvršavanja operacije.



Slika 2. - Strukturna šema konfigurabilne aritmetičko logičke jedinice preko tablica preslikavanja serijskom realizacijom

## 4.2. Serijska realizacija sa računanjem na osnovu više bitova

Prethodni prikaz serijske realizacije aritmetičko logičke jedinice na osnovu jednog bita ima manu, jer za operande dužine  $n$  bita, signal prenosa  $C_n$  se dobija nakon sračunatih svih prethodnih kašnjenja, što znači da je potrebno da signal prođe kroz  $n$  serijski poređanih multipleksera. Da bi se smanjilo to kašnjenje, moguće je promeniti veličinu tablice preslikavanja, tako da se na osnovu više bitova (grupa bitova) vrši preslikavanje pojedinačnog bita rezultata, kao i bita prenosa. Posledica bi bila ta da bi multiplekseri morali da imaju više kanala nego do sada, čime bi se povećao broj tranzistora za realizaciju ovakvog rešenja. Takođe, za svaki bit grupe bitova bi morao da postoji zaseban registar u kome bi se nalazili podaci za preslikavanje. Za računanje grupe preslikavanja veličine  $k$ , potrebno je  $k$  multipleksera sa  $2^{2k+1}$  jednobitna kanala za računanje  $k$  bitova rezultata i još jedan multiplekser sa  $2^{2k+1}$  jednobitna kanala za računanje prenosa ili pozajmice. Pored multipleksera potrebno je i  $k+1$  registara širine  $2^{2k+1}$  bitova namenjenih za podešavanje konfiguracije aritmetičko logičke jedinice. Ako pretpostavimo da je  $k$  deljivo sa  $n$ -bitnim operandima aritmetičko logičke jedinice, onda se dobija opšta formula po kojoj se računa potreban broj komponenti za konfigurabilnu aritmetičko logičku jedinicu:

Broj registara veličine  $2^{2k+1}$  bitova:  $k+1$

Broj multipleksera sa  $2^{2k+1}$  jednobitna kanala:  $(n/k) \cdot (k+1)$

## 4.3. Izvršavanje logičkih operacija u paraleli

Na strukturnoj šemi sa Slike 2 prikazane su tablice preslikavanja u minimalno dva reda (dve operacije) zbog potreba aritmetičko logičkih jedinica i to u jednom redu za izračunavanje rezultata, a u drugom redu za računanje bita prenosa ili pozajmice. Proširivanjem rešenja sa još dva operanda D i E (pored A i B) koji bi bili povezani na tablice preslikavanja koje su korišćene za računanje bita prenosa ili pozajmice, dobila bi se mogućnost vršenja dve logičke operacije u paraleli ili jednu aritmetičku operaciju. Da bi se kod aritmetičkih operacija dobio isti efekat koji je bio i pre dodavanja operandima D i E, moralo bi da važi da su parovi D i A, kao i B i E jednaki. Ovim postupkom bi se na jednostavan način ubrzala aritmetičko logička jedinica pogotovu ako se u procesoru često koriste logičke operacije.

## 5. ARITMETIČKO LOGIČKE JEDINICE REALIZOVANE KORIŠĆENJEM PROTOČNE OBRADE

Povećanjem veličine operandi nad kojima je potrebno izvršiti neku operaciju, povećava se i kritični put za određivanje bita prenosa ili pozajmice, pa se kao posledica toga javlja potreba za smanjivanjem frekvencije signala takta celog čipa čime se drastično smanjuju performanse procesora. U opštem slučaju ovakvi problemi se rešavaju uvođenjem protočne obrade u sistem, čime se za relativno malu cenu (dodavanje registara) mogu dosta povećati performanse sistema.

Serijska realizacija aritmetičko logičke jedinice je pogodna za transformisanje tako da se operacije nad podacima izvršavaju protočnom obradom kroz više jednakih faza. Ovom tehnikom se povećava brzina obrade, jer se rezultat dobija na svaki takt (kada su sve faze protočne obrade pune podacima i operacijama). Pri tome takt može da bude na višoj frekvenciji, jer je za uspešno izvršavanje potrebno da se samo sačeka propagacija signala unutar faze protočne obrade.

U nastavku rada data su dva moguća rešenja za dodavanje protočne obrade u aritmetičko logičkim jedinicama. Pri izvršavanju bilo koje operacije u aritmetičko logičkoj jedinici, svaki bit operanda i zadata operacija imaju uticaj na krajnji rezultat. Na osnovu toga se može zaključiti da svaki bit operanda mora da bude uparen sa operacijom kako bi se izvršila tražena Bulova funkcija (bilo to preko direktnih logičkih kola, bilo to preko tablica preslikavanja). Da bi se kroz protočnu obradu ostvarilo uparivanje operandi i operacije moralo bi da se obezbedi da ili podaci "teku" dok operacije ostaju na fiksnom mestu ili da operacija "teče" kroz sistem dok podaci ostaju na fiksnom mestu.

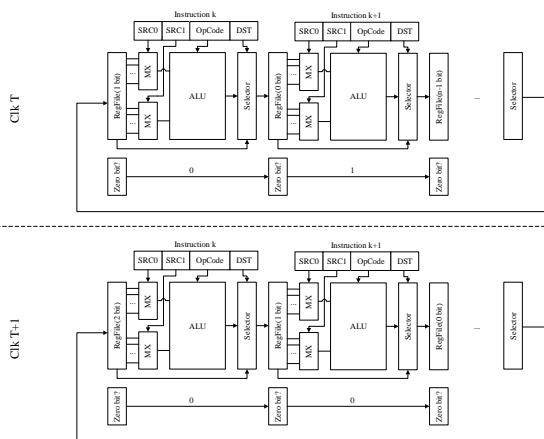
### 5.1. Propuštanje podataka kroz fiksno podešene aritmetičko logičke jedinice određene operacijom instrukcije

Na osnovu izvorišta potrebno je pročitati adekvatne bitove iz registarskog fajla. Pročitane bitove zatim treba propustiti u aritmetičko logičku jedinicu podešenu za izvršavanje operacije koja je definisana operacijskim kodom. Na kraju treba rezultat upisati u registar fajl određen određeništem. Jedno rešenje jeste da se napravi kružna protočna obrada čime bi se instrukcije fiksirale u jednoj fazi protočne obrade, dok bi se svi bitovi svih registara registarskog fajla pomerali prelazeći iz faze u faze, tako da se u svakoj fazi nalaze bitovi istog razred svih registara registarskog fajla. To bi značilo da na primer u trenutku  $clk=T$  u trenutno posmatranoj fazi bi se nalazila instrukcija  $k$  zajedno sa bitovima registara registarskog fajla sa indeksom jedan. U narednoj fazi bi se nalazila instrukcija  $k+1$  zajedno sa bitovima registara registarskog fajla sa indeksom nula i tako dalje. U svakom taku bi se u sledeću fazu prosleđivali bitovi koji se ne menjaju zajedno sa izračunatim rezultatom. Jedinicu koja vrši prosleđivanje bitova u sledeću fazu nazvaćemo *Selector*. Ova jedinica predstavlja niz, dužine kao broj registara u registarskom fajlu, dvokanalnih multipleksera koji prosleđuju ili staru vrednost bita ili sračunati rezultat iz aritmetičko logičke jedinice u zavisnosti od određeništa instrukcije. U trenutku  $clk=T+1$  podaci će se preneti u sledeću fazu tako da će se u prethodno posmatranoj fazi nalaziti instrukcija  $k$  zajedno sa bitovima registarskog fajla sa indeksom dva. U narednoj fazi bi se nalazila instrukcija  $k+1$  zajedno sa bitovima registara registarskog fajla sa indeksom jedan i tako dalje.

Nakon uparenih svih bitova podataka sa operacijom instrukcije, instrukcija treba da se izbaci iz protočne obrade i da se zameni drugom instrukcijom. Da bi se pratilo gde treba ubaciti novu instrukciju, potrebno je da



postoji registar u kome bi se čuvao podatak u kojoj fazi se nalaze bitovi registara registarskog fajla sa indeksom nula. Za tu realizaciju najbolje rešenje je da se koristi registar sa mogućnošću rotiranja bitova. Osim prethodno opisanog problema praćenje faze gde se nalaze bitovi registara registarskog fajla sa indeksom nula, problem može nastati kod operacija koje razmenjuju podatke procesora sa ostalim komponentama računarskog sistema, pa je potrebno znati po fazama kako rekonstruisati kompletan podatak.



Slika 3. – Strukturna šema aritmetičko logičke jedinice sa propuštanjem podataka kroz fiksno podešene faze određene operacijom instrukcije

Na Slici 3 prikazana je strukturna šema aritmetičko logičke jedinice sa propuštanjem podataka kroz fiksno podešene faze određene operacijom instrukcije, kao i princip rada ovakve realizacije. Dekodovana instrukcija za izvršavanje u aritmetičko logičkoj jedinici definisana je indeksima izvorišta (SRC0 i SRC1), indeksom odredišta (DST) i operacijskim kodom (OpCode).

## 5.2. Propuštanje operacija kroz fiksno podešene aritmetičko logičke jedinice određene podacima

Ako bi promenili tačku gledanja u odnosu na prethodno rešenje i umesto da podatke prenosimo iz nivoa u nivo možemo da prenosimo instrukcije. To znači da je svaka faza protočne obrade vezana za jedan razred registar fajla. Posledica toga jeste mogućnost izostavljanja jedinica

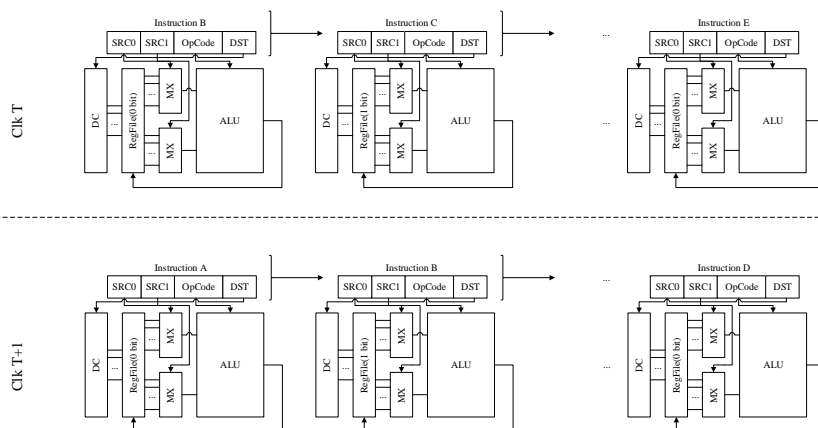
*Selector*, čime smanjujemo složenost šeme, pa i potreban broj kola za realizaciju svake faze.

Obrada podataka bi se realizovala kroz protok aritmetičko logičkih jedinica koje su serijski povezane. Pretpostavimo da u datom trenutku  $clk=T$  instrukcija B obrađuje nulte bitove registarskog fajla, instrukcija C obrađuje prve bitove registarskog fajla i tako dalje. U sledećem taktu  $clk=T+1$  sve instrukcije bi se pomerile za jedno mesto, tj. prešle bi na obradu sledećeg (višeg) bita, što bi značilo da bi instrukcija B obrađivala prve bitove registarskog fajla, instrukcija C bi obrađivala bitove registarskog fajla sa indeksom dva i tako dalje. Ovim pomeranjem bi se na mesto gde je bila instrukcija B mogla ubaciti nova instrukcija A, takođe kao posledica pomeranja, instrukcija koja je obrađivala poslednje bitove registarskog fajla bi izašla iz protočne obrade čime bi završila svoje izvršavanje. Na Slici 4 prikazana je strukturna šema aritmetičko logičke jedinice sa propuštanjem operacija kroz fiksno podešene faze određene podacima, kao i princip rada ovakve realizacije.

Realizacija aritmetičko logičke jedinice gde se operacije kreću kroz protočnu obradu je bolja u odnosu na realizaciju gde se podaci kreću kroz protočnu obradu, jer je potreban manji broj logičkih elemenata, ali je i pogodna za neke optimizacije koje su opisane u nastavku.

## 5.3. Računanje statusnih bitova

Sastavni deo aritmetičko logičkih jedinica je i računanje statusnih bitova koji služe za realizaciju uslovnih skokova ili za realizaciju višerečnih aritmetičkih operacija. Pod statusnim bitovima, smatraju se bitovi koji opisuju rezultat, kao i da li je došlo do neregularnosti pri izvršavanju operacije. Statusni bitovi su jako bitni u upravljanju toka programa. Savremeni procesori dosta instrukcija izvršavaju spekulativno dok ne saznaju da li su na ispravan način izvršili predikciju uslovnog skoka. Što ranije aritmetička logička jedinica izračuna statusne bitove to znači da će procesor biti manje u pogrešnom izvršavanju. Za računanje bitova N, C i V kod aritmetičkih operacija, potrebno je da se završi kompletno izvršavanje, tj. da se podaci ili instrukcija prođe kroz celokupnu protočnu obradu, što može da bude potencijalno veliki problem ako protočna obrada sadrži



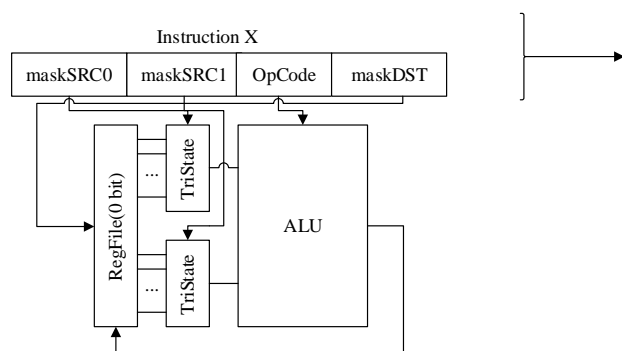
Slika 4. – Strukturna šema aritmetičko logičke jedinice sa propuštanjem operacija kroz fiksno podešene faze određene podacima

veliki broj faza. U slučaju pogrešnog spekulativnog izvršavanja potrebno je da se faze protočne obrade isprazne, a zatim i da se ponovo napune. Ako protočna obrada ima veliki broj faza, onda je punjenje svih faza sporo. Delimično rešenje ovog problema može se potražiti u tehnici izvršavanja *Simultaneous Multi-Threading* (SMT)[5][6] čime se aritmetičko logička jedinica deli između niti procesora. Ako neka nit izvršava nespekulativnu instrukciju, onda bi ta instrukcija trebala da ima viši prioritet u odnosu na spekulativne.

Kod računanja bita Z nije takav slučaj, jer pri prolasku podatka ili instrukcije kroz izvršavanje može se ranije izračunati njegova vrednost. Ako se u nekoj fazi protočne obrade naiđe na neku vrednost različitu od nule, to odmah povlači da će i konačni bit Z imati neaktivnu vrednost, pa nema potrebe za čekanjem da se prođe celokupna protočna obrada. U slučaju da je potrebno što pre saznati vrednost statusnog bita, ovom tehnikom može da se dobije ubrzanje sistema, jer je vrlo moguće da jedinica za obradu skokova čeka rezultat izvršavanja operacije. Obzirom da se u programima često ispituje da li su dva broja jednaka, a bit Z se koristi pri tom izračunavanju, onda dodavanje logike ima smisla. Još jedna optimizacija se može dobiti kod logičkih operacija. Vrednost bita N se može ranije dobiti tako što bi se na početku nezavisno vršilo izračunavanje operacije poslednjih bitova.

#### 5.4. Odabir podataka na osnovu maske

Za dobijanje još boljih performansi moguće je izbeći korišćenje multiplexera pri odabiru podataka iz registarskog fajla radi njihovog prosleđivanja aritmetičko logičkim jedinicama. Da bi se to realizovalo, potrebno je da indeksi izvorišta i odredišta ne budu definisani u vidu indeksa, već u vidu bit maske. Bit maska se dobija kao rezultat dekodera sa ulazima indeksa registara. Bit maska bi bila spojena na trostatičke bafere u slučaju izvorišta, čime bi se omogućio odabir operanada, a u slučaju odredišta, maska bi se prosleđivala na upravljačke signale *ld* registara registarskog fajla, čime bi se omogućio paralelni upis rezultata u registar.



Slika 5. – Strukturalna šema odabira podataka sa indeksima registara definisani maskom

Ovim postupkom se dobija brža faza protočne obrade, ali zato je potrebno veći broj bitova za čuvanje maske u odnosu na čuvanje indeksa, pa je sama realizacija skuplja. Na Slici 5 prikazana je strukturalna šema odabira podataka sa indeksima registara definisani maskom.

## 6. ZAKLJUČAK

U ovom radu je prikazano nekoliko realizacija konfigurabilnih aritmetičko logičkih jedinica pomoću tablica preslikavanja. Za realizaciju kompletne tablice preslikavanja ovakvo rešenje bi predstavljalo realizaciju sa velikim brojem logičkih elemenata. Iz tog razloga kod opisanog rešenja, aritmetičko logička jedinica je podeljena na serijski povezane delove čime je realizacija imala manji broj logičkih elemenata, ali se zato smanjila brzina izvršavanja operacija.

Konfigurabilne aritmetičko logičke jedinice ostavljaju mogućnost izvršavanja bilo koje logičke funkcije sa dva operanda u vidu jedne instrukcije. Ovim postupkom moguće je smanjiti ukupan broj instrukcija. U radu je pokazano je da logika unutar protočne obrade kojom bi se obavljao protok podataka zahteva veći broj logičkih kola u odnosu na broj logičkih kola kojom se obavlja protok instrukcija. Mana rešenja se ogleda u sporom punjenju svih faza u slučaju pogrešnog spekulativnog izvršavanja.

Konfigurabilne aritmetičko logičke jedinice potencijalno mogu da imaju primenu na binarnim neuralnim mrežama, gde svaka aktivaciona funkcija neuralne mreže se može predstaviti sa nekom Bulovom funkcijom. Učenjem ove mreže se može dinamički menjati način preslikavanja. Ove ideje će predstavljati dalji istraživački pravac autora, kao i uticaj konfigurabilnih aritmetičko logičkih jedinica na performanse izvršavanja pojedinačnih instrukcija, kao i među zavisnost većeg broja instrukcija.

## ZAHVALNICA

Rad na ovom projektu je delimično bio finansiran od strane Ministarstva prosvete i nauke Republike Srbije (III44009). Autori zahvaljuju na finansijskoj podršci.

## 7. REFERENCE

- [1] Z. Jovanović, Instrukcijski nivo pralelizma, *ATC Avangarda*, Beograd 2006.
- [2] Kanter, David, "Intel's Haswell CPU microarchitecture.", *Real World Technologies*, 2012.
- [3] Intel, "Intel® 64 and IA-32 Architectures Optimization Reference Manual", 2016, <https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-optimization-manual.pdf>
- [4] The Linley Group, "EPYC: Designed for Effective Performance", <https://www.amd.com/system/files/2017-06/EPYC-Designed-for-Effective-Performance.pdf>
- [5] D. Patterson, J. Hennessy, "Computer Organization and Design: The Hardware/ Software Interface", *Morgan Kaufmann*, 2013.
- [6] D. Patterson, J. Hennessy, "Computer Architecture: A Quantitative Approach", *Morgan Kaufmann*, 2011.

# Radni okvir za automatizovano modelovanje podataka

## Automated data modeling framework

Maja Milić<sup>1</sup>, Petar Bjeljac<sup>2</sup>, Marjan Maruna<sup>3</sup>, Vladimir Maruna<sup>4</sup>

MD&Profy 1,3,4

Fakultet Tehničkih Nauka – Univerzitet u Novom Sadu 2

**Sadržaj** – U radu je prikazana situacija koja se najčešće može zateći u preduzeću, i to iz nekoliko razloga: nedostatak formalno definisane i primenjene metodologije za projektovanje i razvoj struktura podataka i arhitekture preduzeća, izostanak adekvatnog alata kojim bi metodologija bila implementirana, izostanak jasno definisanog vlasništva u smislu razvoja struktura podataka, nedostatak strateškog pristupa prilikom donošenja odluka i podrške razvoju, izostanak kolaboracionog napora organizacije da implementira arhitekturu preduzeća i pravilno je sprovodi.

Opisani su kompleksni i međusobno zavisni uzroci problema, alat, metod i pristup koji se koriste kako bi problem bio rešen, uzimajući u obzir objektivna i subjektivna ograničenja. Predloženo rešenje je bazirano na modelovanju koje adresira celokupni domen, uz inkrementalno uvođenje i uz obaveznu upotrebu odgovarajućeg, jedinstvenog i integrisanog modelskog okruženja. Trenutna situacija, metodologija i razvijeno rešenje kod klijenta predstavlja se pomoću alata SAP PD (PowerDesigner). Upotrebom jasno definisanog pristupa i metoda, uspostavlja se stabilno okruženje za razvoj, projektovanje, realizaciju, implementaciju i upotrebu struktura podataka i arhitekture preduzeća, u razvojnom, testnom i produkcijom ambijentu.

**Abstract** - The paper describes the problematic situation that can most often be encountered at client organization, for several reasons: lack of formally defined and applied methodologies for design and data structure development and enterprise architecture, absence of an adequate tool through which the methodology would be implemented, lack of unequivocal and precisely defined ownership in terms of data structure development, lack of strategic approach in decision making and development support, the absence of collaborative effort from the organization to implement the enterprise architecture.

Paper also describes complex and interdependent causes of the problem, tool, method and approach that can be used to solve the problem, taking into account the objective and subjective limitations. The solution is based on modeling that addresses the entire domain, with incremental introduction and with the obligatory use of an appropriate, unique and integrated model environment. The current situation, methodology and solution are presented with SAP PD (PowerDesigner) tool. Using a clearly defined approach and methods, a stable environment for the development, design, implementation and use of data structures and enterprise architecture, have been established in the development, testing and production environment.

## 1. UVOD

Podrška informacionih tehnologija u poslovanju danas je od ključnog značaja i vrlo često preduslov za uspeh poslovanja. Sa druge strane, razvojni procesi i unapređenja podrške informacione tehnologije su vrlo često na nezadovoljavajućem nivou. Direktna posledica toga je da postignuti rezultati često nisu u skladu sa očekivanim. Kvalitet servisa podrške, dugoročno gledano se pogoršava dok kvalitet informacija i podataka opada, a znanje i pripadajuće veštine, su vrlo često parcijalne, nedostupne i izolovane.

Jasno definisan metod za upravljanje procesom uvođenja i upravljanja promenama, na jednom ili više domena poslovanja, predstavlja osnov za kvalitetno i efikasno sprovođenje svih promena.

Izostanak tačno definisane odgovornosti za vlasništvo nad poslovnim i informacionim entitetima, pri intenzivnim i kompleksnim promenama, izazvanim poslovnim i organizacionim razvojem, dovodi do postepene degradacije funkcionalnosti celokupnog informacionog sistema.

Ukoliko ne postoji prihvaćena metodologija za projektovanje i upravljanje razvojem i upotrebom struktura podataka, informacioni sistem može postati nefunkcionalan. Kao posledica, podaci mogu biti nekonzistentni, netačni, neprecizni, mogu da se ponavljaju i preklapaju, mogu biti nepotpuni. Osnovni razlog za takvo stanje leži u nemogućnosti da se kvalitetno upravlja procesom projektovanja i realizacije struktura podataka.

Izostanak celokupne organizacije poslovanja i neprepoznavanje potrebe za uvođenjem i uređenjem arhitekture preduzeća, dovodi do stvaranja ambijenta u kom ne postoji jedinstven i jednoznačan jezik koji će se koristiti između IT i poslovnih korisnika. Rešenja parcijalnih problema mogu biti svrsishodna na određenim segmentima za koja su implementirana, ali na nivou organizacije nemaju pravu vrednost. Jedan od uzroka je nedostatak i/ili nizak nivo kvaliteta komunikacije između projektnih timova i neusaglašenost sa strateškim planom razvoja celokupne organizacije.

## 2. POLAZNA SITUACIJA

Analizom trenutne situacije kod klijenta, izdvajaju se nedostaci čije je uzroke potrebno identifikovati. Neki od njih su:

- Izolovane projektne aktivnosti dokumentovane na razne načine, sporadično, neformalno, netransparentno,
- Neravnomerno dokumentovanje po tehnologijama,
- Veliki broj timova koji uporedo rade na razvoju,
- Neformalan metod za upravljanje projektima i razvojem informacione podrške,
- Nedefinisano formalno vlasništvo nad strukturama podataka,
- Sistem za upravljanje promenama nad strukturama podataka baze je najčešće deskriptivan, netransparentan, parcijalan i nepotrebno komplikovan,
- Nestandardizovana i neuređena celokupna arhitektura,
- Nedostatak kolaboracionog napora da pojedincu omogući doprinos u razvoju arhitekture preduzeća,
- Nepostojanje zajedničkog jezika i ambijenta za planiranje razvoja organizacije,
- Izostanak procene varijacije rešenja problema i posledice raznih varijacija na poslovanje,
- Izostanak dugoročnog strateškog planiranja i standardizacije celokupne arhitekture.

Znanje, veštine i iskustvo su neki od najvažnijih resursa kompanije. Fundamentalna znanja o podacima, stečena iskustvom, su u vlasništvu pojedinaca, umesto da se sakupljaju kao zajednička imovina koja se deli međusobno. Da bi kompanija napredovala i razvijala se tako da bude konkurentna na tržištu, potrebno je da ulaže u razvoj kadrova, akumulaciju i deljenje znanja, unapređenje veština i sticanje iskustva. Nedostatak formalnog načina dokumentovanja i specifikacije artifakata rešenja, dizajna i slično, kao i nedostatak formalnog načina za kontrolisano i kvalitetno upravljanje promenama dovodi do toga da znanje, veštine i iskustvo budu izolovani.

Ovo je uobičajena situacija u velikom broju kompanija. Formalizovano znanje o trenutnim strukturama baza podataka, koje se koriste, je netransparentno i vrlo privatno, parcijalno, fragmentirano što dovodi do paralize razvojnih aktivnosti.

Tehnologije su najčešće neravnomerno dokumentovane, u zavisnosti od rukovodioca i njegovih preferencija, što predstavlja dodatno otežavajuću okolnost. Uz neformalan metod vođenja, realizacija i implementacija komponenti rešenja je veoma otežana a bočni efekti takve implementacije dovode do nestabilnosti i nedostupnosti sistema.

Najčešće, u momentu uključivanja u projekat, klijenti nemaju formalno definisanu metodologiju projektovanja i upravljanja promenama, niti koriste bilo kakav alat za projektovanje. U slučaju da postoje definisana pravila imenovanja ili određene validacije, najčešće su nestruktuirane i u velikoj meri neformalne. Pri tom stroga i formalna podela na uloge, obaveze i prava članova timova, nadležnosti unutar timova, između timova i slično predstavlja jedan od glavnih nedostataka.

Ukoliko nije uspostavljeno jasno koncipirano vlasništvo u smislu razvoja i strukture podataka, ažuriranje i unapređenje deljenih struktura je otežano. To dovodi do

pojave višestrukih kopija baza podataka, suzdržavanja od promena, nepotrebno proširivanja struktura i slično.[1]

Izostanak strateškog planiranja razvoja organizacije i rešavanje problema na pojedinačnom nivou umesto globalnog sagledavanja uzroka i rešenja problema, dovodi do nekonzistentnosti rešenja. Uz to, izostanak komunikacije između timova različitih projekata, nepredvidljivost raspoloživosti različitih resursa i preklapanje projekata koji se međusobno blokiraju povećavaju potrebu za usaglašenosti celokupne arhitekture. Potrebno je primeniti revolucionarno drugačiji pristup koji obuhvata definisanje jedinstvene arhitekture i sagledavanje problema na globalnom nivou i koje će obezbediti uključivanje zaposlenih u proces planiranja.

Nedostatak strateškog, agilnog pristupa zasnovanog na modelovanju prilikom donošenja odluka i podrške razvoju dovodi do eskalacije navedenih problema i širenja njihovih posledica kroz sve domene poslovanja.

Pokušaji da se problemi reše i zahtevi ispune doradom i prilagođavanjem već gotovih rešenja i standarda, ne uzimajući u obzir konkretne potrebe, mogućnosti, resurse, znanje, budžet i motive, ne daje zadovoljavajuće rezultat.

### 3. PRISTUP

Jedna od osnovnih karakteristika pristupa koji se sprovodi je da se rad sa klijentom posmatra kao kooperacija. Zajedničkim aktivnostima, gde svako ima jasno definisanu ulogu, nastoji se da se dođe do očekivanog rešenja. Klijent vodi projekat, određuje prioritete, zahteve i njihova ograničenja.

Isporučilac rešenja pokušava da razume problem i shodno tome da savete i preporuke, trenira ljude kako bi usvojili određeni nivo potrebnog znanja, pri čemu je nivo odlučivanja i odgovornosti uvek na strani klijenta. Isporučilac obrađuje sve zahteve i pomaže prilikom utvrđivanja prioriteta istih, ali se realizuju samo jasno definisani zahtevi, nakon faze analize.

Zaposleni kod klijenta bi trebalo da usvoje određeni nivo znanja kako bi mogli da održavaju modelsko okruženje. Insistira se na modelskom pristupu, dokumentovanju svih koncepata, njihovih struktura, domena i veza u odgovarajućem alatu. Postavljen modelski ambijent je potrebno razvijati, tako da bude sposoban da pretrpi promene bez prevelikog remećenja rada sistema i održavati ga tako da obuhvati dokumentovane sve promene.

Osnova pristupa jeste da se insistira na proveru realizovanih izmena, kroz pilot projekat koji mora biti realan i relevantan kako bi učesnici bili motivisani da se angažuju, a istovremeno prihvatljivog obima kako bi mogao da se sprovede u konačnom vremenu projekta. Preporuka je da se rešenje uspostavlja fazno, inkrementalno i iterativno i time izbegne pokušaj rešavanja svih problema odjednom i istovremeno.

Ključ uspeha ovog pristupa je u konstantnom, kontrolisanom, postepenom i opreznom uvođenju promena. Agilan pristup je praktičan i fleksibilan i omogućava održivost celokupnog procesa modelovanja i realizacije modelovanja. U kontekstu poslovanja i informacionih tehnologija, ovaj pristup se bazira na definisanju strateških ciljeva i donošenju strateških odluka koje se odnose na: obim, ciljeve, zainteresovane strane na projektu i njihovu motivaciju, odgovornosti, principe i slično.

Osnovni principi kojih je potrebno pridržavati se tokom modelovanja a potom i realizacije:

- Jednostavnost – Uvoditi samo potrebne i upravljive izmene,
- Striktost i formalnost – Striktna upotreba politike modelovanja, standarda i isporuke rešenja (IMM, DADM, MDADM, DMA i EAM<sup>1</sup>),
- Postepenost – Nove izmene se uvode tek kada je organizacija za to spremna u potpunosti i to kada je prepoznata potreba za izmenama,
- Podrška – Interni kapaciteti za razvoj i transfer znanja moraju postojati,
- Heterogenost – Potrebno je problem sagledati iz više uglova i domena (Poslovnog, Informacionog, Tehnološkog, Arhitekture IKT kompanije),
- Obim – Proceniti šta je sve potrebno izmeniti i uključiti potrebne izmene koje su upravljive,
- Sveobuhvatnost – Rešenje treba da ispuni zahteve koji se odnose na sve domene i sve nivoe,
- Prilagodljivost – Rešenje koje se kreira mora biti dizajnirano tako da u slučaju novih izmena, ono bude pogodno za buduća poboljšanja i proširenja,
- Održivost – Da bi se došlo do dobrog rešenja potrebno je vreme i kontinuitet u radu i uspostaviti proces kontinuiranog razvoja,
- Automatizacija – Rešenje treba da bude automatizovano uz pomoć primenjenog alata,
- Modelski razvoj – Rešenje bi trebalo da bude u potpunosti podržano i upravljivo kroz modelovanje,
- Dvostruko upravljanje – Upravljanje podacima i meta podacima arhitekture i
- Integrisanost – Mogućnost integrisanja sa ostalim alatima.

#### 4. METODOLOGIJA

Predložena metodologija predstavlja modifikacije različitih metodologija, upotpunjene višegodišnjim iskustvom i rezultatima dobre prakse. Sprovodi se kroz nekoliko faza i u potpunosti je nezavisna od alata koji se koriste.

##### Uvodna faza obuhvata:

- Donošenje odluka o tome ko su učesnici projekta, koje su sve zainteresovane strane, njihovi motivi i potrebe, nivo učešća (uloga) učesnika projekta,

- Definisanje kompletnog skupa zahteva, kako funkcionalnih tako i nefunkcionalnih,
- Definisanje prioriteta, kako lokalno tako i globalno,
- Definisanje pokazatelja uspeha iz različitih uglova posmatranja, rizika i principa,
- Prikupljanje svih zahteva za koje je naručilac zainteresovan, kako bi se donela informisana odluka,
- Proces određivanja prioriteta zahteva, prioriteta lokalno na nivou pojedinca i globalno na nivou kompanije.

Svi zahtevi određenog prioriteta ulaze u procenu kompleksnosti. Zahteve koji nisu ušli u realizaciju projekta, i dalje treba držati u evidenciji kao osnov sledećim iteracijama razvoja.

##### Proizvodi: Model zahteva

##### Faza analize obuhvata:

- Konsolidaciju svih prikupljenih zahteva po prethodno definisanim prioritetima,
- Definisanje predloga rešenja,
- Definisanje inicijalnog plana projekta.

Potrebno je doći do konsenzusa koji podrazumeva kompromis u smislu postojeće prakse i rešenja. Svi učesnici na kraju projekta će koristiti isto rešenje i metod tako da samo rešenje i postojeća praksa moraju da pretrpe određene promene, što je naročito izazovno u neuređenom ambijentu.

**Proizvodi:** Model zahteva, Metodologija za modelovanje celokupne, Dizajnerske odluke i alternative, Predlog rešenja i inicijalni plan projekta

##### U fazi dizajna:

- Definiše se informacioni meta model - IMM, koncepti koji se koriste, struktura koncepata kroz njihove atribute, domeni, podrazumevane vrednosti, relacije, različiti pogledi (view point), validaciona pravila po grupama, pravila automatizacije,
- Definisanje načina i metode za: upravljanje samim procesom razvoja, upravljanje i propagaciju promena, integraciju sa ostalim okruženjima (za razvoj ili upravljanje zahtevima za izmene),
- Definisanje pravila za kontrolu ispunjenosti zahteva (validacija), automatizaciju i transformacije,
- Formiranje potrebnog modelskog sadržaja, biblioteka i modelskih šablona,
- Uvoz potrebnog sadržaja koji se referencira u modelskom ambijentu, kao na primer organizaciona struktura, entiteti višeg nivoa i slično,
- Formiranje slučajeva korišćenja rešenja a time i osnove za testiranje i primopredaju rešenja,
- Osnovno strukturno proširenje meta-modela SAP PD (PowerDesigner).

<sup>1</sup> IMM – Information Meta Model, DADM – Data Architecture Development Method, MDADM - Meta Data Architecture Development Method, DMA - Data

Modeling Architecture i EAM - Enterprise Architecture Model



**Proizvodi:** Informacioni meta model (IMM), Model arhitekture preduzeća (EAM), Modelska arhitektura i specifikacija integracija, Modelski sadržaji biblioteka i šablona, Specifikacija za proširenja modela, Specifikacija za proširenja datoteka za konfiguraciju i upravljanje bazom podataka, Specifikacija za integracione komponente, Uputstva za rad, upotrebu i instalacije, Slučajevi korišćenja i zapisnik testiranja

U fazi realizacije/implementacije se realizuje ono što je u fazi dizajna projektovano:

- Realizacija komponenti rešenja proširenjem SAP PD (PowerDesigner) meta-modela, prema zadatim pravilima imenovanja, validacije, automatizacije i transformacije,
- Realizacija komponenti rešenja proširenjem komponente za konfiguraciju i upravljanje bazom podataka,
- Dalje unapređenje modelskog sadržaja, biblioteka i šablona,
- Migracija modelskih sadržaja,
- Razvoj i uspostavljanje modelske arhitekture (modeli),
- Uspostavlja se takozvano “trenutno” („As - Is“) i “željeno” („To – Be“) stanje koja uključuju sve definisane domene i entitete iz prethodnih faza,
- Sprovođenje pilot projekta, jednog ili više, radi potvrde realizovanog,
- Sprovođenje testiranja prema prethodno definisanim slučajevima korišćenja,
- Prenos znanja i veština, realizacija radionica, potrebne obuke i slično.

**Proizvodi:** Proširenja modela, Proširenja datoteka za konfiguraciju i upravljanje bazom podataka, Integracione komponente, Pilot projekat, Uputstva za rad, upotrebu i instalacije, Korisnički profili, zapisnik o testiranju, zapisnik o održanoj obuci i slično.

U metodologiji se primenjuje tzv. agilni, tj. inkrementalni i iterativni pristup u razvoju i upravljanju rešenjem. Inkrementalni razvoj predstavlja razvoj rešenja korak po korak kroz sprintove. Sprint predstavlja samostalnu zaokruženu jedinicu razvojnog procesa u kojoj je potrebno obaviti određene aktivnosti. [2][3] Svaki sprint kao rezultat daje određene proizvode, opisane u **Tabela 1. Prikaz proizvoda i njihov opis**. Proizvod se isporučuje u radnim paketima. Radni paketi predstavljaju skup aktivnosti koji čini logičku celinu i najčešće daju jedan dobar proizvod (prikupljanje zahteva, konsolidacija, analiza i prioriteta, konsenzus rešenja i dobre prakse, skup validacija po tehnologijama, skup transformacija, skup automatizacija...). Svaki sprint pojedinačno ima sve gore navedene faze kroz koje je potrebno proći.

Iterativni pristup se odnosi na način vremenskog planiranja sprintova, gde se kroz svaki sprint rešenje iterativno usavršava. Usitnjavanjem razvojnog procesa na sprintove smanjuje se mogućnost da krajnje rešenje ne bude očekivanog kvaliteta.

U ovoj fazi rade se najmanje dva pilot projekta. Prvi, čim se uspostavi osnovna funkcionalnost kako bi se proverili definisana arhitektura i koncepti. Drugi pilot projekat

označava primopredaju. Shodno tome, pilot projekti se rade zajedničkim naporom sa klijentom. Ova faza se sprovodi sa timom klijenta koji je obučen za rad sa SAP PD (PowerDesigner). Obezbeđivanje stabilnog, korisnog i sveobuhvatnog okruženja jedan je od glavnih preduslova za uspešno primenjeno i korišćenu praksu modeliranja podataka. Istovremeno, efikasna, sveobuhvatna, brza i precizna podrška i upravljanje tim rešenjem je podjednako važna.

**Faza testiranja** integrisano se sprovodi sa prethodnim fazama, i to kroz sve sprintove. Na osnovu prethodno definisanih korisničkih slučajeva, proverava se:

- Nakon izrade proširenja i izmene datoteka za upravljanje i konfiguraciju baze podataka, programer sprovodi testiranje pojedinačnih komponenti i njihovih metoda kako bi se obezbedilo da metode nemaju greške u kodu i da odgovaraju definisanoj specifikaciji,
- Nakon testiranja pojedinačnih komponenti rešenja, isporučilac rešenja proverava rad svih komponenti u integrisanom rešenju,
- Interna provera da li sistem ispunjava definisane zahteve i da li je u skladu sa poslovnim procesima (slučajevima korišćenja),
- Korisnik testira rešenja i provera da li je rešenje prihvatljivo tj. da li je u skladu sa definisanim zahtevima i poslovnim procesima.

Rešenje testira isporučilac rešenja i korisnici:

- Sprovode se testovi gde se rešenje posmatra kao „crna kutija“ („black box“). Ovi testovi se odnose na testiranje, kako funkcionalno tako i nefunkcionalno, gde osoba koja testira, nema uvid u internu strukturu rešenja, njegov dizajn i implementaciju. Ovakvim testovima se proverava da li su implementirane funkcije dobre i da li neka funkcija nedostaje, vizuelne greške u rešenju, greške u struktura podataka, na koji način su greške prezentovane, kako se rešenje ponaša prilikom inicijalizacije grešaka itd.
- Sprovode se testovi gde se rešenje posmatra kao „bela kutija“ („white box“). Osoba koja testira ima uvid u dizajn i implementaciju rešenja, i izborom različitih ulaza proverava kakvi i koji su izlazi rešenja.

**Proizvodi:** Slučajevi korišćenja i zapisnik o testiranju

## 5. PROIZVODI

Naziv/Mapiranje na alat	Opis
<b>Informacioni meta model (IMM)/OOM</b>	Model pomaže pri sprovođenju pristupa i metodologije i daje dobru osnovu za definisanje upravljivog modelskog okruženja. U IMM modelu opisani su svi koncepti i njihove strukture, atributi i veze, svi pogledi, validacije i automatizacije.

<b>Model arhitekture preduzeća/EAM</b>	Model pomaže da se vidi jasnija slika zašto su određeni koncepti povezani i na koji način u okviru celokupne organizacije. Model ne definiše kako komponente izvršavaju svoju funkciju već prikazuje njihovu kooperaciju i kolaboraciju.
<b>Model zahteva</b>	Model zahteva predstavlja konsolidovanu specifikaciju zahteva sa usaglašenim prioritetima, organizovanu po radnim paketima. Model zahteva sadrži sve zahteve klijenta kako bi se stekao uvid u celokupnu problematiku.
<b>Modelska arhitektura i specifikacija integracija/PD Enterprise Architecture Model – EAM</b>	Modelska arhitektura predstavlja metod za definisanje vrste modela koji će se koristiti, pravila imenovanja, pravila čuvanja modela i strukture datoteka u kojima se čuvaju. Metod definiše i specifikacije integracija koje je potrebno omogućiti. Modelska arhitektura omogućava pravilnu upotrebu alata, iskorišćavanje njegovih mogućnosti na najbolji mogući način i upravljivo dokumentovanje celokupnog postupka i metodologije, kao i dobru osnovu za jednostavniji nastavak daljih projekata.
<b>Metodologija za modelovanje/ PD Requirement Model – RQM i MS Word .docx</b>	Metodologija za modelovanje omogućava definisanje i postavljanje dobre osnove za rešenje koje se primenjuje, iterativno i inkrementalno uvođenje promena u održivom i kontrolisanom ambijentu. Metodologija omogućava upravljanje promenama na odgovarajući način kako bi se održao kvalitet rešenja i omogućila njegova nadogradnja.
<b>Dizajnerske odluke i alternative/PD Requirement Model – RQM</b>	Skup rešenja koje isporučilac predloži klijentu kao najbolje rešenje, zajedno sa njegovim pozitivnim i negativnim aspektima, vremenom potrebnim za razvoj i implementaciju, uticajem na projekat i rad na istom, kao i testiranje. Skup rešenja uključuje i skup alternativnih rešenja i njegovih karakteristika.
<b>Modelski sadržaj/RQM,</b>	Modelski sadržaj se odnosi na sve modelske datoteke koje se

<b>PDM, LDM, CDM, DMM<sup>2</sup></b>	definišu, počevši od zahteva do IMM-a, proširenja modela i ostalih fajlova. Modelski sadržaj omogućava postavljanje integrisanog modelskog ambijenta.
<b>Proširenja modela/RQM i .xem datoteke</b>	Proširenja modela koja omogućavaju prilagođavanje radnog okruženja potrebama korisnika.
<b>Proširenja datoteka za konfiguraciju i upravljanje bazom podataka/RQM i PD .xdb datoteke</b>	Izmene koje se odvijaju nad već postojećim datotekama za konfiguraciju i upravljanje bazom podataka (.xdb datoteke). U datoteke je potrebno uvoditi samo potrebne izmene kako bi rešenje moglo da ispunji zahteve.
<b>Integracione komponente/RQM i .xem datoteke</b>	Komponente sa kojima je potrebno integrisati postavljeni modelski ambijent. Komponente omogućavaju integraciju sa drugim rešenjima i alatima. Podržavaju sve razvojne i implementacione aktivnosti koje mogu da obuhvate izmene modela.
<b>Pilot projekat/PD Project</b>	Pilot projekat predstavlja svojevrsan instrument evaluacije definisanog rešenja. Pokreće se sa ciljem da se proverí da li je rešenje dobro osmišljeno i da se isprave potencijalne greške i nedostaci u realnom ambijentu. Pilot projekat omogućava testiranje definisanog i implementiranog rešenja u stvarnom ambijentu sa ciljem provere i unapređenja rešenja.
<b>Uputstva za rad, upotrebu i instalacije/Word, Excel i ostali standardni formati(.docx, .xlsx)</b>	Uputstva za instalaciju alata, njegovu pravilnu upotrebu i ostala uputstva za rad koja su potrebna klijentu prilikom instalacije, upotrebe i pravilnog sprovođenja metodologije i pristupa.
<b>Slučajevi korišćenja/Word</b>	Dokument sa svim slučajevima korišćenja koji se koristi za proveru funkcionalnosti rešenja. Dokument omogućava pravilno testiranje i proveru funkcionalnosti rešenja. Svaki slučaj korišćenja ima sekciju koja sadrži podatke o testiranju. Nakon svakog testiranja, potrebno je popuniti ove sekcije.

Tabela 1. Prikaz proizvoda i njihov opis

Requirement Model – RQM, Physical Data Model – PDM, Conceptual Data Model – CDM, Object Oriented Model –

OOM, Data Movement Model – DMM, Logical Data Model – LDM, PD Enterprise Architecture Model - EAM

## 6. IMM MODEL

Naziv Objekta	Mapiranje na alat
<b>Koncepti</b>	Koncepti su prikazani klasama objektno orijentisanog modela.
<b>Struktura koncepata</b>	Strukture atributa su prikazane kroz attribute klase koji imaju svoje tipove podataka, domene i podrazumevane vrednosti
<b>Relacije između koncepata</b>	Veze između koncepata su prikazane asocijacijom, agregacijom ili kompozicijom u zavisnosti od odnosa koncepata
<b>Validaciona pravila po grupama</b>	Validacije su opisane kroz posebno proširenje napravljeno specijalno za njihovo opisivanje. Za validacije je potrebno definisati: <ul style="list-style-type: none"> <li>•Kategoriju (npr. imenovanja ili ograničenja),</li> <li>•Nivo validacije (npr. Upozorenje ili greška),</li> <li>•Jedinstveni kod validacije i naziv koji odgovara definisanim pravilima imenovanja,</li> <li>•Obaveznost validacije,</li> <li>•Uslovi pod kojima se dešava,</li> <li>•Odgovarajuće poruke koje je potrebno ispisati korisniku nakon validacije,</li> <li>•Instrukcije za korekciju ili automatsku korekciju.</li> </ul>
<b>Pravila Automatizacije</b>	Automatizacije su opisane kroz posebno proširenje napravljeno specijalno za njihovo opisivanje. Prilikom opisa automatizacije, pri tom poštujući definisana pravila imenovanja, potrebno je definisati: <ul style="list-style-type: none"> <li>•Kontekst automatizacije, tj. kada, kako i koliko puta se izvršava,</li> <li>•Uslove koje automatizacija treba da ispuni,</li> <li>•Parametre,</li> <li>•Korake automatizacije,</li> <li>•Izuzetke,</li> <li>•Rezultat i to sve poštujući definisana pravila imenovanja.</li> </ul>
<b>Različiti pogledi (view point)</b>	Dijagrami, liste, matrice zavisnosti i izveštaji.

Tabela 2 Prikaz elemenata IMM-a i njihov opis

**Upravljivi pogledi** - Trenutni pregled različitih nivoa arhitekture sa potrebnim nivoom detalja koji se predstavlja široj publici. Zahteva konstantno ručno ažuriranje.

**Trenutni pregled** – Kratkotrajni pregled arhitekture na različitim nivoima sa potrebnim nivoom detalja, kreiran za određenu svrhu i ciljnu grupu. Mogu biti generisani upotrebom automatskih procedura i skupa uslova koje je potrebno da ispune.

**Standardni izveštaji** - Trajni izveštaji iz jednog ili više modela koji prikazuju određene aspekte i predstavljaju se široj ali izabranoj grupi.

**Liste** – Kratkotrajna lista instanci određenih koncepata i njihovih atributa na različitim nivoima. Kreira se zbog određene namere da se koncepti distribuiraju izvan SAP PD (Power Designer) okruženja. Pogodni su izvoz u CSV, XML datoteke i mogu se koristiti za integracije sa drugim alatima.

**Matrice zavisnosti** - Direktne ili indirektno zavisnosti između instanci dva izabrana koncepta. Mogu prikazivati zavisnosti između koncepata različitih nivoa arhitekture (modela), direktne zavisnosti određenih relacija ili jednostavne i kompleksne zavisnosti između dva izabrana koncepta.

**Analiza uticaja** - Predstavlja mrežu zavisnosti uticaja u oba smera, objekte koji utiču i objekte na koje utiču određene akcije nad objektima. Odnose se na konkretno poslovno pitanje.

## 7. ZAKLJUČAK

Zajednički, jednoznačan jezik i visok nivo komunikacije među članovima tima i klijenta, jedinstven pristup i metodologija, jasno određeno vlasništvo nad podacima, precizno definisane i delegirane uloge i njima dodeljene odgovornosti, deljenje znanja i konstantno unapređenje kapaciteta, spadaju među najbitnije faktore uspeha prilikom konsolidacije i integracije (do tada) neorganizovanih, neodržanih, parcijalnih i nekonzistentnih podataka i skupova podataka. Do sada stečena iskustva i primeri dobre prakse, pokazali su da je agilna (inkrementalna i iterativna) pristup u pet faza, uz aktivnu participaciju klijenta (naročito u fazi prikupljanja zahteva i njihove konsolidacije) vodi ka uspostavljanju integrisane, jedinstvene arhitekture preduzeća i deljene strukture podataka.

## LITERATURA

- [1] DAMA International, "DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK)", ISBN: 9781935504023
- [2] Shore, J, "The Art of Agile Development", ISBN: 978-0-596-52767-9
- [3] Schwaber, K, "Agile Project Management with Scrum", ISBN: 978-0-7356-1993-7

# REGULATORNI IZAZOVI U PROCESU UVOĐENJA M2M/IoT USLUGA REGULATORY CHALLENGES IN THE PROCESS OF M2M/IoT SERVICES IMPLEMENTATION

Zoran Janković, Milosav Grubović

Regulatorna agencija za elektronske komunikacije i poštanske usluge

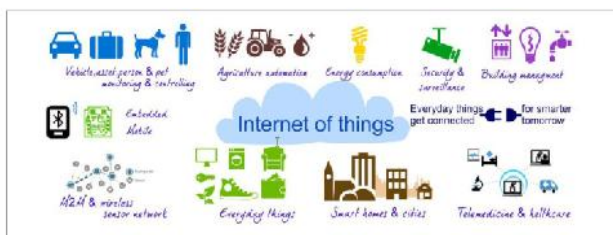
**Sadržaj** – U ovom radu predstavljena je analiza M2M/IoT usluga kao i procena i perspektiva obezbeđivanja okruženja koji će rezultovati održivom konkurencijom, međusobno usklađenih elektronskih komunikacionih servisa i dobiti za krajnje korisnike. Daje se i procena da li će i u kojoj meri M2M/IoT usluge zahtevati poseban tretman u budućoj regulativi s obzirom na ulogu Regulatorne agencije za elektronske komunikacije i poštanske usluge. Prestavljeno je i trenutno stanje u Republici Srbiji po pojedinačnim pitanjima.

**Abstract** – In this paper analysis of the M2M/IoT services is presented as well as the estimate and perspective of establishing the environment which will result sustainable competitions, electronic communications services interoperability and end-user benefits. Estimations is given if and in what extent will M2M/IoT services require special treatment in future regulative which Regulatory Agency of Electronic Communications and Postal Services has ingerences. Current status in the Republic of Serbia regarding specific topics is given.

## 1. UVOD

U ovom trenutku, M2M/IoT servisi imaju karakteristike automatizovane komunikacije podataka između udaljenih uređaja i mali obim saobraćaja koji se karakteriše sporadičnim odnosno nepravilnim i neritimničnim periodima komunikacije. Uređaji koji se koriste u procesu M2M/IoT su najčešće malih dimenzija i relativno jednostavni po konstrukciji. Mogu biti nepokretni (npr. statični merači potrošnje) ili mobilni (u vozilima). Najčešće se uređaji proizvode za svetsko tržište i mogu biti namenjeni za globalnu mobilnost. Radni vek uređaja se projektuje na više godina a jedan od razloga je da s obzirom na brojnost ugrađenih uređaja, zamena često predstavlja veliki trošak.

Glavne oblasti primene M2M/IoT usluga su u: vozilima, pametnim meracima potrošnje (struja, gas...), pametnim zgradama i gradovima, industriji, poljoprivredi, e-zdravstvu itd.



Slika 1: Oblasti primene M2M/IoT

## 2. USLOVI ZA IMPLEMENTACIJU M2M/IOT USLUGA

Da bi se stekli neophodni uslovi za efikasnu implementaciju, nesmetan rad i adekvatno održavanje i proširenje M2M/IoT usluga, potrebno je ispunjenje nekoliko zadataka.

Prvi uslov za punu primenu M2M/IoT usluga je obezbeđivanje adekvatnih tehničkih resursa. Ovo podrazumeva rešavanje pitanja dodele i korišćenja frekvencija, numeracije i IP adresa. Dalje je neophodno prilagođavanje regulatornom okviru EU (naročito je važno pitanje *roaming*-a i mogućnost promene mrežnog operatora). Na kraju, važno je i prihvatanje od strane krajnjih korisnika što podrazumeva obezbeđivanje transparentnosti, privatnosti, zaštite podataka i sl.

Trenutno najrasprostranjenija rešenja za primenu M2M/IoT servisa su ona koja su bazirana na mobilnoj mreži. Razlog za to je što je trenutno ta tehnologija dominantna, ali treba naglasiti da postoje i rešenja bazirana na drugim tehnologijama kao što je fiksna veza ili drugačiji tipovi bežičnih komunikacija. U slučaju bežične komunikacije nameće se pitanje frekvencijskog opsega koji se koristi, a bez obzira na tehnologiju i pitanja identifikatora (brojeva ili IP adresa). Ipak, ne postoji potreba za globalnim identifikatorom za sve M2M/IoT uređaje. Razlog za to je što postoje i oni uređaji koji nisu povezani na javnu komunikacionu mrežu.

Resursi koje treba obezbediti za nesmetano funkcionisanje M2M/IoT usluga su:

- frekvencijski opseg – za bežičnu komunikaciju M2M uređaja;
- numeracija (telefonski brojevi) – kada je M2M uređaj vezan na javnu mrežu;
- IP adrese – ako se kao identifikator koristi ovaj tip.

Frekvencije i numeracija su u nadležnosti nacionalnih regulatornih tela za elektronske komunikacije (u Republici Srbiji RATEL - Regulatorna agencija za elektronske komunikacije i poštanske usluge), dok je upravljanje IP adresama u ingerenciji drugih tela (na svetskom nivou ICANN - *Internet Corporation for Assigned Names and Numbers*; na nivou Evrope: RIPE NCC - *Réseaux IP Européens Network Coordination Centre*; u Republici Srbiji RNIDS - *Registar nacionalnog internet domena Srbije*).



### 3. FREKVENCIJSKI SPEKTAR

Ne postoji jedinstveni zahtev za frekvencijskim opsegom već to umnogome zavisi od specifične prirode servisa. Na primer, niži frekvencijski opsezi omogućavaju šire pokrivanje i bolju penetraciju u zgradama. Sa druge strane, licencirani opsezi za privatne, profesionalne ili javne mobilne mreže namenjene za pruženje elektronskih komunikacionih usluga obezbeđuju pouzdanu isporuku podataka u poređenju sa nelicenciranim opsezima. Na kraju, može postojati i potreba za specijalno dodeljene, namenske opsege za određenu vrstu primene da bi se osigurala efikasnost – na primer za specifične zahteve gde se traži vrlo dug baterijski rad uređaja.

U zavisnosti od konkretnog tipa i osobina M2M/IoT usluga, bira se i najpogodnija tehnologija koja će biti primenjena. To dalje uslovljava i određuje koji delovi frekvencijskog spektra će se koristiti.

- 3G i 4G (u budućnosti i 5G) tehnologije mobilnih mreža se trenutno široko koriste i najzastupljenije su u primeni M2M/IoT servisa. Najkarakterističniji primer su bežične PoS (*Point-of-sale*) aplikacije.
- Frekvencijski opsezi ispod 1 GHz se koriste za primene kada je neophodno koristiti uređaje malih snaga i široke pokrivenosti. Ovde je moguće koristiti kako licencirane tako i nelicencirane frekvencijske opsege.
- Postojeće *WiFi* i *Bluetooth* tehnologije (kao i njihove buduće unapređene verzije) se koriste za potrebe lične komunikacije i komunikacije na malim udaljenostima. Pogodne su za široko rasprostranjene potrošačke servise (npr. vezani za zdravlje i održavanje kondicije).
- Satelitske tehnologije mogu biti korišćene, a trenutno su aktuelne kod avio kompanija i firmi koje se bave logistikom.

Po uputstvu u izveštaju Evropske komisije [1] se navodi da je najbolje realizovati zahteve za M2M/IoT usluge u frekvencijskom spektru ispod 1 GHz. Za M2M/IoT usluge koje koriste mobilne tehnologije, može se koristiti bilo koji harmonizovani opseg za terestrijalne sisteme namenjen za javne komunikacione servise. Ovi opsezi uključuju 800 MHz, 900 MHz, 1450 MHz, 1800 MHz, 2 GHz, 2.6 GHz i 3.4 – 3.8 GHz a u perspektivi i 700 MHz opseg.

Kada su u pitanju nelicencirani frekvencijski opsezi koji mogu da se koriste za M2M/IoT usluge, oni su harmonizovani odlukom Evropske komisije [2] i CEPT preporuke [3]. Tehnologije koje se koriste su *WiFi* i *Bluetooth*, kao i frekvencije na 868 MHz koje se koriste za M2M uređaje malih snaga i široke pokrivenosti. U Evropi takođe postoje i PMR/PAMR frekvencijski opsezi između 30.01 MHz i 942 MHz koji se mogu koristiti za M2M/IoT usluge.

S obzirom na brz rast M2M/IoT usluga neophodno je preduzeti sledeće korake koji će omogućiti nesmetan rad u narednom periodu:

- Modifikovati obaveze iz licenci u cilju omogućavanja upotrebe M2M/IoT tehnologija unutar postojećih već dodeljenih opsega.
- Modifikovati uslove korišćenja određenih opsega za novu primenu.
- Izanalizirati dodatna tehnička rešenja. Na primer:
  - iskorišćenje slobodnih delova frekvencijskog spektra (*gap*-ova) koji se trenutno ne koriste a nalaze se između dva opsega; npr *gap* između transmisija digitalne terestrijalne televizije <1 GHz
  - korišćenje *duplex gap*-a na nacionalnom nivou 700MHz. *Duplex gap* je deo nekorišćenog spektra između opsega za *uplink* i *downlink* transmisija FDD (*Frequency Division Duplex*) sistema.

#### Stanje u Republici Srbiji:

Očekuje se da se po usvajanju novog Zakona o elektronskim komunikacijama, obavezama iz licenci doda i omogućavanje M2M/IoT usluga. U skladu sa Planom namene radio-frekvencijskih opsega [4] i Pravilnikom o načinu korišćenja radio-frekvencija po režimu opšteg ovlašćenja [5] definisani su nespecificirani uređaji kratkog dometa (SRD – *Short Range Devices*) koji su prevashodno namenjeni za telemetriju, telekomandu, alarme i druge slične primene. Ovo upravo pripada M2M/IoT uslugama i za njihovu primenu je predviđen opseg frekvencija od 863-870 MHz.

### 4. NUMERACIJA

Kada su u pitanju resursi potrebni za identifikaciju M2M uređaja, ograničenja se mogu pojaviti samo kod onih servisa koji koriste javnu komunikacionu mrežu. Ti ograničeni resursi su: telefonski brojevi, specijalni kodovi i IP adrese. Primene koje ne koriste javnu komunikacionu mrežu ne koriste ove resurse i tu ograničenja nema, npr. MAC adrese.

Za korišćenje M2M/IoT usluga koji se povezuju na javne komunikacione mreže koriste se formati brojeva i pravila koja je propisala Međunarodna unija za telekomunikacije (ITU - *International Telecommunication Union*) svojim preporukama E.164 i E.212. Na kratak i srednji rok sigurno, a verovatno i na duži, korišćenje ovih brojeva će ostati dominantan način identifikacije M2M entiteta. Tek u daljoj perspektivi u budućnosti, IPv6 adrese će postati preovlađujući način identifikacije. Numeracija koja se koristi u M2M/IoT servisima koji se povezuju na javne komunikacione mreže može biti sledećih tipova:

#### E.164 brojevi

- Nacionalni: iz plana numeracije sa međunarodnim prefiksom pojedinačnih država.
- Globalni: specijalni međunarodni brojevi sa prefiksom +882 i +883. To su kodovi koji se ne dodeljuju pojedinačnim državama već su namenjeni za globalno korišćenje. Trenutno je dodeljeno 47 kodova ovog tipa operatorima koji imaju servise koje pružaju na globalnom nivou. Dodeljuje ih ITU.

## E.212 brojevi

- **Nacionalni:** IMSI (*International Mobile Subscriber Identity*) broj se sastoji od tri dela : MCC (*Mobile Country Code*) koji dodeljuje ITU (Republici Srbiji je dodeljen kod 220); MNC (*Mobile Network Code*), dužine 2 cifre, koji dodeljuje RATEL i može biti od 00 do 99 i MSIN (*Mobile Station Identification Number*), dužine najviše 10 cifara, koji je u nadležnosti operatora koji imaju dodeljen MNC kod. MNC kod u kombinaciji sa MCC kodom jednoznačno određuje elektronsku komunikacionu mrežu a MSIN jednoznačno identifikuje pojedinačnog korisnika u okviru elektronske komunikacione mreže operatora.

MCC	MNC	MSIN
3 cifre	2 cifre	Najviše 10 cifara
IMSI broj		
Najviše 15 cifara		

Tabela 1. Struktura IMSI broja

- **Globalni:** ITU dodeljuje MNC kodove sa specijalnim MCC 901 koji je namenjen za globalne operatore.

Precizno definisana pravila, jednostavna implementacija i (do sada) dovoljno dostupni resursi numeracije glavni su razlog što se trenutno i u narednom srednjoročnom periodu dominantno koriste ovi tipovi numeracije kao identifikatori.

U ovom trenutku, dostupni resursi E.164 brojeva nisu ugroženi u pogledu novih zahteva za M2M/IoT usluge. Ovo pitanje svaki nacionalni telekomunikacioni regulator treba da analizira nezavisno i da nađe rešenje pogodno za svoju situaciju. Ova rešenja mogu biti: otvaranje posebnog opsega za M2M/IoT usluge ili povećanje opsega mobilnih brojeva.

Kad su u pitanju E.212 brojevi, postoji rizik iscrpljivanja dostupnih MNC kodova, s obzirom da je, najčešće, samo 100 MNC kodova na raspolaganju svakoj državi (odnosno po MCC kodu). Ranije preporuke ITU za kriterijum dodele MNC kodova na nacionalnom nivou su ublažene (Aneks B preporuke E.212). Osim operatora mobilnih mreža, satelitskih mreža i nekih aplikacija u fiksnim mrežama, preporučeno je da se dodela proširi i na druge operatore (na primer M2M i eCall) pod uslovima i procedurama koje bi propisali nacionalni telekomunikacioni regulatori.

Važno pitanje je i ekstra-teritorijalna upotreba nacionalnih E.164 i E.212 brojeva. Mnogi M2M uređaji namenjeni su za globalnu primenu odnosno za svetsko tržište a pojedine primene (npr. u vozilima) po prirodi servisa predodređeni su da se koriste i van matične države. Ovo pitanje se razmatra u dokumentima CEPT-a [6]. Generalni stav je da:

- Države generalno treba da odbiju dodelu E.164 brojeva iz svog nacionalnog plana numeracije ako je kao cilj korišćenje tih brojeva u drugoj državi na permanentnoj bazi.

- Države u principu ne treba da dozvoljavaju korišćenje E.164 brojeva koji pripadaju drugoj državi na svojoj teritoriji na permanentnoj bazi.
- Ekstra-teritorijalna upotreba brojeva može biti dozvoljena u pojedinačnim opravdanim slučajevima upotrebe koji će biti definisane ECC odlukom. Potencijalni kandidati su, između ostalog i M2M/IoT usluge.

Alternativno rešenje ovog problema je u korišćenju globalnih resursa koje dodeljuje ITU: globalni E.212 (IMSI sa MNC pod MCC 901) i E.164 (+882 i +883) brojevi.

### Stanje u Republici Srbiji:

Planom numeracije Republike Srbije [7] predviđen je poseban opseg (prefiks 72 – usluga za komunikaciju između uređaja) za M2M primene. Ovaj opseg obezbeđuje 10 miliona brojeva, a po potrebi, moguće je otvoriti i nove opsege (npr 73, 74, 75) izmenom Plana numeracije. Opseg 72 je skoro u potpunosti slobodan, odnosno ne koristi se u punoj meri za M2M/IoT usluge.

Može se pretpostaviti da se zahtevi za brojeve kod M2M/IoT usluga rešavaju tako što se koristi numeracija koja je dodeljena operatorima mobilnih mreža. Svaki od 3 postojeća operatora imaju po tri 6x opsega što daje kapacitet od (i više nego dovoljnih) 30 miliona brojeva koji mogu biti upotrebljeni za klasične dodele brojeva mobilnim pretplatnicima za usluge prenosa glasa, poruka i podataka ali i za M2M/IoT usluge.

U pogledu MNC kodova, ukupno je dodeljeno 6 MNC kodova. Uslov za dodelu MNC koda imaju operatori mobilnih mreža i virtuelnih mobilnih mreža kao i za neke aplikacije u fiksnim mrežama. Trenutno operatori koji bi pružali samo M2M/IoT usluge nemaju mogućnost dodele MNC koda. Ako bi bilo potrebe za relaksacijom uslova dodele i za ove operatora bila bi neophodna izmena Plana numeracije uz oprezan pristup da bi se zaštitilo iscrpljivanje nacionalnog resursa od 100 MNC kodova.

## 5. IP ADRESE

Kao identifikatori, osim tradicionalnih brojeva i kodova mogu se koristiti i IP adrese. U ovom trenutku one nisu preovlađujući način identifikacije M2M uređaja i uglavnom se koriste za M2M/IoT usluge na fiksnim lokacijama kao i u bežičnim LAN mrežama.

Postojeći 32-bitni IPv4 koji obezbeđuje identifikaciju teoretskih  $2^{32}$  adresa postaje nedovoljan pa se uveliko radi na prelasku na 128-bitni IPv6 sa  $2^{128}$  adresa. Očekuje se, da će oba standarda koegzistirati paralelno u narednim godinama sve dok IPv6 ne postane dominantan (procena: narednih 5-10 godina). U ovom trenutku, oko 30% mreža u EU podržava IPv6 [8]. Kada IPv6 postane dominantan, problemi oko ograničenih resursa tradicionalnih E.164 brojeva će se umanjiti. Kada su u pitanju E.212 brojevi, potreba će i dalje postojati i to prvenstveno za servise gde je neophodna mobilnost uređaja.



## 6. M2M/IOT USLUGE I REGULATORNI OKVIR EU

Regulatorni okvir elektronskih komunikacija u EU predstavlja seriju pravila koja se primenjuju u državama članicama EU. Ona podstiču konkurentnost, poboljšavaju funkcionisanje tržišta i garantuju osnovna prava korisnika. Novi predloženi dokument Evropske komisije: *European Electronic Communications Code* [9] koji će inovirati i pojednostaviti pravila je predložen i trenutno je u proceduri.

Glavna pitanja u pogledu regulative koja se nameću u procesu šire implementacije M2M/IoT usluga uključuju:

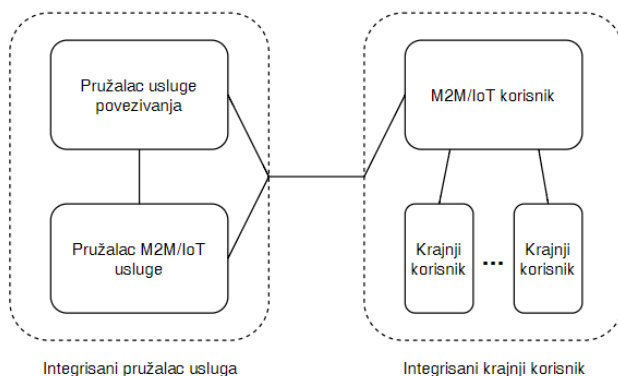
- Da li se M2M/IoT usluge trebaju/mogu kvalifikovati kao elektronski komunikacioni servisi iz čega bi proizašla prava i obaveze M2M operatora ?
- Pitanje *roaming-a* odnosno pravila i obaveze koje proističu iz toga.
- Pitanje prava i mogućnosti da se promeni operator mreže u M2M lancu.

Nacionalni telekomunikacioni regulatori treba da doprinesu identifikovanju prepreka i potencijalnih barijera kao i otklanjanju pravne nesigurnosti u procesu masovnog uvođenja M2M/IoT usluge uzimajući u obzir načela regulatornog okvira EU, domaćeg zakonodavstva i bezbednosnih normi.

## 7. M2M/IOT USLUGE KAO ELEKTRONSKE KOMUNIKACIONE USLUGE

Primena Regulatornog okvira elektronskih komunikacija na M2M/IoT usluge i operatore koji ih pružaju direktno zavisi od kategorizacije tih usluga kao elektronskih komunikacionih usluga (EKU). Ako se tako kategorišu, za njih se primenjuju sva prava i obaveze kao i za ostale operatore EKU.

U skladu sa definicijom, EKU je svaka usluga koja ispunjava sledeće kriterijume: 1) da se usluga u standardnim okolnostima pruža uz naknadu; 2) da se usluga pretežno ili u potpunosti sastoji od prenosa signala preko elektronske komunikacione mreže; 3) da se usluga sastoji od prenosa sadržaja a ne proizvodnje sadržaja.



Slika 2: Različite kombinacije M2M/IoT lanca

Glavni učesnici u M2M/IoT lancu su: pružalac usluge povezivanja (operator mreže), pružalac M2M/IoT usluga, M2M/IoT korisnik i krajnji korisnici. Tipičan M2M/IoT lanac može postojati u više različitih kombinacija: sa nezavisnim ili integrisanim pružaocima povezivanja i M2M/IoT usluga sa jedne strane i odvojenim ili integrisanim M2M/IoT korisnicima i krajnjim korisnicima.

### Stanje u Republici Srbiji:

Pravilnikom o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja [10] definisana je usluga prenosa podataka (koja uključuje i M2M usluge) i trenutno je registrovano 18 operatora koji pružaju ovu vrstu usluge.

## 8. ROAMING

U zavisnosti od poslovnog modela primenjene M2M/IoT usluge, *roaming* može biti stalan ili privremen. Trenutno se pitanje *roaming-a* razmatra za javne mobilne mreže u tehnologijama xG (x=2,3,4...) mada se u budućnosti mogu očekivati i druge bežične tehnologije koje imaju potrebu za *roaming-om*. Iz dokumenta *Roaming III Regulation* [11] koji je usvojen u Evropskom parlamentu, može se zaključiti da ovaj regulatorni okvir generalno obuhvata i mobilnu povezanost u M2M/IoT uslugama. Iz ovoga proističu i prava i obaveze pružaoca M2M/IoT usluga kao i mobilnih operatora. Kada je u pitanju stalan *roaming* postoje različite situacije primene u zavisnosti od prirode servisa:

- Kada se M2M uređaj prodaje van države gde je proizveden ali pritom koristi SIM karticu sa IMSI brojem iz države porekla (vozila, *e-readers*).
- U cilju postizanja bolje pokrivenosti (pametni merači potrošnje u pograničnim delovima država).

U slučaju stalnog *roaming-a*, pravila *Roaming III Regulation* ne daju jednoznačan odgovor. U zavisnosti od konkretnog slučaja, pojedine M2M/IoT usluge nedvosmisleno spadaju u domen te regulative, neke ne a za neke je potrebna analiza od slučaja do slučaja (*case-by-case*). Generalno, mogu se uočiti tri scenarija:

### Scenario 1:

Povezani uređaj putuje privremeno (primer: vozilo na godišnjem odmoru)

➡ **primenjuju** se pravila *Roaming III Regulation*

### Scenario 2:

Povezani uređaj je većinu vremena u stalnom *roaming-u*, a samo povremeno prelazi granice i vraća se (primer: vozilo prodato u inostranstvu)

➡ koristi se primena pravila *Roaming III Regulation* **u zavisnosti od slučaja** do slučaja (*case-by-case*)

### Scenario 3:

Povezani uređaj je u stalnom *roaming-u* i ne kreće se uopšte dugi niz godina (primer: pametni merači potrošnje ili senzori koji se koriste van države u kojoj su proizvedeni)

➡ **ne primenjuju** se pravila *Roaming III Regulation*

Pored ovoga, moguće je i alternativni način postizanja transnacionalnog *roaming*-a, a to je već pomenuta mogućnost korišćenja MNC koda u okviru deljenog MCC 901 koda koji dodeljuje ITU na zahtev registrovanih operatora.

## 9. PROMENA OPERATORA (PORTABILNOST)

Prenosivost broja (odnosno promena operatora) sama po sebi nije pitanje od značaja za M2M/IoT korisnika i/ili krajnjeg korisnika. Razlog je što, u slučaju kada nema ljudskog učestvovanja u komunikaciji, već to obavljaju mašine između sebe potpuno autonomno, brojevi sami po sebi nisu od većeg značaja za krajnjeg korisnika pa ih on uglavnom i ne zna (niti ima potrebu da ih zna). Ono što je važno u pogledu razvoja tržišta i konkurencije je mogućnost M2M/IoT korisnika da promeni operatora mreže (pružaoca usluge povezivanja) u M2M/IoT lancu (Slika 2).

Trenutno je situacija takva, da u slučaju kada M2M/IoT korisnik želi da promeni operatora mreže (npr. da pređe od jednog mobilnog operatora kod drugog), potrebna je fizička zamena SIM kartica (ili čak celih modula) na svim, već postavljenim M2M uređajima. Ovi troškovi zamene mogu biti značajni a često i tehnički komplikovani (nije uvek laka dostupnost M2M uređaja i sl.). Ovo dovodi do praktične nemogućnosti promene operatora mreže i „zaključavanja“ kod postojećeg operatora (tzv. *lock-in issue*).

Postoje dva rešenja za prevazilaženje ovog problema. Prvi podrazumeva fizičku zamenu SIM kartica u uređajima a drugi novi pristup tj udaljeni *provisioning*.

### a) Dodela MNC koda M2M/IoT korisnicima

Kada bi se uslovi dodele MNC koda relaksirali u pogledu da bude dozvoljena dodela ovog koda M2M/IoT korisnicima, problem promene operatora mreže bi bio rešen. Pod pretpostavkom da se ova izmena regulative i dogodi (što nije izvesno kada će se dogoditi, ako se uopšte i dogodi) ostaju određena pitanja na koja treba odgovoriti:

- koju infrastrukturu treba da poseduje M2M/IoT korisnik;
- kategorisanje M2M/IoT korisnika kao operatora ECU i obaveze koje iz toga proističu;
- efikasna procedura promene operatora (ugovori, rutiranje);
- operativni troškovi promene operatora;
- problem ograničenih resursa MNC (100 po državi).

U slučaju da se ide na ovo rešenje treba odmeriti troškove u odnosu na klasičnu (fizičku) zamenu SIM kartica i na *OTA provisioning* kao i to da li dodelu MNC kod treba omogućiti svim M2M/IoT korisnicima ili ograničiti samo na one najveće.

### b) *OTA (Over-the-air) provisioning* SIM kartica

GSMA asocijacija (*Groupe Speciale Mobile Association*) je specificirala mehanizam upravljanja i *provisioning*-a ugrađenih SIM kartica (obično na udaljenoj lokaciji) tzv *embedded SIM*. Ova tehnologija omogućava promenu operatora na daljinu, bez fizičke zamene SIM kartica. Iako je ova tehnologija u tehničkom pogledu potpuno spremna, u ovom trenutku se primenjuje u maloj meri ali se očekuje njeno širenje. Ovaj proces treba pratiti i ohrabrivati jer treba imati u vidu da postojeći operatori mreže neće rado prelaziti na *OTA* mehanizam jer tako gube svoje sadašnje pozicije. Preporuka za nacionalne telekomunikacione regulatore je da se prate tendencije, i da ukoliko u narednom periodu ne bude šire upotrebe ove tehnologije, razmotri i nametanje obaveze operatorima prelazak na nju ili bar regulatorni mehanizam koji će je favorizovati.

## 10. ZAKLJUČAK

U godinama pred nama, širenje M2M/IoT servisa je neminovnost. Procena BEREC-a (*Body of European Regulators for Electronic Communications*) je da će broj IoT konekcija u EU dostići  $6 \cdot 10^9$  u 2020. sa godišnjim rastom od 20%. Rešavanje regulatornih pitanja u tom procesu omogućavaju tehničke preduslove za formiranje M2M/IoT lanca kao i održivo tržište i konkurenciju.

## LITERATURA

- [1] RSPG Report on Strategic Sectoral Spectrum Needs, RSPG13-540 (rev2), European Commission 2013.
- [2] Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices, European Commission, 2013.
- [3] Relating to the use of Short Range Devices (SRD), ERC Recommendation 70-03, CEPT, 2017.
- [4] Plan namene radio-frekvencijskih opsega, Službeni glasnik RS broj 99/12.
- [5] Pravilnik o načinu korišćenja radio-frekvencija po režimu opšteg ovlašćenja, Službeni glasnik RS broj 28/13.
- [6] Extra-territorial Use of E 164 Numbers - High level principles of assignment and use, CEPT, 2016.
- [7] Plan numeracije, Službeni glasnik RS“, br. 32/11, 35/12, 64/13, 60/16.
- [8] Report Enabling the Internet of Things, BoR (16) 39. BEREC, 2016.
- [9] European Electronic Communications Code, COM/2016/0590, European Commission, 2016.
- [10] Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja, Službeni glasnik RS, br. 38/11, 13/14.
- [11] Roaming III Regulation No 531/2013, European Parliament, 2013.

# Centralizovana detekcija neispravnih veza u mešovitoj telefonskoj mreži

## Centralized detection of faulty links in mixed telephone network

Vladimir Matić, Aleksandar Lebl, Dragan Mitić, Žarko Markov  
IRITEL AD Beograd, Batajnički put 23, 11080 Beograd, Srbija

**Sadržaj** - U radu je opisan način korišćenja vremena odziva pozvane strane, osnovnog pokazatelja brzine uspostavljanja telefonske veze, za nadgledanje ispravnosti pojedinih delova i detekciju neispravnih veza u mešovitoj telefonskoj mreži. Koristeći ovu osobinu, predložen je detektor neispravnih veza u mreži Elektroprivrede Srbije.

**Abstract** - In this paper, the possibility of using Post Selection Delay, main indicator of the network service quality, for monitoring the network operation and detection of faulty links in mixed telephone network is described. Applying this feature, the faulty link detector in electric power utility network is proposed.

### 1. UVOD

Osnovni zahtev za izgradnju posebne telefonske mreže elektroprivrede Srbije (EPS) je bio visoka raspoloživost. U tom cilju koriste se sva moguća sredstva, kao što su: ostvarivanje veza svim prenosnim putevima, bez obzira na tehnološku realizaciju, i nehijerarhijska organizacija mreže (obilazno upućivanje). Korišćenje različitih tehnologija (optički kablovi, bakar, radio) povećavaju raspoloživost, uz problem usaglašavanja različitih signalizacija i oblika govornog signala [1]. Međutim, takva mešovita mreža može da iskoristi različite vrste signalizacija za nadgledanje ispravnosti pojedinih delova mešovite mreže i detekciju neispravnih veza u njoj.

Kao primer primene pomenute osobine, opisan je detektor predalarmnog stanja tj. neispravnih digitalnih prenosnih puteva u mešovitoj telefonskoj mreži EPS-a. Princip rada detektora je otkrivanje razlike u vrednostima vremena odziva pozvane strane u slučajevima korišćenja različitih prenosnih puteva, na osnovu koje se može zaključiti da je određena veza neispravna.

Vreme odziva pozvane strane (*Post Dialing Delay* - PDD) je osnovni činilac brzine uspostavljanja veze. Definiše se kao vremenski interval od izbora poslednjeg adresnog parametra (cifre) traženog korisnika od strane pozivajućeg korisnika, do početka odgovora traženog korisnika [2].

### 2. TELEFONSKA MREŽA EPS-a

Za efikasan rad elektroprivrede je od posebnog značaja pružanje usluge telefonije, jer ona omogućava obavljanje operativnih i administrativnih zadataka zaposlenog osoblja koji rade u geografski razduženim objektima [3].

Da bi se obezbedila telefonska usluga u elektroprivredi, moguće je koristiti javnu telefonsku mrežu ili telefonsku mrežu posebne namene (tzv. korporacijska ili privatna mreža). Javna mreža nije dobro rešenje za elektroprivredu jer se tako ne garantuje ostvarivanje telefonskih poziva onda kada je to potrebno. U javnoj mreži je dozvoljen procenat poziva koji se ne mogu ostvariti unapred definisan, pri čemu su u uslovima povećanog opterećenja dozvoljeni veći gubitak poziva i veće kašnjenje. U vreme povećane aktivnosti na održavanju elektroenergetskog sistema očekuje se i povećanje opterećenja u telefonskoj mreži. U ovim kritičnim radnim periodima, vreme za donošenje i sprovođenje odluka je ograničeno i kratko, pa je stoga nedopustivo narušavanje kvaliteta telefonske usluge. Usled toga je najvažnija funkcija koju treba da pruži telefonska usluga u elektroprivredi svakako bezuslovno ostvarivanje telefonskih poziva.

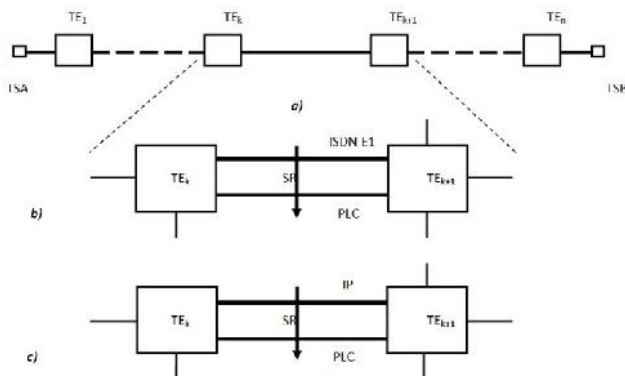
Problem telefonske komunikacije u okviru EPS-a rešen je uvođenjem privatne klasične telefonske mreže, nastale u prethodnoj jedinstvenoj organizaciji preduzeća. Njeno osnovno tehničko svojstvo je visoka raspoloživost mreže u pogledu ostvarivanja telefonskih razgovora. Nakon donošenja odluke o modernizaciji telefonske mreže, izabrana je strategija prelaza ka paketskoj telefoniji. Ona se sastojala u zameni postojećih, najstarijih, centrala, izgradnji nove paketske mreže sposobne da podrži višestruke komunikacione servise, aplikacije i integraciju preostalih postojećih centrala u novu IP infrastrukturu, a sve to bez značajnih prekida telefonskog servisa.

Telefonska mreža EPS-a je mešovita mreža, čime se označava jedinstvo klasične i paketske mreže. Prednost ovakve mreže je mogućnost korišćenja postojećih resursa prilikom izgradnje nove mreže. U datoj telefonskoj mreži izvršeno je objedinjavanje klasične i paketske telefonske mreže, u cilju uvođenja novih usluga. Ovo je izvedeno dodavanjem nove opreme u postojeću mrežu [4].

Jedna od značajnih razlika u odnosu na javnu telefonsku mrežu je mogućnost prenosa telefonskog signala po vodovima visokog napona. To su tzv. VF veze ili veze po dalekovodu (*Power Line Carrier* - PLC), na kojima je počivala stara mreža EPS-a. PLC je tehnika obrazovanja telefonskog kanala korišćenjem energetskih kablova za prenos. Ona se u novoj mešovitoj mreži EPS-a zadržava zbog povećanja raspoloživosti. Njena osnovna svojstva su primena spore signalizacije E&M sa dekadnim prenosom cifara i nešto lošiji kvalitet prenosa govornog signala.

### 3. NAČIN DETEKCIJE NEISPRAVNIH VEZA

Primer veze kroz mešovitu telefonsku mrežu EPS-a je prikazan na slici 1. Data mreža se sastoji od telefonskih centrala (TE) i prenosnih sistema koji mogu biti klasični (ISDN), paketski (IP) ili veze po dalekovodu (PLC). Veza se uspostavlja između dva korisnika odnosno telefonskih aparata TSA i TSB, slika 1 (a). Ponuđeni saobraćaj grupi prenosnih puteva je označen sa A. Broj kanala ISDN veza ili najveći broj mogućih veza po IP prenosnom putu je  $N$ . Veza prolazi kroz  $n$  čvorova. Posmatraju se dva susedna čvora kroz koje prolazi veza, slike 1 (b) i (c).



Slika 1. Model uspostavljanja veze u mreži EPS-a

Telefonske centrale  $TE_k$  i  $TE_{k+1}$  su povezane ISDN ili IP vezom, a iz prethodne (klasične) mreže one su i dalje povezane PLC-om. Ostvarivanje veza između centrala  $TE_k$  i  $TE_{k+1}$  se vrši prema unapred definisanom pravilu izbora (*Selection Rule - SR*), po kome se uvek prvo bira digitalni kanal (ISDN ili IP), a ukoliko oni nisu dostupni bira se PLC. Ovakav način izbora je posledica bržeg uspostavljanja veze i boljeg kvaliteta govornog signala preko digitalnih veza nego preko PLC-a. Normalno stanje (rad) je ono u kome su ispravne sve veze između centrala. Stanje alarma se definiše u slučaju kada se ne može ostvariti veza između susednih centrala  $TE_k$  i  $TE_{k+1}$  usled neispravnosti svih prenosnih puteva između njih. Stanje predalarma se definiše u slučaju kada se veza ne može ostvariti putem prvog izbora tj. ISDN ili IP kanalom zbog neispravnosti, već se može ostvariti samo PLC-om. Pretpostavlja se da se u mreži primenjuje petocifrena numeracija i da je prenos svih brojeva jednako verovatan (uniformna raspodela).

Parametar PDD je definisan kao vremenski interval od poslednje izabrane cifre do početka odgovora pozvane strane tj. signala kontrole poziva. Osnovne komponente PDD-a su vremena prenosa informacije o izabranom broju između čvorova mreže. Zbog toga treba upoznati svojstva ovih vremena u oba slučaja.

U klasičnom delu telefonske mreže koristi se ISDN tehnika i signalizacija SS7. Najduža dozvoljena vremena rada centrala data su u ITU-T preporuci Q.543 [5]. Od svih propisanih normi i pomenutoj preporuci, najveće su one koje se odnose na ISDN tehniku, poruku koja nosi adresnu informaciju i signalizaciju tipa „svi zajedno”.

Najduže dozvoljeno srednje vreme za aktivnosti jedne deonice i jednog čvora mreže je 600 ms (*load A*) odnosno 800 ms (*load B*). Najduže vreme za koje će se data aktivnost obaviti u slučaju 95 % veza je 800 ms (*load A*) odnosno 1200 ms (*load B*). Raspodela verovatnoća trajanja vremena prosleđivanja adresne informacije je eksponencijalna, a osnovna komponenta ovog vremena je vreme čekanja na uslugu signalnog procesora. Vreme usluge procesora može biti jednakog ili eksponencijalnog trajanja [6]. Ovde se pretpostavlja da signalni procesor uslužuje zahteve tako da je vreme usluge raspodeljeno po eksponencijalnoj raspodeli. Pretpostavka je uvedena iz dva razloga: poslovi signalnog procesora za različite poruke su različitog trajanja, a na ovaj način se dobijaju pouzdaniji (konzervativniji - *on the safe side*) rezultati.

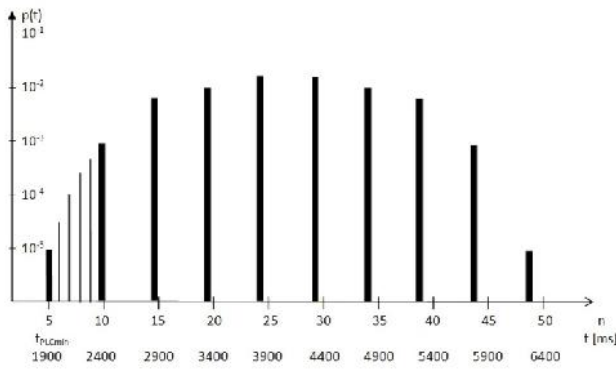
Delovi telefonske mreže koji su realizovani paketskom tehnikom za ostvarivanje veza koriste protokol SIP. Adresna informacija za ostvarenje veze se nalazi u poruci *INVITE* ili *INVITE REQUEST*, nakon čega se očekuje potvrda nekim od odgovora iz grupe 1xx. Poruka *INVITE* se može slati i nepouzdanim protokolom UDP, pa se tada mora vršiti preventivna retransmisija. Prva retransmisija se vrši posle 500 ms [7]. Realna je pretpostavka da će u privatnoj mreži, kakva EPS-ova, vreme od 500 ms biti dovoljno da se dobije odgovor na 95 % zahteva *INVITE*. Moguće je pretpostaviti još da za vreme prenosa adresne poruke između dva mrežna čvora paketskom tehnikom važi isto što je rečeno za vreme prenosa ISDN vezom.

Na osnovu propisanih normi i uvedenih pretpostavki može se zaključiti da je najduže dozvoljeno vreme prenosa adresne informacije između dva čvora digitalne veze (ISDN ili IP) ono koje važi za 95 % veza pri povećanom saobraćajnom opterećenju i iznosi 1200 ms.

U PLC tehnici cifre se prosleđuju u dekadnom obliku i bez potvrde. Zbog toga se smatra da je po završetku slanja izabranog broja završen i prenos adresne informacije između centrala. Vreme prenosa adresne poruke između centrala u ISDN i IP tehnici zavisi od opterećenosti procesora i kanala tj. signalnih resursa, a neznatno zavisi od trajanja signalizacione poruke. Nasuprot tome, u PLC tehnici vreme prenosa adresne poruke između centrala zavisi od trajanja adresne informacije tj. od broja dekadnih impulsa. Ovo vreme je slučajna veličina koja uzima diskretne vrednosti, što se može videti iz sledećeg primera. Ukoliko u mreži ima više od 10000 korisnika pa se primenjuje petocifrena numeracija, tada se vreme prenosa adresne informacije  $t_{PLC}$  može izračunati kao:

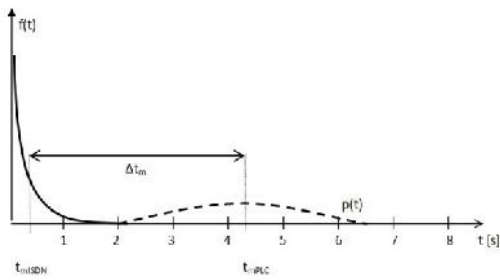
$$t_{PLC} [\text{ms}] = 4 \cdot t_p + 100 \cdot i, \quad i = 5, 6, \dots, 50 \quad (1),$$

gde je  $t_p$  vreme pauze između cifara koje iznosi 350 ms, a  $i$  broj dekadnih impulsa, čije trajanje iznosi 100 ms. Raspodela verovatnoća trajanja vremena prenosa adresne poruke data je na slici 2. Sa slike se jasno vidi da je reč o diskretnoj slučajnoj veličini i da je vrednost verovatnoće različita od nule samo za vrednosti  $t = 1400 + 100 \cdot n$  [ms], gde je  $n$  ceo broj odnosno samo za vrednosti  $t = 1900, 2000, 2100, \dots, 6300$  i  $6400$  ms (na slici je prikazana svaka peta vrednost).



Slika 2. Raspodela verovatnoća trajanja vremena prenosa adresne poruke po PLC vezi

Gustina raspodele dužine trajanja vremena potrebnog za prenos adresne poruke po ISDN kanalu  $f(t)$  je prikazana na slici 3. Jasno je da se radi o kontinualnoj slučajnoj veličini, čija je srednja vrednost označena sa  $t_{mISDN}$ . Na istoj slici je isprekidanom linijom prikazana i raspodela verovatnoća vremena prenosa adresne informacije po PLC vezi i za petocifrenu numeraciju  $p(t)$ . Ova slučajna veličina je diskretna, sa srednjom vrednošću  $t_{mPLC}$ .



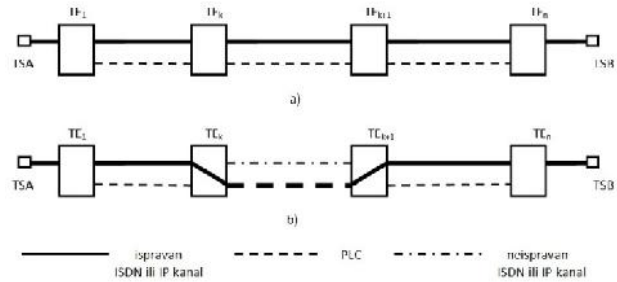
Slika 3. Gustina raspodele dužine trajanja vremena prenosa adresne poruke

Na osnovu grafika na slici 3., može se zaključiti da se vreme prenosa adresne informacije između dva susedna čvora u mešovitoj mreži EPS-a u slučaju ISDN ili IP kanala ( $t_{ISDN}$ ) i PLC veze ( $t_{PLC}$ ) značajno razlikuje. Kod ISDN-a ili IP prenosa signalizacija o uspostavljanju veze obavlja se razmenom poruka koja traje nekoliko desetina ili stotina milisekundi. Sa druge strane, u PLC-u se koristi spora signalizacija E&M sa dekadnim prenosom cifara, tako da prenošenje signala potrebnih za uspostavu veze traje nekoliko sekundi. Kao što se na slici vidi, srednja vrednost razlike u vremenu prenosa adresne poruke između dva susedna čvora za petocifrenu numeraciju iznosi oko 4 s. Ova razlika u vremenu prenosa adresne informacije između dva susedna čvora za različite prenosne puteve se može iskoristiti za proveru njihove ispravnosti tj. za detekciju neispravnosti nekog od njih.

#### 4. PRINCIP RADA DETEKTORA

Centralni detektor predalarmnog stanja vrši proveru ispravnosti prenosnih puteva između dva susedna čvora u mreži. Osnovni princip rada detektora se zasniva na tome da on generiše ispitne telefonske pozive u celoj mreži i upoređuje izmereno vreme odziva PDD sa uobičajenim

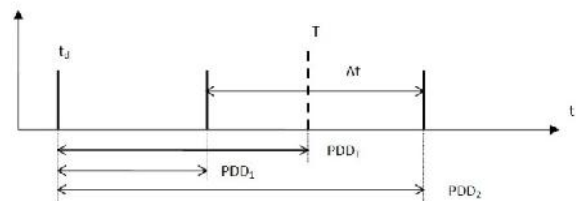
vrednostima. U slučaju velikih odstupanja, detektor proglašava stanje predalarma. Predloženi princip rada detektora je predstavljen na slikama 4. i 5.



Slika 4. Način uspostavljanja veze kroz mrežu

Na slici 4. (a) je prikazan način uspostavljanja veze kroz mrežu u normalnom stanju tj. u slučaju kada su svi ISDN i IP kanali ispravni. Sa druge strane, na slici 4. (b) prikazano je uspostavljanje veze između telefona TSA i TSB, ako je na jednoj deonici neispravan ISDN ili IP kanal i usled toga je zamenjen PLC-om. Uspostavljena veza je na slici prikazana podebljanom linijom.

Slika 5. prikazuje vremenske vrednosti veličine PDD. Trenutak slanja ispitnog poziva je označen sa  $t_d$ . Vreme od slanja do odgovora pozvane strane u slučaju ispravnosti svih ISDN i IP kanala na putu do pozvanog telefonskog aparata je označeno sa  $PDD_1$  a vreme odgovora pozvane strane u slučaju neispravnosti nekog ISDN ili IP kanala je označeno sa  $PDD_2$ . Razlika u dužini vremena prenosa adresne informacije ( $\Delta t$ ) na deonici koja se nalazi u predalarmnom stanju, obuhvaćena je ukupnim vremenom PDD-a. Vreme  $PDD_T$  je unapred definisana vrednost praga. Ukoliko je izmerena vrednost  $PDD > PDD_T$ , proglašava se stanje predalarma.



Slika 5. Vrednosti PDD-a za različite prenosne puteve

#### 5. LAŽNI PREDALARM I PROMAŠAJ

Obzirom da je rad detektora zasnovan na posmatranju slučajnih veličina, moguće su i neplanirane posledice: lažni predalarm i promašaj detektora. Lažni predalarm je pojava kada detektor pokazuje postojanje predalarma iako su sve veze ispravne. Promašaj detektora predstavlja obrnutu pojavu, postoji kvar na ISDN ili IP vezi, ali detektor to ne pokazuje. Lažni predalarm se može desiti u slučajevima povećanog saobraćajnog opterećenja kada su svi prenosni putevi ispravni, a veza se ostvaruje PLC-om. Promašaj u otkrivanju predalarmnog stanja se može desiti u slučaju izabrane isuviše velike vrednosti praga  $PDD_T$ .

U cilju određivanja verovatnoća dešavanja lažnog predalarma i promašaja, posmatraju se dve mrežne tačke u telefonskoj mreži EPS-a, koje pripadaju jednoj vezi, kao na slici 4. Razmatra se realan slučaj kada se kvar dešava samo na jednoj deonici. Centralni detektor predalarmnog stanja je uključen i u njemu je postavljena granična vrednost vremena odziva pozvane strane, prag  $PDD_T$ . Predalarmno stanje se proglašava ako je  $PDD > PDD_T$ .

Lažni predalarm može nastati u dva slučaja:

1. Ako telefonski saobraćaj ima veliku vrednost, pa iako su ISDN ili IP kanal ispravni, oni su zauzeti prethodnim pozivima, pa se sledeća veza se upućuje po PLC-u.
2. Ako signalizacioni saobraćaj između mrežnih tačaka koje čine vezu ima veliku vrednost, pa je vreme slanja adresne adresne informacije suviše veliko, što utiče da ukupno vreme odziva pozvane strane bude  $PDD > PDD_T$ .

Verovatnoća dešavanja lažnog predalarma, koji nastaje usled velikog telefonskog saobraćaja tj. verovatnoća lažnog predalarma prve vrste  $P_{fa1}$  očigledno je jednaka verovatnoći gubitaka u Erlangovom snopu sa gubicima od  $n$  kanala i ponuđenim saobraćajem  $A$ . Ona se može odrediti korišćenjem formule:

$$P_{fa1} = E_{1,N}(A) = \left( \frac{A^N}{N!} \right) / \left( \sum_{i=0}^N \frac{A^i}{i!} \right) \quad (2),$$

gde je  $E_{1,n}(A)$  poznata Erlangova formula prve vrste [8].

Verovatnoća lažnog predalarma, koji nastaje usled velike vrednosti signalizacionog saobraćaja tj. verovatnoća lažnog predalarma druge vrste, može se izračunati ako se posmatra raspodela vremena prosljeđivanja adresne informacije između čvorova mreže u ISDN ili IP kanalu. Kao što je rečeno, funkcija gustine raspodele je negativno-eksponencijalna (slika 3.) i predstavlja se izrazom:

$$f(x) = \lambda \cdot e^{-\lambda x}, \quad x \geq 0 \quad (3).$$

Kumulativna funkcija raspodele odnosno verovatnoća da je  $t \leq x$ ,  $F(x) = P(t \leq x)$ , je:

$$F(x) = 1 - e^{-\lambda x} \quad (4).$$

Očigledno je da se verovatnoća lažnog predalarma druge vrste  $P_{fa2}$ , dobija kao:

$$P_{fa2} = P(t > PDD_T) = 1 - F(PDD_T) \quad (5).$$

Ukupna verovatnoća lažnog predalarma se dobija kao:

$$P_{fa} = 1 - (1 - P_{fa1}) \cdot (1 - P_{fa2}) \approx P_{fa1} + P_{fa2} \quad (6),$$

obzirom da je  $P_{fa1} \ll 1$  i  $P_{fa2} \ll 1$ .

Način određivanja verovatnoće  $P_{fa}$  se može videti iz primera u kome se posmatra primarna grupa ISDN kanala ( $n = 30$ ), kojoj je ponuđen saobraćaj od 20 Erlanga. Vrednost praga detektora  $PDD_T$  je postavljena na 1.5 s. Na osnovu izraza (2), dobija se  $P_{fa1} = 0.00846$ . Uzimajući najduže dozvoljeno vreme rada centrale (vreme čekanja za 95 % poziva mora biti manje od 1200 ms na osnovu ITU-T preporuka), određuje se intezitet poziva  $\lambda$ :

$$F(x) = 1 - e^{-1200\lambda} = 0.95 \rightarrow \lambda = 2.5 \text{ s}^{-1} \quad (7).$$

Koristeći izraze (4) i (5), za izabranu vrednost praga dobija se  $P_{fa2} = 0.0235$ . Ukupna verovatnoća lažnog predalarma je tako na osnovu izraza (6)  $P_{fa} = 0.03194$ .

Promašaj u otkrivanju predalarmnog stanja nastaje ukoliko je izabrana isuviše velika vrednost praga  $PDD_T$ . To znači da verovatnoća promašaja postoji samo ako je vrednost vremena praga veća od donje granice vremena prosljeđivanja adresne informacije po PLC vezi ( $PDD_T > t_{PLCmin}$ ), kao što je prikazano na slici 2. Tada će, za vrednosti vremena  $PDD_{t_{PLCmin}} < PDD < PDD_T$ , stanje predalarma ostati neotkriveno. Verovatnoća dešavanja promašaja  $P_{miss}$  je očigledno jednaka verovatnoći da je vreme prosljeđivanja adresne informacije po PLC-u manje od praga  $PDD_T$ :

$$P_{miss} = \sum_i P(t_{PLCi} < PSD_T) \quad (8).$$

Način određivanja verovatnoće promašaja se može videti iz sledećeg primera. Ukoliko je u mreži primenjena petocifrena numeracija i za vrednost praga izabrano  $PDD_T = 2.25$  s, tada je na osnovu slike 2. i izraza (8):  $P_{miss} = p(1.9 \text{ s}) + p(2 \text{ s}) + p(2.1 \text{ s}) + p(2.2 \text{ s}) = 0.00056$ .

Verovatnoća lažnog predalarma prve vrste je jednaka verovatnoći gubitaka u Erlangovom snopu kanala i ona očigledno zavisi od vrednosti ponuđenog saobraćaja. Ako se ponuđeni saobraćaj u prethodnom primeru poveća sa 20 Erlanga na 26 Erlanga, tada će se  $P_{fa1}$  povećati sa 0.00846 na 0.06661, što iznosi oko 8 puta. Smanjenje ove verovatnoće može da se izvede dvostrukim testiranjem, pa ako oba pokušaja pokažu predalarmno stanje verovatnoća lažnog predalarma prve vrste će pasti na  $P_{fa1} = 0.0044$ .

Verovatnoća lažnog predalarma druge vrste je u obrnutoj je zavisnosti od vrednosti postavljenog praga  $PDD_T$ . Ukoliko se u već pomenutom primeru vrednost  $PDD_T$  poveća sa 1.5 s na 2 s, tada će se  $P_{fa2}$  sa vrednosti 0.0235 smanjiti na 0.0067. Verovatnoća lažnog predalarma druge vrste se na ovaj način može smanjivati po želji. Međutim, kao što je već napomenuto, povećanje praga  $PDD_T$  posle neke vrednosti dovodi do mogućnosti promašaja detektora u otkrivanju predalarma.

Promašaj detektora se može izbeći izborom odgovarajuće vrednosti praga  $PDD_T$  ( $PDD_T < t_{PLCmin}$ ), ali ukoliko se želi u potpunosti smanjiti verovatnoća  $P_{fa2}$ , tada povećanje vrednosti praga detektora ( $PDD_T > t_{PLCmin}$ ) neminovno dovodi do situacije da je verovatnoća  $P_{miss} > 0$ .

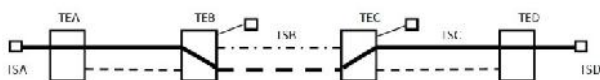
## 6. RAD DETEKTORA U MREŽI EPS-a

Centralni detektor predalarmnih stanja tj. neispravnih ISDN i IP kanala radi na osnovu činjenice da postoji razlika u vremenu odziva pozvane strane za slučajevne neispravnih i ispravnih digitalnih veza. Detektor se nalazi u centru mreže i sadrži plan numeracije cele telefonske mreže. U stanju kada su sve veze ispravne, detektor obavlja probne pozive usmerene ka ispitnim priključcima u čvorovima mreže. Nakon slanja inicijalne signalizacione poruke za ostvarenje veze, uključuje se merač vremena. Po prijemu odgovora i očitavanja vremena, utvrđuje se standardna



vrednost PDD-a. Ovaj podatak se memoriše u detektoru, kako bi se kasnije mogao uporediti sa izmerenim vrednostima PDD-a. Pored toga, na osnovu izabranog broja (adrese) čvora i utvrđene standardne vrednosti PDD-a, za dati čvor se određuje prag  $PDD_T$ . Opisani postupak se sukcesivno ponavlja za svaki čvor u mreži.

Testiranje se vrši tako što se prvo pozivaju priključci najudaljenijih čvorova, a zatim sve bliži. Ukoliko je izmerena vrednost PDD-a manja od praga,  $PDD < PDD_T$ , prelazi se na ispitivanje sledećeg čvora. Ako se za neki udaljeni čvor ustanovi da je izmerena vrednost PDD-a veća od praga,  $PDD > PDD_T$ , potrebno je odrediti na kojoj deonici je nastalo predalarmno stanje. Ova situacija je prikazana na slici 6. Pretpostavlja se da se sa korisničkog aparata TSA vezanog na centralu TEA bira aparat TSD u centrali TED. Izmereno vreme odziva PDD odstupa od standardne vrednosti više nego što prag dozvoljava. To znači da je na jednoj od datih deonica TEA - TEB, TEB - TEC ili TEC - TED nastalo stanje predalarma. U centralnom detektoru postoje podaci za standardne vrednosti PDD-a za veze TSA - TSD, TSA - TSC i TSA - TSB. Sukcesivnim pozivanjem korisničkih aparata TSC i TSB sa aparata TSA se može lako utvrditi na kojoj deonici je nastalo predalarmno stanje (u primeru na slici 6. deonica TEB - TEC).



Slika 6. Detekcija deonice na kojoj je nastalo predalarmno stanje

Vreme detekcije stanja predalarma se može smanjivati po želji smanjivanjem vremena između ispitnih poziva. Srednje vreme od kvara do njegove detekcije je jednako polovini vremenskog intervala između dve uzastopne provere ispravnosti. Ovo vreme bi se moglo znatno skratiti ukoliko bi detektor bio dodeljen nekom vrlo aktivnom aparatu, kao što je dispečerski telefonski aparat.

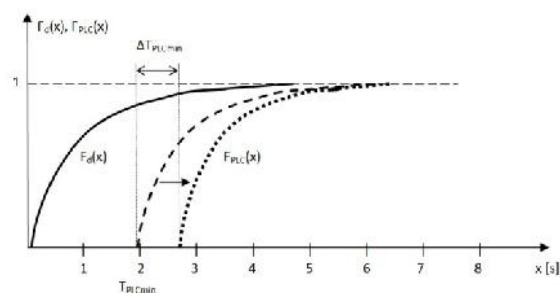
## 7. NUMERACIJA I EFIKASNOST DETEKTORA

Visoka raspoloživost mešovite telefonske mreže EPS-a se ostvaruje korišćenjem svih raspoloživih prenosnih puteva. Mogućnost obilaznog upućivanja telefonskih poziva je značajna osobina mreže. Međutim, kao posledica toga se javljaju neželjeni efekti. Osim mogućeg generisanja petlji u mreži, u mrežama sa obilaznim upućivanjem je znatno otežana detekcija neispravnih kanala između čvorova. Razlog tome je što ukoliko korisnici uspostave vezu preko obilaznog puta, neispravna veza može ostati neprimećena. Jedan od načina prevazilaženja ovog problema je primena centralnog detektora predalarmnih stanja.

Osnovni nedostatak opisanog centralnog detektora je pojava lažnog predalarma odnosno pojave da se signal odziva pojavi sa velikim kašnjenjem (PDD ima veliku vrednost), a svi kanali su ispravni. Verovatnoća lažnog predalarma ima dve komponente, pri čemu je dominantna

verovatnoća lažnog predalarma druge vrste. Usled toga je potrebno razmotriti mogućnost njenog smanjenja.

Kao što je već rečeno, vreme prenosa adresne informacije između dve mrežne tačke je slučajna veličina. Njena kumulativna funkcija raspodele je prikazana na slici 7. Punom linijom je označena kumulativna funkcija raspodele vremena  $T_d$ ,  $F_d(x) = P(T_d \leq x)$ , za slučaj digitalnih ISDN i IP kanala. Isprekidanom linijom je označena kumulativna raspodela vremena  $T_{PLC}$ ,  $F_{PLC}(x) = P(T_{PLC} \leq x)$ , za slučaj PLC veze i petocifrene numeracije. Funkcija  $F_{PLC}(x)$  je stepenasta, ali je na slici prikazana kao kontinualna pošto je broj stepenica dosta veliki (45).



Slika 7. Uticaj plana numeracije na kumulativnu funkciju raspodele vremena prenosa adresne informacije

Verodostojnost detektora predalarma je utoliko veća ukoliko je veća vrednost praga  $PDD_T$ . Naime, ako je  $PDD_{T1} > PDD_{T2}$  tada je:

$$F_d(PDD_{T1}) = P(T_d \leq PDD_{T1}) > F_d(PDD_{T2}) = P(T_d \leq PDD_{T2}) \quad (9)$$

U primeru iz prethodnog poglavlja za prag  $PDD_T = 1.5$  s je dobijena vrednost  $P_{fa2} = 0.0235$ . Ukoliko se detektor postavi na vrednost  $PDD_T = 2.5$  s, verovatnoća lažnog predalarma druge vrste iznosi  $P_{fa2} = 0.00193$ . U ovom slučaju, vrednost  $P_{fa2}$  smanjiće se za red veličine. Jasno je da vreme praga ne sme biti veće od  $T_{PLCmin}$ , tj. mora da važi relacija:  $PDD_T < T_{PLCmin}$ , slika 2. U suprotnom, za  $PDD_T > T_{PLCmin}$  neki slučajevi predalarma ne bi bili detektovani.

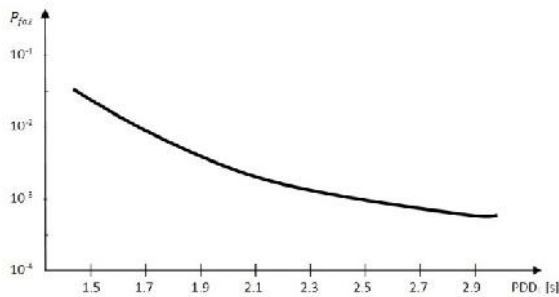
Verovatnoća lažnog predalarma druge vrste se može smanjiti izborom pogodne numeracije s obzirom da razlika vremena odziva pozvane strane po PLC-u i digitalnom kanalu direktno zavisi od broja biračkih impulsa u izabranom broju. Tako, biranje telefonskog broja sa velikim brojem biračkih impulsa omogućava da se prag  $PDD_T$  postavi na veću vrednost, a samim tim se smanjuje  $P_{fa2}$ . U slučaju da se bira broj 11111, a prag detektora je  $PDD_T = 1.9$  s, verovatnoća promašaja je u ovom slučaju  $P_{miss} = 0$ , a  $P_{fa2} = 0.00865$ . Ukoliko se bira broj 11199, prag detektora se može povećati na 3.5 s, pa je  $P_{fa2} = 0.000158$ , uz, i dalje, zadovoljen uslov  $P_{miss} = 0$ . Pretpostaviće se slučaj kada u mreži ima 20000 korisnika i da pozivni brojevi ovih korisnika nisu uniformno raspoređeni od 11111 do 00000, već između 81111 do 90000 tj prve cifre su uvek 8 ili 9. (Napomena: u dekadnom biranju telefonskih brojeva „0“ je najveća cifra

pošto sadrži 10 dekadnih impulsa). Jasno je da će zbir cifara koje se šalju PLC vezom sada biti od 12 do 50, a ne od 5 do 50 kao u slučaju uniformne raspodele pozivnih brojeva. Vrednost  $T_{PLCmin}$  se u ovom slučaju povećava sa 1900 ms na 2600 ms, a kumulativna funkcija raspodele vremena se menja i na slici 7. je označena tačkastom linijom. Vreme praga detekcije  $PDD_T$  se sada može postaviti na veću vrednost što, saglasno nejednačini (9), povećava verodostojnost detektora.

Na slici 8. je prikazana promena verovatnoće lažnog predalarma druge vrste sa promenom praga detektora  $PDD_T$  (za vrednost  $\lambda = 2.5 \text{ s}^{-1}$ ), uz uslov:

$$PDD_T = T_{PLCmin} - 400 \text{ ms} \quad (10).$$

Vrednost 400 ms je usvojena za sigurnosnu marginu između  $PDD_T$  i  $T_{PLCmin}$ .



Slika 8. Zavisnost verovatnoće lažnog predalarma od vrednosti praga  $PDD_T$

## 8. ZAKLJUČAK

Mešovite telefonske mreže koriste različite elemente i signalizacione postupke. Na osnovu posmatranja vremena odziva pozvane strane u toku uspostavljanja telefonske veze, uz željenu verodostojnost se mogu otkriti neki neispravni delovi mešovite mreže. Time se značajno može povećati raspoloživost mešovite mreže, što može biti veoma važno u slučaju posmatrane telefonske mreže elektroprivrede. Obilazno upućivanje poziva je vrlo važno sredstvo povećanja raspoloživosti, ali se na taj način otežava mogućnost otkrivanja kvarova. Upravo zbog toga, opisani centralni detektor posebno dobija na značaju.

Postupak detekcije se sastoji u utvrđivanju razlike u vremenu odziva pojedinih centrala u mreži u odnosu na uobičajene vrednosti. Pri tome su uobičajene vrednosti vremena odziva one koje važe za potpuno ispravnu mrežu tj. za veze koje su ostvarene prioritarnim putevima preko resursa koji pripadaju najnovijim tehnikama. Pogodnim izborom praga vremena  $PDD$  promašaj u detekciji može potpuno izbeći. Centralni detektor pokazuje porast verodostojnosti detekcije sa porastom sume cifara pozivnog broja koji se bira. Ovo se može postići izborom pogodnog imenika ili biranjem ispitnog telefona sa velikom sumom cifara pozivnog broja.

## LITERATURA

- [1] V. Matić, A. Lebl, D. Mitić, Ž. Markov, "Influence of numbering scheme on the efficiency of failure detector in electric power utility", *Przeglad Elektrotechniczny (Electrical Review)*, R. 89, NR 9, 2013., pp. 319-322.
- [2] V. Matić, A. Lebl, D. Mitić, Ž. Markov, "Determination of more realistic target 95% values of post selection delay in modern telephone networks", *Radio-engineering*, vol. 21, no. 1, April 2012., pp. 364-367.
- [3] Ekularn Dhavarudha and Prawit Denvorakul, "The design of reliable VoIP for power utilities' voice service", *CIGRE 2007 Colloquium*, Lucerne, Switzerland, Study Committee D2, 2007., paper D2-01 C11.
- [4] "Adaptacija i inovacija projekta telefonske mreže sa aspekta primene IP tehnologije i nove organizacije Elektroprivrede", ETF, Beograd, 2007.
- [5] ITU-T, "Digital exchange performance design objectives", *Recommendation Q.543*, March 1993.
- [6] Ž. Markov, I. Manević, "Determination of more stringent criterion for common control unit of digital telephone exchange", *Int. Journal of Eletronics and Communications*, vol. 52, 1998., pp. 101-103.
- [7] IETF, "RFC 3261, SIP: Session Initiation Protocol", June 2002.
- [8] Villy Iversen, "Teletraffic engineering and network planning", DTU Course 34340, Technical University of Denmark, 2011.

# UTICAJ NEIDEALNE ESTIMACIJE KANALA NA PERFORMANSE CELULARNOG POKRIVANJA PREKO UAV-ova

## IMPACT OF IMPERFECT CHANNEL ESTIMATION ON UAVs-CELLULAR COVERAGE PERFORMANCES

Uglješa Urošević<sup>1</sup>, Zoran Veljović<sup>1</sup>  
*Elektrotehnički fakultet, Univerzitet Crne Gore<sup>1</sup>*

**Sadržaj** – Celularno pokrivanje velikih događaja može ponekad predstavljati problem, obzirom na činjenicu da se mjesta većih događanja u mrežnom planiranju ne pretpostavljaju sa tolikim opterećenjem. Takođe, u sadašnjim društvenim mrežama jedna od ključnih karakteristika je ogromno povećanje live uplink saobraćaja. U takvim situacijama često je ključno pružiti odgovarajući kvalitet servisa. Moguće rješenje za ispunjavanje tih zahtjeva je uvođenje bespilotnih letilica (UAV - Unmanned Aerial Vehicles) koje mogu djelovati kao releji između bazne stanice (BS) i mobilnih jedinica (MU – Mobile Unit). Ovdje je razmotreno kako neidealna estimacija kanala utiče na jedan praktični scenario za implementaciju UAV-ova za distribuiranu realizaciju prostornog diversity-ja, tj. MIMO (Multiple Input Multiple Output) kanala između MU i BS.

**Abstract** - Cellular covering of big events can be sometimes difficult, due to the fact that places of happening in network planning are not assumed to be so crowded. Also, in present social networks one of the key characteristics is tremendous increasing of uplink live streams. In these situations it is often critical to provide appropriate quality of service. A solution for meeting these requirements is implementation of unmanned aerial vehicles (UAVs) that can act as relays between base station (BS) and mobile units (MUs). Here, we considered how imperfect channel estimation impacts on a practical scenario for UAVs implementation, for distributed realization of space diversity, i.e. multiple input multiple output (MIMO) channel between MUs and BS.

### 1. UVOD

UAV-ovi se koriste u različitim aplikacijama, kao što su saobraćajna sigurnost, vojne operacije, operacije spašavanja, pokrivanje velikih događaja, itd. [1]- [5]. Praćenjem saobraćajnih linija i slanjem informacija operativnom centru, sigurnost saobraćaja može se značajno poboljšati. Odnosi između UAV-ova i vojske sve su više vidljiviji. Svaka moderna vojska koristi UAV-ove u komunikaciji i praćenju dijela svojih aktivnosti ili na kraju u ofanzivnim akcijama. Operacije spašavanja u udaljenim i izolovanim područjima olakšavaju se s UAV-ovima, a procenat uspjeha može se povećati. Ovdje smo se fokusirali na pokrivenost velikih događaja putem UAV-ova. Na primjer, veliki muzički festivali se često održavaju u područjima gdje mobilna mreža nije planirana za tako velik broj korisnika. Dalje, jedan od

glavnih trendova u društvenim mrežama, tokom posljednjih nekoliko godina, je želja mnogih korisnika za live streaming-om. Ogroman broj korisnika, posebno mlađi, koristi gotovo svaku priliku za live streaming. Zbog toga, uplink konekcija na velikim događajima je ponekad kritična, a korisnici nemaju odgovarajuće iskustvo.

Jedno od praktičnih rješenja za ispunjavanje tih zahtjeva, posebno vezano za uplink konekcije, predstavlja implementacija UAV-ova za poboljšanje celularne pokrivenosti. UAV-ovi se mogu koristiti kao relejne stanice (RS) između bazne stanice (BS) i mobilnih jedinica (MU), [6] - [8]. Implementacija UAV-ova može značajno smanjiti uticaj multipath fadinga, zbog realne pretpostavke da će linija vidljivosti (LOS) između UAV-a i MU-a postojati. Takođe, može se očekivati direktna putanja između BS i UAV-a. Očito, ovo rješenje s UAV-ovima pruža brojne prilike u poređenju sa scenarijem gdje je BS daleko od mjesta događaja.

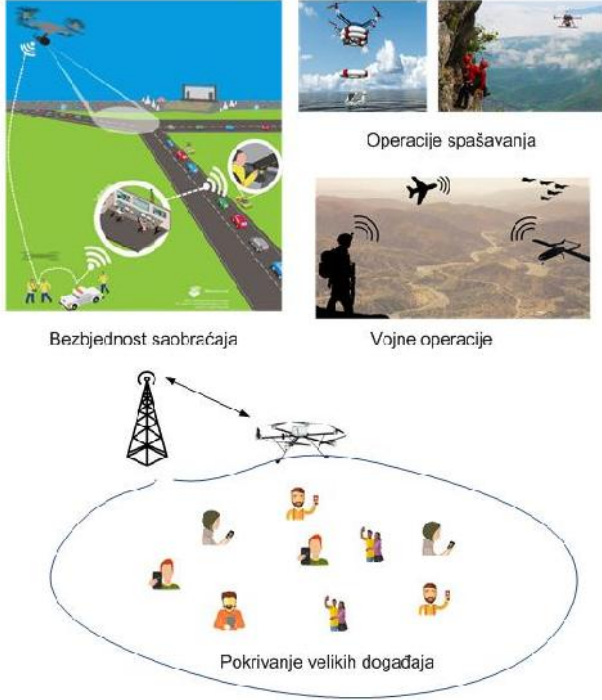
Postoji nekoliko važnih pitanja kada se UAV-ovi koriste kao releji između BS i krajnjih korisnika. Odnos između složenosti i cijene UAV-ova podrazumijeva da UAV-ovi ne bi trebalo da obavljaju složenu obradu signala kao što je dekodiranje i prosleđivanje (DF - Decode and Forward). Takođe, modulacije višeg reda, potrebne za dobijanje potrebnih kapaciteta, povećavaju kašnjenje u slučaju DF obrade. Drugi problem je potrošnja energije koja zahtijeva nove načine za produženje vremena rada UAV-a.

Ovdje je razmotren uticaj neidealne estimacije kanala u praktičnom scenariju za implementaciju UAV-ova kao releja između BS-a i MU-a. Analizirana je distribuirana realizacija prostorno vremenskih kodova (STBC - Space Time Block Codes). STBC-ovi su podesni za praktičnu primjenu i pripadaju tehnikama prostornog diversity-ja, [9]-[12]. Tehnike prostornog diversity-ja se mogu koristiti za povećanje pouzdanosti komunikacije, za povećanje energetske efikasnosti zbog činjenice da se mogu postići iste BER performanse uz manji odnos potrebne energije po bitu itd. To je posebno važno u implementaciji UAV-ova, jer je jedan od glavnih ciljeva produženje radnog vremena. Poređene je izvršeno u odnosu na vjerovatnoću greške na mjestu prijema, u slučaju uplink komunikacije.

### 2. RAZMATRANI SCENARIO

Različite primjene UAV-ova, poput bezbjednosti saobraćaja, vojnih operacija, operacija spašavanja i

pokrivanja velikih događaja, prikazane su na sl. 1. Posebno je razmatrana posljednja varijanta. Specifičan podslučaj je dat na sl. 2, gdje postoji mnoštvo pametnih telefona, mnogo live stream-ova itd. što otežava postizanje odgovarajućeg kvaliteta servisa. Ovdje je razmotren jedan praktični uplink scenario za implementaciju UAV-ova kao releja.



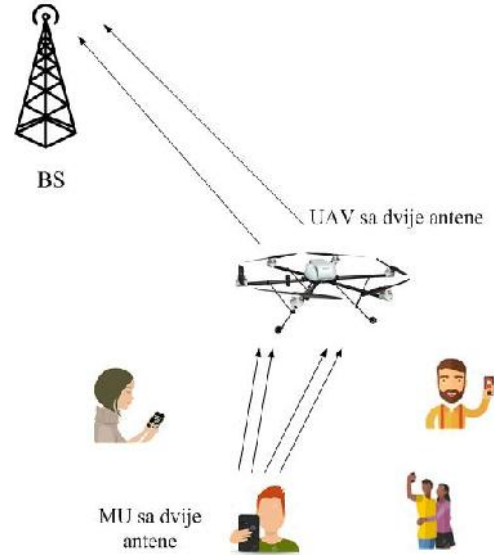
Slika 1. Različite primjene UAV-ova



Slika 2. Mnoštvo smart telefona i mnoštvo live konekcija

Scenario podrazumijeva da su UAV i MU-ovi opremljeni sa po dvije antene, sl. 3. Ovdje se distribuirani STBC, namijenjen za klasične MIMO sisteme sa četiri antene može realizovati, [13]-[14].

$$\text{OSTBC}_{4, 1/2} = \frac{1}{\sqrt{8}} \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 & a_1^* & -a_2^* & -a_3^* & -a_4^* \\ a_2 & a_1 & a_4 & -a_3 & a_2^* & a_1^* & a_4^* & -a_3^* \\ a_3 & -a_4 & a_1 & a_2 & a_3^* & -a_4^* & a_1^* & a_2^* \\ a_4 & a_3 & -a_2 & a_1 & a_4^* & a_3^* & -a_2^* & a_1^* \end{bmatrix} \quad (1)$$



Slika 3. Uplink scenario, UAV i MU-ovi su opremljeni sa po dvije antene

Postupak prenosa je sledeći.

Za svaka četiri informaciona simbola  $a_n$ ,  $n=1, \dots, 4$ , MU generiše dvije sekvence simbola koje se emituju sa dvije antene:

$$\mathbf{MU}_{1,\text{OSTBC}} = \frac{1}{\sqrt{4}} \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 & a_1^* & -a_2^* & -a_3^* & -a_4^* \end{bmatrix} \quad (2)$$

$$\mathbf{MU}_{2,\text{OSTBC}} = \frac{1}{\sqrt{4}} \begin{bmatrix} a_2 & a_1 & a_4 & -a_3 & a_2^* & a_1^* & a_4^* & -a_3^* \end{bmatrix} \quad (3)$$

Ukoliko je  $h_{\text{UAV}_i-\text{MU}_j}$  koeficijent kanala između  $i$ -te,  $i=1,2$ , antene na  $\text{UAV}_i$ , i  $j$ -te,  $j=1,2$ , antene na  $\text{MU}_j$ , a  $h_{\text{BS}-\text{UAV}_i}$  koeficijent kanala između BS i  $i$ -te antene na UAV, tada je prejemna sekvenca na  $\text{UAV}_i$ :

$$\mathbf{UAV}_{i,\text{in,OSTBC}} = \sum_{j=1}^2 \mathbf{MU}_{j,\text{OSTBC}} \cdot h_{\text{UAV}_i-\text{MU}_j} + \mathbf{N}_{\text{UAV}_i,\text{OSTBC}} \quad (4)$$

$\mathbf{N}_{\text{UAV}_i,\text{OSTBC}}$  je AWGN na  $\text{UAV}_i$ :

gdje je:

$$\mathbf{N}_{\text{UAV}_i,\text{OSTBC}} = [n_{\text{UAV}_i,1,\text{OSTBC}} \ n_{\text{UAV}_i,2,\text{OSTBC}} \ \dots \ n_{\text{UAV}_i,8,\text{OSTBC}}] \quad (5)$$

Izlazne sekvence na  $\text{UAV}_i$  su:

$$\mathbf{UAV}_{1,\text{out,OSTBC}} = \frac{1}{\sqrt{2}} \mathbf{UAV}_{1,\text{in,OSTBC}} \quad (6)$$

$$\begin{aligned} \text{UAV}_{2,\text{out,OSTBC}} = & \\ \frac{1}{\sqrt{2}} \left[ \begin{array}{cccc} -\text{UAV}_{2,\text{in,OSTBC}}(4) & -\text{UAV}_{2,\text{in,OSTBC}}(3) & \text{UAV}_{2,\text{in,OSTBC}}(2) & \text{UAV}_{2,\text{in,OSTBC}}(1) \\ -\text{UAV}_{2,\text{in,OSTBC}}(8) & -\text{UAV}_{2,\text{in,OSTBC}}(7) & \text{UAV}_{2,\text{in,OSTBC}}(6) & \text{UAV}_{2,\text{in,OSTBC}}(5) \end{array} \right] & (7) \end{aligned}$$

Prijemna sekvenca na BS je:

$$\text{BS}_{\text{in,OSTBC}} = \sum_{i=1}^2 \text{UAV}_{i,\text{out,OSTBC}} \cdot h_{\text{BS-UAV}i} + \mathbf{N}_{\text{BS,OSTBC}} \quad (8)$$

$\mathbf{N}_{\text{BS,OSTBC}}$  je AWGN na BS:

$$\mathbf{N}_{\text{BS,OSTBC}} = [n_{\text{BS1,OSTBC}} \ n_{\text{BS2,OSTBC}} \ \dots \ n_{\text{BS8,OSTBC}}] \quad (9)$$

Virtuelni 4x1 MISO kanal između MU i BS je kreiran:

$$\text{BS}_{\text{in,OSTBC}} = \frac{1}{\sqrt{8}} \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 & a_1^* & -a_2^* & -a_3^* & -a_4^* \\ a_2 & a_1 & a_4 & -a_3 & a_2^* & a_1^* & a_4^* & -a_3^* \\ a_3 & -a_4 & a_1 & a_2 & a_3^* & -a_4^* & a_1^* & a_2^* \\ a_4 & a_3 & -a_2 & a_1 & a_4^* & a_3^* & -a_2^* & a_1^* \end{bmatrix}^T \begin{bmatrix} H_{1,\text{OSTBC}} \\ H_{2,\text{OSTBC}} \\ H_{3,\text{OSTBC}} \\ H_{4,\text{OSTBC}} \end{bmatrix} + \mathbf{N}_{\text{OSTBC}} \quad (10)$$

gdje je:

$$H_{1,\text{OSTBC}} = h_{\text{UAV1-MU1}} \cdot h_{\text{BS-UAV1}} \quad (11)$$

$$H_{2,\text{OSTBC}} = h_{\text{UAV1-MU2}} \cdot h_{\text{BS-UAV1}} \quad (12)$$

$$H_{3,\text{OSTBC}} = h_{\text{UAV2-MU2}} \cdot h_{\text{BS-UAV2}} \quad (13)$$

$$H_{4,\text{OSTBC}} = h_{\text{UAV2-MU1}} \cdot h_{\text{BS-UAV2}} \quad (14)$$

i:

$$\begin{aligned} \mathbf{N}_{\text{OSTBC}} = & \mathbf{N}_{\text{BS,OSTBC}} + \frac{1}{\sqrt{2}} \mathbf{N}_{\text{UAV1,OSTBC}} \cdot h_{\text{BS-UAV1}} + \\ \frac{1}{\sqrt{2}} \left[ \begin{array}{cccc} -n_{\text{UAV23,OSTBC}} & -n_{\text{UAV24,OSTBC}} & n_{\text{UAV21,OSTBC}} & n_{\text{UAV22,OSTBC}} \\ -n_{\text{UAV27,OSTBC}} & -n_{\text{UAV28,OSTBC}} & n_{\text{UAV25,OSTBC}} & n_{\text{UAV26,OSTBC}} \end{array} \right] \cdot h_{\text{BS-UAV2}} & (15) \end{aligned}$$

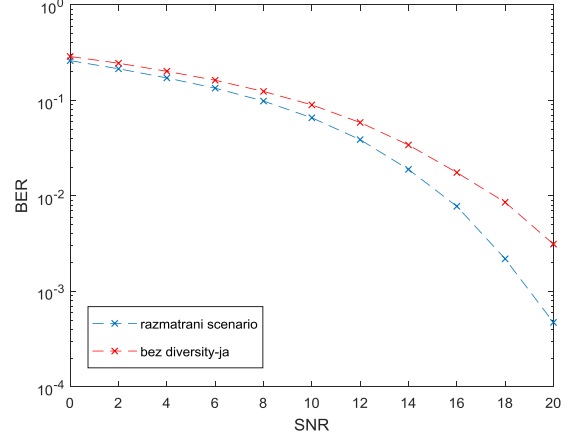
### 3. SIMULACIONI REZULTATI

Poređenje je izvršeno u odnosu na BER performanse. Pretpostavljen je Rice-ov fading na oba linka, između MU-a i UAV-a kao i između UAV-a i BS-a.

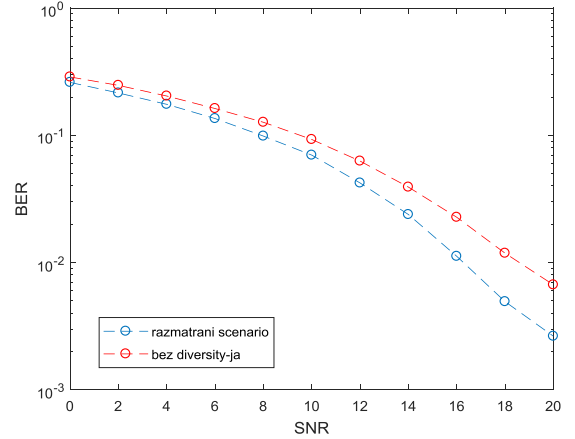
BER performanse u zavisnosti od odnosa signal/šum (SNR) po bitu, za 64QAM modulacionu šemu, su prikazane su na slikama 4, 5 i 6. Pretpostavljeno je da je Rice-ov faktor 10dB na linku između UAV i BS, odnosno 6dB na MU-UAV linku. Razmatrana je realna situacija sa neidealnom estimacijom kanala, pri čemu su date BER performanse za MSPE (*Mean Square Percentage Error*) vrijednosti od 1%, 2% i 3%. BER performanse šeme razmatranog scenarija su upoređene sa slučajem kada su svi mrežni elementi opremljeni samo jednom antenom, odnosno kada nema diversity-ja. Npr. u slučaju upoređivanja razmatranog scenarija sa slučajem bez diversity-ja SNR dobitak za BER vrijednost  $2 \cdot 10^{-3}$  iznosi 2dB (MSPE=1%).

Kao što se može uočiti što je veća greška prilikom estimacije lošije su BER performanse.

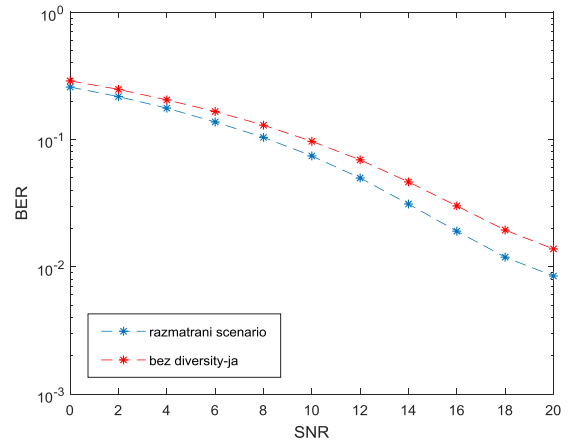
Kao što se može primijetiti, pretpostavljeno je da BS ima samo jednu antenu. Treba napomenuti da broj antena na BS-u može biti proizvoljan i više antena bi smanjilo BER vrijednosti, ali nema uticaja na proces kodiranja. Takođe, modulacija višeg reda ne povećava vrijeme obrade u UAV-ovima jer nema STBC dekodiranja.



Slika 4. BER performanse 64QAM, MSPE=1%



Slika 5. BER performanse 64QAM, MSPE=2%



Slika 5. BER performanse 64QAM, MSPE=3%

#### 4. ZAKLJUČAK

U ovom radu je razmotren uticaj neidealne estimacije kanala kod primjena UAV-ova kao rješenja za poboljšanje celularne pokrivenosti na velikim događajima, uz mnoštvo pametnih telefona, live stream-ova itd. gdje je teško postići odgovarajući kvalitet servisa na uplinku. Pretpostavljen je praktični scenario sa uplink komunikacijom između MU-a i BS-a, preko UAV-a, za distribuiranu realizaciju STBC-a, kao rješenje za poboljšanje ukupnih rezultata.

#### LITERATURA

- [1] L. Gupta, R. Jain, G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," *IEEE Communications Surveys & Tutorials*, Volume: 18, Issue: 2, 2016.
- [2] Z. Xiao, P. Xia, X. Xia, "Enabling UAV cellular with millimeter-wave communication: potentials and approaches," *IEEE Communications Magazine*, Volume: 54, Issue: 5, May 2016.
- [3] S. Hayat, E. Yanmaz, R. Muzaffar, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," *IEEE Communications Surveys & Tutorials*, Volume: 18, Issue: 4, 2016.
- [4] L. Afonso, N. Souto, P. Sebastiao, M. Ribeiro, T. Tavares, R. Marinheiro, "Cellular for the skies: Exploiting mobile network infrastructure for low altitude air-to-ground communications," *IEEE Aerospace and Electronic Systems Magazine*, Volume: 31, Issue: 8, Aug. 2016.
- [5] N. H. Motlagh, T. Taleb, O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," *IEEE Internet of Things Journal*, Volume: 3, Issue: 6, Dec. 2016.
- [6] Y. Zeng, R. Zhang, T. J. Lim, "Throughput Maximization for UAV-Enabled Mobile Relaying Systems," *IEEE Transactions on Communications*, Volume: 64, Issue: 12, Dec. 2016.
- [7] F. Ono, H. Ochiai, R. Miura, "A Wireless Relay Network Based on Unmanned Aircraft System With Rate Optimization," *IEEE Transactions on Wireless Communications*, Volume: 15, Issue: 11, Nov. 2016.
- [8] L. Sboui, H. Ghazzai, Z. Rezki, M. Alouini, "Achievable Rates of UAV-Relayed Cooperative Cognitive Radio MIMO Systems," *IEEE Access*, Volume: 5, April 2017
- [9] O. S. Badarneh, R. Mesleh, "Space-Time Block Codes from Orthogonal Designs," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 360 - 363, August 2016.
- [10] S. Ma, Y. Yang, H. Sharif, "Distributed MIMO Technologies in Cooperative Wireless Networks," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 78– 82, May 2011.
- [11] H. Jafarkhani, *Space-Time Coding, Theory and Practice*, Cambridge University Press, 2005.
- [12] T. Yamaoka, Y. Hara, N. Fukui, H. Kubo and T. Yamazato, "A Simple Cooperative Relaying with Alamouti Coded Transmission," *IEICE Trans. Commun.*, Vol. E95–B, No.2, pp. 643-646, February 2012.
- [13] U. Urosevic, Z. Veljovic, M. Pejanovic-Djurisic, "A New Solution for Simple Cooperative Relaying", *Wireless Personal Communications*, Vol. 75, Issue 2, pp. 1235-1250, Springer, March 2014.
- [14] Z. Veljovic, U. Urosevic, "Increasing Code Rate of the Cooperative Relaying with Virtual OSTBC", *Wireless Personal Communications*, Vol. 83, Issue 1, pp. 399-410, Springer, July, 2015.



# Single RAN u mreži "Telekom Srbija" područje Kopaonika Single RAN in "Telekom Srbija" network Kopaonik area

Danijela Aleksić<sup>1</sup>, Saša Gavrić<sup>1</sup>, Nemanja Protić<sup>1</sup>, Miljana Milić<sup>2</sup>  
Telekom Srbija<sup>1</sup>  
Elektronski fakultet, Univerzitet u Nišu<sup>2</sup>

**Sadržaj** – Cilj ovog rada je prepoznavanje ideje SRAN koncepta, kao rešenja za sve veću složenost sloja makro radio pristupa, koji se brzo razvija i donosi brojne nove pogodnosti za mobilne operatere širokopojasnih mreža. SBTS (Single BTS) proizvodi podržavaju Single RAN (radio mrežne pristupe) i RAT (radio mrežne tehnologije) u okviru jedinstvenog SW paketa. Pored toga, SRAN koncept podrazumeva jednu radio-instalaciju sa zajedničkim transportnim, operativnim i upravljačkim sistemom, kao i sa integriranim jedinstvenim zaštitnim sistemom za sve RAT-ove. U radu su date smernice SRAN modularnosti, koja omogućava skalabilnost kapaciteta u skladu sa korisničkim saobraćajnim zahtevima. SRAN rešenje je uspešno implementirano u mobilnoj mreži "Telekom Srbija", a finalna analiza dodatnih pogodnosti je data na kvalitativnoj osnovi.

**Abstract** -The goal of this paper is to propose the idea behind SRAN (Single Radio Access Network) solution for ever-growing intricacy of the macro radio access layer that it is being developed rapidly and will bring many new benefits for mobile broadband operators. SBTS (Single BTS) Product includes Single RAN and RAT (Radio Access Technology) features, all packaged into a single SW delivery. In addition, SRAN will comprise one radio installation with common transport, operational and management system with integrated unified security across RATs. This paper defines guidelines for SRAN modularity, allowing capacity to be scaled up in line with demand. SRAN solution has been successfully implemented in "Telekom Srbija" network, and main benefits are concluded, but only on a qualitative basis.

## 1. UVOD

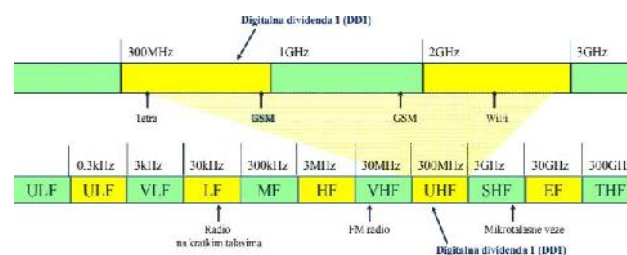
Sve zahtevnije telekomunikaciono tržište, pored kvalitetne, brze i ekonomski prihvatljive usluge, nameće potrebu za visokim stepenom mobilnosti, što upravo širokopojasnu pristupnu mobilnu mrežu čini pogodnim prostorom za nove konvergentno orijentisane servise. Neminovan tehnološki razvoj, pojava sve većeg broja aplikacija i uređaja koji koriste resurse mobilnih mreža, kao i mnogostruki rast količine prenetih podataka, inicijalni su stimulatori razvoja i izgradnje novih, kao i optimizacije postojećih mobilnih mrežnih arhitektura.

Imajući u vidu da je radiofrekvencijski (RF) spektar ograničeni prirodni resurs, efikasno upravljanje licenciranim frekventnim opsezima i alokacija mrežnih tehnologija u njima, postaju sve veći izazov mrežnim operaterima. Kao pogodni i nužni mehanizmi efikasnog iskorišćenja spektra prepoznati su procesi refarming-a,

korišćenje digitalnih dividendi i koegzistencija tehnologija i servisa.

Refarming, kao konsolidacija radiofrekventnog spektra, u opštem slučaju predstavlja prirodnu migraciju starijih tehnologija u cilju oslobađanja frekventnih resursa i njihove dodele novim, spektralno efikasnijim mrežnim tehnologijama.

Strateško planiranje frekventnih opsega omogućava nastanak digitalnih dividendi, odnosno oslobađanje poželjnih frekventnih opsega, u kojima se implementacija novih tehnologija može lakše ostvariti uz izbegavanje interferencija, usklađivanje zahteva za pograničnom koordinacijom, obezbeđivanje roaming-a i sveukupni povoljniji ekonomski aspekt. Posebno je od interesa digitalna dividenda 1 (DD1), opseg 790-862 MHz (opseg na 800MHz) koji se koristi za mobilne širokopojasne sisteme četvrte generacije [1].



Slika 1. RF spektar i DD1

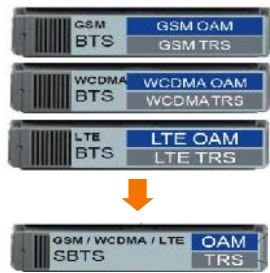
Dobre propagacione karakteristike u nižim frekventnim opsezima, bolje pokrivanje većih teritorija u ruralnim krajevima, kao i dodatno proširenje kapaciteta u CA (Carrier Aggregation) konfiguracijama u urbanim oblastima, daju prednost korišćenju digitalnih dividendi.

Koegzistencija tehnologija i servisa se sve češće pored tehničkih, geografskih i vremenska ograničenja, proširuje na deljenje frekventnih resursa, a u skladu sa opštom harmonizacijom na evropskom ili međunarodnom nivou [2]. Aktuelne su studije koje se odnose na inteligentne sisteme CR (Cognitive Radio), koji mogu da prepoznaju „praznine“ u već dodijeljenom spektru i adaptirano ih koriste [3].

Analiza implementiranog SRAN rešenja u mobilnoj mreži "Telekom Srbija" je data u narednim poglavljima. U drugom poglavlju su najpre date osnove SRAN mrežnog koncepta, a zatim i konkretni SRAN model. Glavni dobici ostvareni ovim rešenjem istaknuti su u poglavlju Kvalitativna analiza.

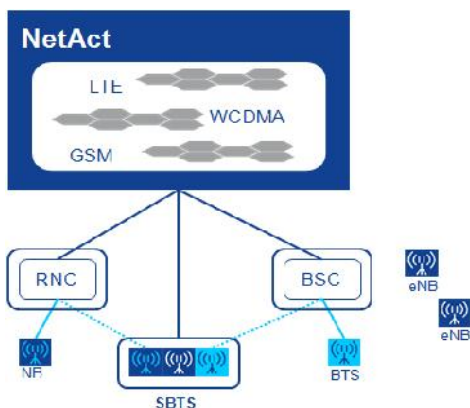
## 2. SRAN KONCEPT

SRAN (Single Radio Access Network - Single RAN) konfiguracije podržavaju pojedinačne radio mrežne pristupe (RAN) i radio mrežne tehnologije (RAT), istovremeno u konkurentnom operabilnom modu. SRAN koncept, odnosno model jedinstvene radio pristupne mreže, pojednostavljuje sve veću složenost sloja makro radio pristupa, nudeći brojne pogodnosti mobilnim radio operaterima. Visoka modularnost SRAN konfiguracija, operativna efikasnost poboljšana deljenjem mrežnih resursa i optimizacijom istih, dodatno su unapređeni sa aspekta energetske i sveukupne ekonomske efikasnosti.



Slika 2. Migracija na SRAN

Glavni motiv za ponudu SRAN rešenja je upravo uvođenje LTE tehnologije u GSM i UMTS okruženju, uz potencijalno efikasnije balansiranje saobraćaja mobilnih radio tehnologija, na osnovu monitoringa korisničkog saobraćaja. Ideja SRAN konfiguracije je elegantna - različite radio tehnologije rade na jedinstvenoj hardverskoj platformi sa zajedničkim transportnim i O&M pristupom. Već implementirani hardver na sajtovim a sa GSM i/ili UMTS baznim stanicama se može iskoristiti u SRAN rešenju, uz mogućnost implementacije LTE tehnologije u dodatnim frekventnim opsezima. Unificiranost O&M pristupa podrazumeva postojanje jednog entiteta za sve tehnologije na jedinstvenom NetAct-u (NSN OSS-u).



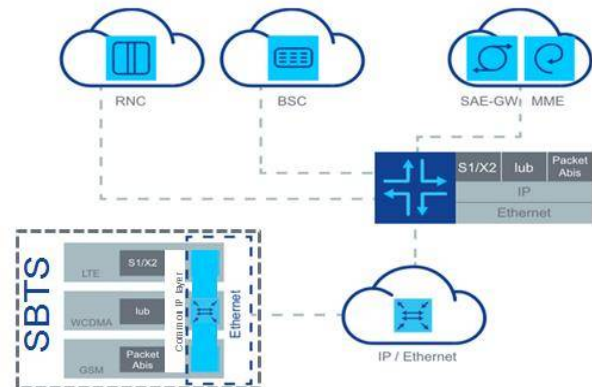
Slika 3. SRAN OAM - NetAct integracija

Preduslov za realizaciju jedinstvenog SRAN sajta je ALLIP Ethernet transportni pristup, čime se podiže sigurnost mrežne i korisničke strukture, obzirom na postojeću izloženost bezbedonosnom riziku kod IP mreža. Sa aspekta transportnog mrežnog sloja SBTS (SRAN

bazna stanica) je jedinstveni IP host sa fleksibilnim VLAN i IP adresiranjem, jedinstvenom ToP licencom, QoS i IPsec konceptom.

Migracija transporta na jedinstveni Ethernet pristup, uključuje i modelovanje postojećih i/ili planiranih interfejsa:

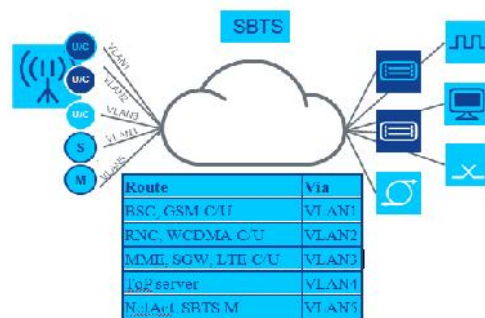
- GSM Packet Abis over Ethernet
- WCDMA IP Iub
- LTE S1/X2



Slika 4. Migracija transporta

IP adresni concept i VLAN specifikacija u SRAN konfiguraciji su veoma fleksibilni. U tom smislu se mogu rezervirati deljene (shared) i individualne (dedicated) IP adrese za RAT-ove kao i U/C/S/M ravni (User/ Control/ Synchronization/ Management Plane). Za SBTS M-ravan se uvek dodeljuje jedinstvena IP adresa, koja se u ekstremnom slučaju može deliti sa ostalim ravnima.

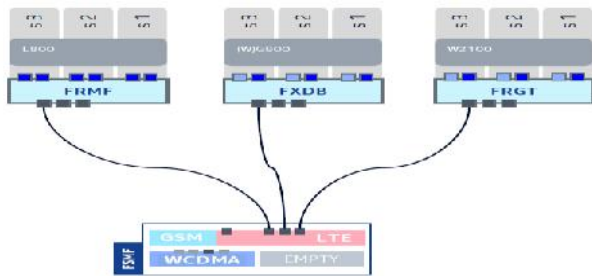
Prihvaćeni IP adresni koncepti VLAN specifikacija u mreži "Telekom Srbija" je:



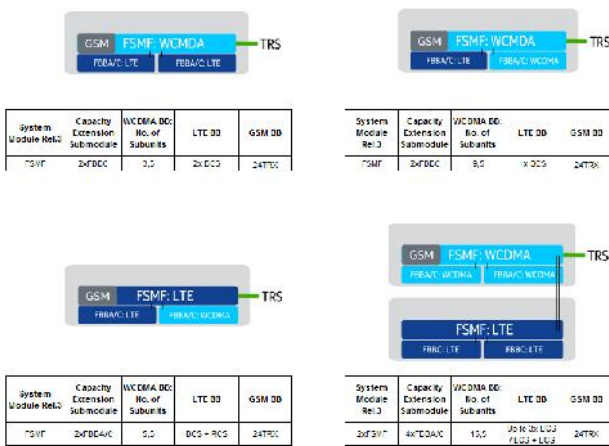
Slika 5. VLAN koncept

Modularni BB (Baseband) dizajn omogućava mobilnim operaterima inicijalnu HW konfiguraciju sa minimalnim kapacitetom, odnosno sa jedinstvenim ili zajedničkim BB kapacitetom Sistemskog modula (FSMF). Dalje proširenje BB procesnih kapaciteta moguće je ostaviti daljinskim softverskim korekcijama, fizičkim dodavanjem FBBA/C modula za proširenje kapaciteta i ulančavanjem dodatnih sistemskih modula (FSMF).

Na sl. 6 je prikazana minimalna SRAN konfiguracija za 3 RAT-a, a potencijalne modularne arhitekture i BB kapaciteti su date na sl.7.

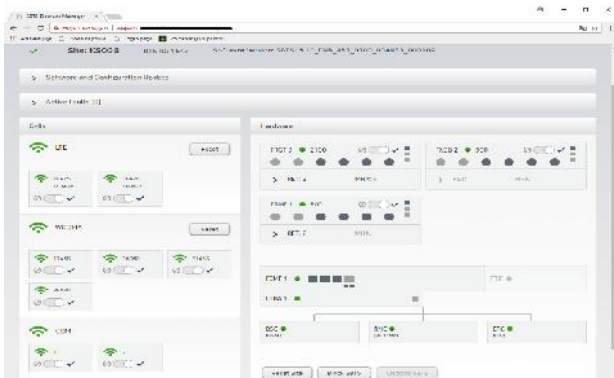
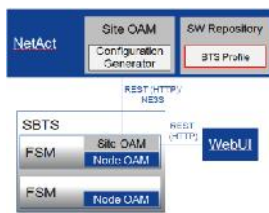


Slika 6. Minimalna SRAN konfiguracija za 3 RAT-a



Slika 7. Potencijalne HW konfiguracije 3 RAT-a

Obzirom da aktuelna konfiguracija mora biti deo BTS SW profila, a uzimajući u obzir ograničenja maksimalne HW konfiguracije podržanu tim profilom, potrebno je prilagoditi željene kapacitete po RAN tehnologijama.

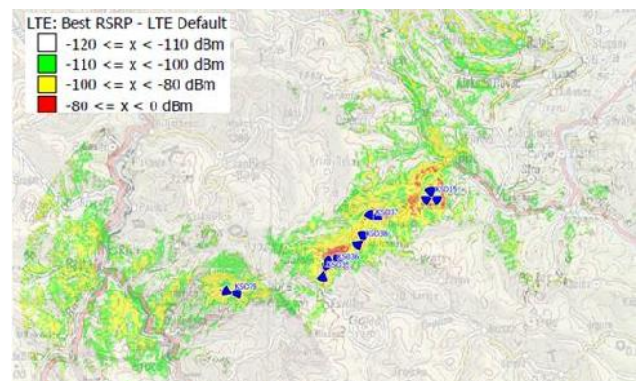
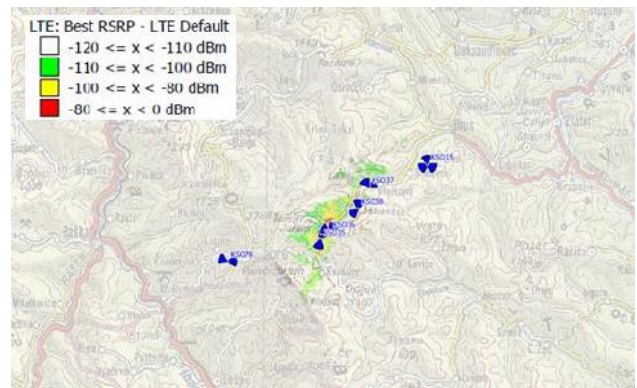


Slika 8. WebUI za SRAN 16.10

### 3. KVALITATIVNA ANALIZA

SRAN mrežni koncept je rešenje koje je u mobilnoj mreži "Telekom Srbija" implementirano samo na području Kopaonika. U prvoj fazi projekta su odrađena SRAN rešenja na sajtovima duž prilaznih putnih pravaca, dok se u drugoj fazi planira i realizacija SRAN rešenja na sajtovima u centru kompleksa kao i duž skijališnih staza. Motivacioni aspekt projekta je poboljšanje pokrivanja 4G signalom u DD1 frekventnom opsegu (opseg na 800 MHz).

U nastavku na sl.9 su date uporedne analize pokrivanja teritorije 4G signalom pre i nakon implementacije SRAN rešenja. Prikazi se odnose izolovano samo na područje pokrivanja sajtova na kojima su realizovana SRAN rešenja, dok su ostali sajtovi kao i pokrivanje koje potiče od tih sajtova, izostavljeni iz analize.



Slika 9. Uporedne predikcije pokrivanja 4G signalom

### 4. ZAKLJUČAK

U radu je najpre dat osnovni idejni koncept SRAN rešenja, pogodnog za makro radio pristupni sloj, kao i motivacioni aspekt prihvatljivosti ovog rešenja za više RAT-ova. Predočeni su preduslovi i minimalni zahtevi za realizaciju SRAN koncepta, kao i konkretno rešenje realizovano u mobilnoj mreži "Telekom Srbija". Aktuelne konfiguracije odlikuje visoki stepen modularnosti što dodatno olakšava adaptaciju prema porastu korisničkog saobraćaja po RAT-ovima. Glavni argument kvalitativne analize je značajno poboljšanje pokrivenosti LTE mrežom, koja po izboru mobilnih operatera treba da omogući širokopoljasne usluge prenosa podataka. Sveukupna ekonomska i dodatna energetska efikasnost, nisu predmet ovog rada, ali dodatno

ostavljaju prostora za dalje analize predloženog SRAN koncepta.

## **LITERATURA**

[1] CEPT Report 30 - "The identification of common and minimal (least restrictive) technical conditions for 790 - 862 MHz for the digital dividend in the European Union", October 2009

[2] ECC Report 80, "Enhancing harmonisation and introducing flexibility in the spectrum regulatory framework", Oulu, March 2006

[3] Report ITU-R SM.2405-0, "Spectrum management principles, challenges and issues related to dynamic access to frequency bands by means of radio systems employing cognitive capabilities", Jun 2017



# SIMULACIONI MODEL ORGANIZACIJE PREVOZA GRAĐEVINSKOG MATERIJALA NA PLOVNIM PUTEVIMA SIMULATION MODEL OF TRANSPORT OF BUILDING MATERIALS ON INLAND WATERWAYS

Katarina Milović, Danijela Pjevčević, Vladislav Maraš, Aleksandar Radonjić  
*Univerzitet u Beogradu, Saobraćajni fakultet*

**Sadržaj** - Predmet rada je analiza organizacije prevoza građevinskog materijala od Velikog Gradišta na Dunavu, do Žablja na Tisi. Simulaciono modeliranje je izvršeno u softveru „Simio”. Definisani su pokazatelji rada transportnih i pretovarnih sredstava i praćeni kroz scenarije angažovanja različitog broja potiskivača i sastava potisnica.

**Abstract** - The subject of the paper is an analysis of the organization of the transport of building material from Veliko Gradište on the Danube river, to Žabalj on Tisa river. Simulation modeling was done in the Simio software. The indicators of the operation of transport and handling devices have been defined and monitored through the development of scenarios of a different number of pushers and tows (composition of barges).

## 1. UVOD

Zahvaljujući niskim transportnim troškovima i masovnosti, unutrašnji vodni transport je veoma značajan vid transporta tereta [1]. Organizacija transporta, i izbor metode prevoženja, zavisi od osobina, pojavnog oblika i količine robe koja se prevozi. Na organizaciju transporta na unutrašnjim plovnim putevima utiču osobine plovnog puta, karakteristike transportnih i manipulativno-pretovarnih sredstava, kao i veličina i oblik robnih tokova.

Predmet ovog rada je analiza organizacije prevoza građevinskog materijala u cilju povećanja iskorišćenosti transportnih i pretovarno manipulativnih sredstava.

Transport građevinskog materijala – šljunka, obavlja se na unutrašnjim plovnim putevima Srbije, i to na reci Dunav od Velikog Gradišta (km 109 reke Dunav), i na reci Tisi do Žablja (km 36 reke Tise) [2].

U radu je razmatran procesa prevoženja građevinskog materijala potiskivanim sklopom koji čine motorni potiskivač i sastav od četiri potisnice.

Izvršeno je simulaciono modeliranje procesa prevoženja građevinskog materijala na posmatranoj relaciji. Razmatrano je više scenarija u zavisnosti od broja angažovanih sastava i potiskivača. Broj sastava se kretao od dva do četiri u kombinaciji sa jednim ili dva potiskivača.

## 3. OSNOVNE KARAKTERISTIKE PROSECA PEVOŽENJA ŠLJUNKA

Šljunak po svojim osnovnim osobenostima ne spada u grupu materijala koji su osetljivi na atmosferske i klimatske uslove, tako da se skladišti na otvorenim deponijama i prevozi u otvorenim plovilima.

U razmatranom transportnom zadatku potrebno je izvršiti prevoz 600000 t šljunka ( $G = 600000$  t) od Velikog Gradišta do Žabalja. Usvaja se da je navigacioni period (period fizički moguće plovidbe) na posmatranoj relaciji 300 dana ( $T_p = 300$  dana).

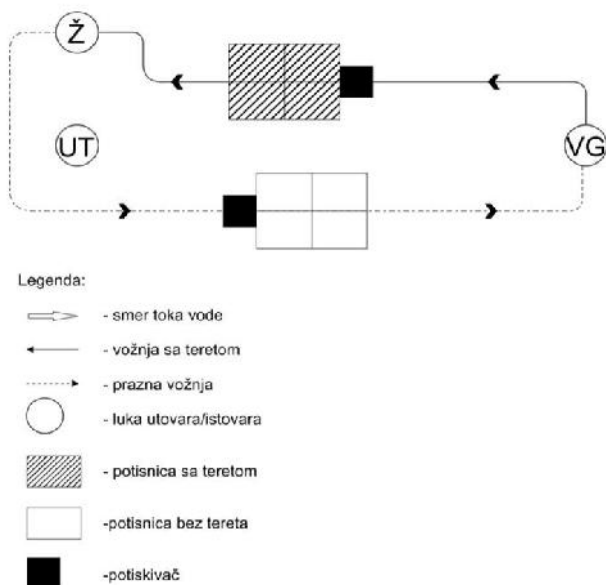
Prevoz šljunka od Velikog Gradišta do Žabalja obavlja se potiskivanim sastavom sa potiskivačem. Prevoz je direktan, tj. broj potisnica u sastavu je konstantan, i ne menja se na mestima utovara i istovara i u toku plovidbe. Izabrana je polukontinualna (poluslobodna) veza između sastava potisnica i potiskivača, što znači da u toku plovidbe ili na mestima utovara ili istovara može doći do preuzimanja sastava od strane drugih potiskivača.

Karakteristični podaci prevoza na zadatoj relaciji prikazani su u tabeli 1.

Tabela 1: Polazni podaci

Naziv i oznaka veličine		Vrednost
Rastojanje - Dunav	$l^D$ (km)	156
Rastojanje - Tisa	$l^T$ (km)	36
Količina tereta	$G$ (t)	600 000
Navigacioni period	$T_p$ (dani)	300
Eksploataciona nosivost potisnice	$Q_e(t)$	1248

Na slici 1. data je šema plovidbe na relaciji Veliko Gradište – Žabalj.



Slika 1. Šema plovidbe

### 3. RAZVOJ SIMULACIONOG MODELA PREVOZA ŠLJUNKA

Modeliranje transportnog procesa ima odlučujuću ulogu pri tekućem i operativnom planiranju rada flote.

U radu je simuliran proces prevoženja šljunka od utovarnog mesta Veliko Gradište do istovarnog mesta Žabalj potiskivanim sklopom.

Pri analizi tehnološkog procesa prevoza šljunka uočavaju se veličine, kao što su: vremena utovar i istovara, vremena plovidbe i sl., koje se opisuju kvantitativno, ali koje se kreću u određenim granicama, odnosno, pri ispitivanja ili posmatranja uzimaju različite vrednosti, pa se mogu smatrati slučajnim promenljivim.

Velikim brojem ispitivanja ili posmatranja utvrđuje se ono što je zajedničko za te promenljive, odnosno određuju se tipične vrednosti statističkog obeležja [3].

Koristeći podatke iz putnih listova brodova o vremenima nizvodne i uzvodne plovidbe na posmatranoj relaciji pri prevozu šljunka utvrđeno je da se empirijska raspodela verovatnoća uzorka vremena plovidbe ponaša po zakonu Normalne raspodele.

Takođe je utvrđeno da se vremena utovara i istovara šljunka portalnim dizalicama u mestu utovara i mestu istovara mogu opisati Normalnom raspodelom.

U cilju modeliranja transportnog procesa prevoženja šljunka za početni simulacioni eksperiment korišćene su sledeće pretpostavke:

- ✓ Količina šljunka koju je potrebno prevesti je  $G=600000$  t;
- ✓ Mesto utovara - Veliko Gradište km 109 reke Dunav; Mesto istovara – Žabalj km 36 reke Tise;
- ✓ Navigacioni period na posmatranoj relaciji je 300 dana;
- ✓ Prevoz se obavlja potiskivanim sklopom koji čini motorni potiskivač i sastav od četiri potisnice;
- ✓ Eksploataciona nosivost jedne potisnice je 1248 t;
- ✓ Vreme uzvodne plovidbe sastava može se opisati Normalnom raspodelom sa sledećim parametrima  $N(\mu=30.2h; \sigma=3.3h)$
- ✓ Vreme nizvodne plovidbe sastava može se opisati Normalnom raspodelom sa sledećim parametrima  $N(\mu=11.5h; \sigma=2.7h)$
- ✓ Norma utovara se može opisati Normalnom raspodelom sa parametrima  $N(\mu=23.4h; \sigma=3.5h)$ ;
- ✓ Norma istovara se može opisati Normalnom raspodelom sa parametrima  $N(\mu=29.6h; \sigma=4.3h)$ .

Pored navedenih vrednosti, za polazne podatke u simulacionom modelu, preuzete su i proračunate vrednosti:

- ✓ Rastojanje na relaciji V.Gradište – Žabalj iznosi 192 km.
- ✓ Vreme tehničkih operacija pri utovaru i istovaru je po 3h;
- ✓ Vreme koje potiskivač provede na mestima utovara/istovara (vreme formiranja i rasformiranja sastava) je 2h;

Simulacioni model procesa prevoženja šljunka razvijen je u simulacionom softveru „SIMIO” [4]. Posmatrano je više simulacionih scenarija u cilju praćenja definisanih pokazatelja pri promeni broja sastava i broja potiskivača.

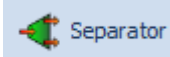
Pri izradi simulacionog modela u simulacionom softveru „SIMIO” korišćeni su sledeći objekti:

**Source** - Objekat *Source* je objekat koji generiše entitete (izvor), i definiše njihov broj i učestalost njihovog stvaranja. Korišćen je za generisanje potiskivanih sastava, kao i za generisanje tereta koji se transportuje (šljunka).

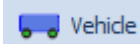
**Combiner** – Objekat *Combiner* se koristi za spajanje dva različita entiteta, tj. ukupnjivanje jedinica. Moguće je definisati vreme potrebno da se taj proces izvrši, kao i vreme koje je potrebno da svaki od



entiteta pristupi u objekat. Korišćen je za proces utovara šljunka u potisnice.



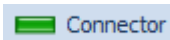
**Separator** – Objekat *Separator* modelira proces koji razdvaja članove (entitete) koji su grupisani. Moguće je definisati vreme potrebno da se taj proces izvrši, kao i vreme koje je potrebno da svaki od entiteta pristupi u objekat. Korišćen je za proces istovara šljunka iz potisnice.



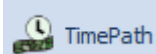
**Vehicle** – Objekat *Vehicle* predstavlja vozilo koje transportuje entitete između određenih tačaka. Korišćen je kao sredstvo transporta, motorni potiskivač.



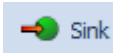
**BasicNode** – Objekat *Basic Node* predstavlja određenu tačku u mreži.



**Connector** – Objekat *Connector* predstavlja direktnu vezu između tačaka ili objekata u sistemu, podrazumevajući da je rastojanje između te dve tačke jednako nuli.

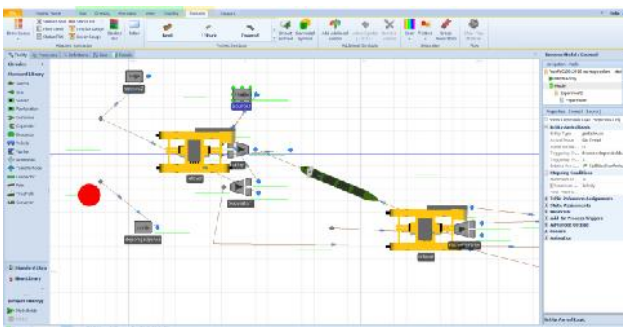


**TimePath** – objekat *Time Path* predstavlja stazu između dve tačke, sa tačno definisanim vremenom putovanja između te dve tačke. Korišćen je za predstavljanje plovidbe sklopa od mesta utovar do mesta istovara.



**Sink** - objekat *Sink* predstavlja izlaz iz sistema. Korišćen je da uništi objekte (entitete) čiji proces u modelu je završen (šljunak koji je istovaren).

Radna površina simulacionog softvera „SIMIO” sa objektima i njihovim međusobnim vezama pri izradi simulacionog modela prevoza šljunka, prikazana je na Slici 2.



Slika 2. Radna površina simulacionog softvera „SIMIO”

#### 4. ANALIZA SIMULACIONIH REZULTATA

Za analizu procesa prevoženja šljunka definisani su i praćeni sledeći pokazatelji rada:

- ✓ Prosečno vreme čekanja praznih potiskivanih sastava – vreme koje svi potiskivani sastavi nakon istovara

provedu čekajući na potiskivač u mestu istovara, podeljeno sa brojem istovarenih potiskivanih sastava.

- ✓ Prosečno vreme čekanja utovarenih potiskivanih sastava – vreme koje svi potiskivani sastavi nakon utovara provedu čekajući na potiskivač u mestu utovara, podeljeno sa brojem utovarenih potiskivanih sastava.
- ✓ Prosečno vreme čekanja potiskivača- vreme koje potiskivač provede čekajući na prazan ili utovaren potiskivni sastav u mestu istovara ili utovara, podeljeno sa brojem angažovanih potiskivača.
- ✓ Iskorišćenost dizalice na utovaru šljunka - odnos vremena efektivnog rada dizalice na utovaru šljunka sa ukupnim vremenom trajanja prevoženja šljunka.
- ✓ Iskorišćenost dizalice na istovaru šljunka - odnos vremena efektivnog rada dizalice na istovaru šljunka sa ukupnim vremenom trajanja prevoženja šljunka.

Razmatrano je šest scenarija sa po 100 ponavljanja. Izlazni rezultati simulacionih scenarija prikazani su u tabeli 2.

Tabela 2. Rezultati simulacionih eksperimenata

	Scenario					
	1	2	3	4	5	6
<b>BAP</b>	2	1	1	2	2	2
<b>BAS</b>	2	3	4	2	3	4
<b>T<sub>p</sub> (dan)</b>	300	300	300	300	300	300
<b>TP<sub>p</sub> (dan)</b>	360	243	243	260	187	184
<b>TČ<sub>ps</sub> (h)</b>	40,80	16,70	63,74	0,00	6,41	39,78
<b>TČ<sub>ns</sub> (h)</b>	0,00	24,60	24,63	0,00	0,00	0,00
<b>TČ<sub>s</sub> (h)</b>	40,80	41,30	88,37	0,00	6,41	39,78
<b>TČ<sub>p</sub> (h)</b>	22,80	1,50	0,00	54,40	24,80	23,90
<b>ID<sub>u</sub> (%)</b>	32,60	38,40	38,40	40,40	39,50	39,87
<b>ID<sub>i</sub> (%)</b>	41,40	51,80	51,80	49,90	50,40	50,10

**BAP** - Broj angažovanih potiskivača

**BAS** - Broj angažovanih sastava

**T<sub>p</sub>** - Trajanje navigacionog perioda

**TP<sub>p</sub>** - Vreme potrebno za realizaciju prevoza

**TČ<sub>ps</sub>** - Prosečno vreme čekanja praznog sastava

**TČ<sub>ns</sub>** - Prosečno vreme čekanja natovarenog sastava

**TČ<sub>s</sub>** - Ukupno prosečno čekanje sastava

**TČ<sub>p</sub>** - Prosečno vreme čekanja potiskivača na sastav potisnica

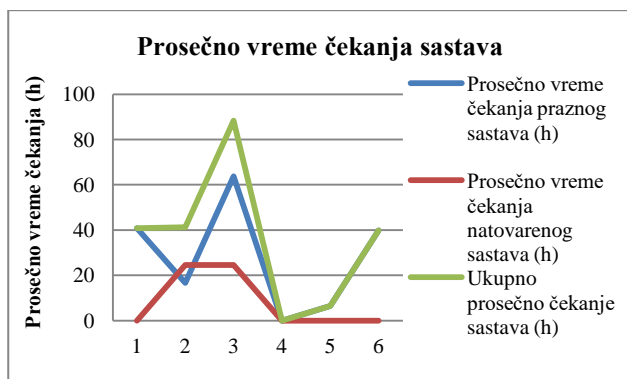
**ID<sub>u</sub>** - Prosečna iskorišćenost dizalice na utovaru

**ID<sub>i</sub>** - Prosečna iskorišćenost dizalice na istovaru

Pri analizi dobijenih rezultata, potrebno je uzeti u obzir da se u posmatranom modelu, angažovani potiskivači, sastavi potisnica, kao i dizalice na mestu utovara i mestu istovara koriste samo za proces prevoženja šljunka, što se naravno razlikuje od realnog sistema.

Pokazatelji su definisani i praćeni samo za predloženi sistem prevoženja.

Na grafiku 1. dat je prikaz ukupnog prosečnog vremena čekanja sastava na potiskivač.



Grafik 1. Prosečno vreme čekanja sastava

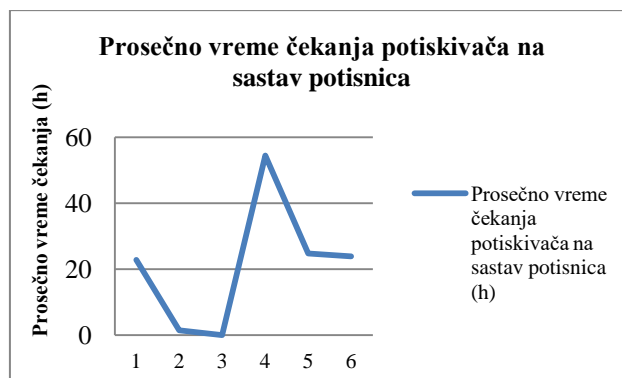
Na osnovu prikazanih rezultata prosečnog vremena čekanja praznih i natovarenih sastava, kao i ukupnog prosečnog vremena čekanja sastava, izvodi se zaključak da se povećavanjem broja angažovanih sastava povećava i ukupno prosečno vreme čekanja sastava na potiskivač.

Pri angažovanju jednog potiskivača i dva sastava ukupno prosečno vreme čekanja sastava iznosi 41,4 časova, dok porast broja sastava za jedan donosi povećanje vremena čekanja za 0,5 časova. Angažovanje dva dodatna sastava prouzrokuje povećanje vremena čekanja za čak 47,5 časova.

Angažovanje dva potiskivača sa dva sastava potisnica obezbeđuje rad bez čekanja sastava na potiskivač. Uključivanje dodatnog sastava izaziva ukupno prosečno vreme čekanja od 6,41 časova, dok još jedan dodatni sastav ima za posledicu ukupno prosečno vreme čekanja sastava na potiskivač od ukupno 39,78 časova.

Kako potiskivač i sastav rade u sklopu, neophodno je analizirati i prosečno vreme čekanja potiskivača na sastav.

Grafik 2. daje prikaz prosečnog vremena čekanja potiskivača na sastav potisnica.

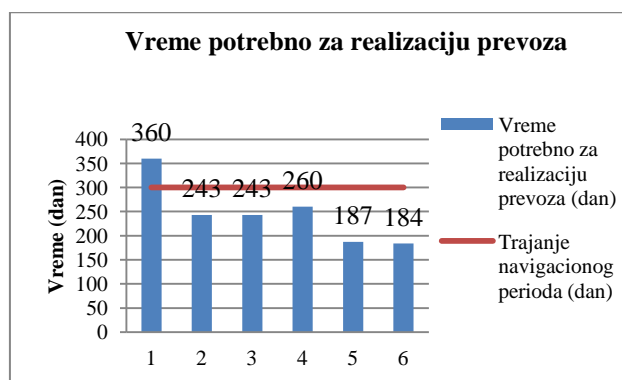


Grafik 2. Prosečno vreme čekanja potiskivača na sastav potisnica

Na osnovu tabele 2. i grafika 2. očigledno je da vreme čekanja potiskivača na sastav opada sa povećanjem broja sastava. Pri angažovanju jednog, kao i pri angažovanju dva potiskivača njihovo prosečno vreme čekanja je najveće kada se angažuju dva sastava potisnica. U prvom slučaju (Scenario 1) iznosi 22,8 časova, dok je drugom (Scenario 4) više nego udvostručeno i iznosi 54,4 časa.

Dakle, može se zaključiti da povećanje broja angažovanih sastava utiče na smanjenje prosečnog vremena čekanja potiskivača. Najbolje rešenje organizacije prevoza je kada potiskivač nema vremenske gubitke, ili su minimalni.

Simulacijom je utvrđen vremenski period potreban za realizaciju prevoza zadate količine šljunka na posmatranoj relaciji od Velikog Gradišta do Žablja u zavisnosti od predložene organizacije. Grafik 3. daje prikaz potrebnog vremena i njegovo odstupanje od projektovanog navigacionog perioda.

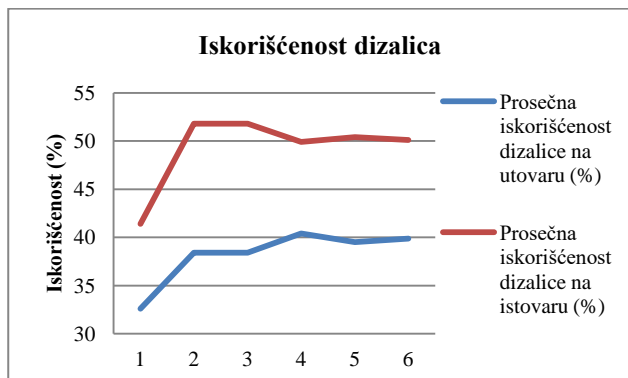


Grafik 3. Vremenski period potreban za realizaciju prevoza šljunka

Na osnovu prikazanog grafika, zaključak je da osim prvog scenarija, svi ostali zadovoljavaju zahtev da se prevoz izvrši u toku navigacionog perioda od 300 dana. Naravno među scenarijima postoje veće razlike u trajanju prevoza povećanjem broja angažovanih potiskivača. Angažovanjem dva potiskivača i tri, odnosno četiri

sastava potisnica, vreme potrebno za realizaciju prevoza šljunka je njmanje i iznosi 187 dana, odnosno 184 dana.

Dizalice koje su angažovane na utovaru i istovaru zadate količine šljunka imaju relativno nisku iskorišćenost, posmatrano u vremenskom periodu u kome se realizuje prevoz. Dijagram iskorišćenosti dizalica na utovaru i istovaru prikazan je na grafiku 4.



Grafik 4. Iskorišćenost dizalica na utovaru i istovaru

Prikazani rezultati iskorišćenosti dizalica ukazuju na potrebu njihovog dodatnog angažovanja na pretovaru drugih vrsta robe u mestu utovara i istovara kako bi se umanjio njihov prazan hod.

Pri donošenju odluke o izboru scenarija prevoženja šljunka na posmatranoj relaciji, potrebno je sagledati sve pokazatelje kako bi se donela ispravna odluka.

Na osnovu tumačenja ukupnog prosečnog vremena čekanja sastava na potiskivač ispravno bi bilo odlučiti se za Scenario 4. Scenario 4 podrazumeva angažovanje dva potiskivača i dva sastava potisnica. Ovakva organizacija prevoženja ima za rezultat ukupno prosečno vreme čekanja sastava na potiskivač jednako nuli ali je prosečno vreme čekanja potiskivača na sastav izuzetno visoko i iznosi 54,4 časova. Sa druge strane, na osnovu prosečnog vremena čekanja potiskivača na sastav ispravno bi bilo izabrati Scenario 2 ili Scenario 3, jer je u tim slučajevima vreme čekanja jednako nuli. Što se tiče vremena potrebnog za realizaciju prevoza zadate količine šljunka, najkraće vreme daje Scenario 6.

Dakle, potrebno je sagledati da li po svim posmatranim pokazateljima ijedan od navedenih scenarija može da se

izdvoji kao najbolje rešenje organizacije prevoženja šljunka na relaciji Veliko Gradište - Žabalj. Sumiranjem napred navedenog, kao najbolje rešenje organizacije prevoženja izdavanja se Scenario 2. Ovaj scenario podrazumeva angažovanje jednog potiskivača i tri sastava potisnica, realizaciju prevoza za 243 dana, sa prosečnim vremenom čekanja potiskivača na sastav od 1,5 časova i ukupnim prosečnim vremenom čekanja sastava na potiskivač 41,3 časova.

## 5. ZAKLJUČAK

Na osnovu usvojenih pretpostavki izrađen je simulacioni model i praćeni su definisani pokazatelji kroz različite scenarije angažovanja broja potiskivača i broja sastava. Prikazani rezultati kao najbolji scenario organizacije prevoženja šljunka izdvajaju Scenario 2, tj. prevoz šljunka od Velikog Gradišta do Žablja angažovanjem jednog potiskivača i tri sastava potisnica za 243 dana.

Razvijeni simulacioni model može da se koristi za analizu organizacije prevoza i drugih vrsta tereta.

Pored posmatranih pokazatelja potrebno je u analizu uključiti i troškove predloženih scenarija organizacije prevoza. Svakako, buduća analiza će obuhvatiti i ovaj aspekt organizacije prevoženja.

Naravno, pri izradi simulacionog modela od izuzetnog je značaja posmatranje mesta uključivanja sastava i potiskivača u proces prevoženja, što će svakako biti jedan od pravaca daljeg istraživanja.

## Literatura

1. Radmilović Z., *Transport na unutrašnjim plovnim putevima*, Beograd, Univerzitet u Beogradu, Saobraćajni fakultet, 2007.
2. Milošević, K., *Analitičko i simulaciono modeliranje prevoza građevinskog materijala na unutrašnjim plovnim putevima*, Završni rad, Beograd, Univerzitet u Beogradu, Saobraćajni fakultet, 2017.
3. Radenković, B., Stanojević, M., Marković, A., *Računarska simulacija*, Beograd, 1999.
4. <https://www.simio.com>

# Bežično upravljanje mobilnog robota pomoću Wi-Fi mreže putem Raspberry Pi3 uređaja

## Wireless control over a mobile robot via Wi-Fi network using Raspberry Pi3 device

Filip Ilić<sup>1</sup>, Đorđe Nisić<sup>2</sup>, Dušan Đorić<sup>2</sup>  
Vojna akademija, Univerzitet odbrane u Beogradu<sup>1</sup>  
Elektrotehnički fakultet, Univerzitet u Beogradu<sup>2</sup>

**Sadržaj** – U ovom radu je pokazan praktičan rad u kojem je opisano daljinsko upravljanje pomoću Wi-Fi komunikacije koje je implementirano na robotskoj platformi pametnog vozila. Komunikacija putem GPIO pinova je ostvarena između kompjutera ili Android mobilnog uređaja, klijentska strana, i Raspberry Pi3 uređaja, serverska strana, koji upravlja perifernim komponentama. Senzorski sistemi za merenje parametara su postavljeni na vozilu. Na osnovu merenja su izvršene određene upravljanja robotom.

**Abstract** – In this paper is described remote control using Wi-Fi communication, which is implemented on the smart vehicle robotic platform. The communication via GPIO pins is achieved between computer or Android phone, client side, and Raspberry Pi3 device, server side, which controls peripheral components. Sensor systems for measuring parameters are implemented on the vehicle. It was done particular control action of a robot based on acquired measurement.

### 1. UVOD

Sve šira rasprostranjenost mikrokontrolera je dovela do eksponencijalnog razvoja pratećeg softvera za upravljanje njima. Neki od njih su detaljno opisani u [1]. Na taj način se otvorila mogućnost ljudima koji nisu specijalisti iz oblasti elektronike i programiranja da razviju složenije sisteme upravljanja. Predložene osnove za rad su date u [2,3]. Međutim, ostvarivanje komunikacije i poznavanje programskog jezika nije upotpunjeno ukoliko se ne primenjuje na konkretan hardver. Ovakav sa sobom nosi i mnoge probleme, koji su predmet rešavanja, što u vidu optimizacije kodova, a nešto u vidu prilagođavanje softvera hardveru i obrnuto, [4]. Naravno, uvek je potrebno imati i uvid u rad sistema. To se ostvaruje implementacijom senzora, koji formiraju merenja, čijom obradom se mogu opisati karakteristike i ograničenja sistema, [5]. Konkretniji primeri komunikacije Raspberry Pi3 sa hardverom su dati u [6,7], dok su primene daljinskog upravljanja obrađene kroz radove [8,9]. Za softversku realizaciju sistema preuzete su gotove funkcije i biblioteke sa [10,11].

U ovom radu je ideja da se formira daljinsko upravljanje mobilnog robota pomoću Raspberry Pi3 a na osnovu predstavljenih rezultata u navedenim radovima. Ovako definisan sistem bi se mogao opisati kao sistem koji pokazuje kako sinergija više jednostavnijih komponenata

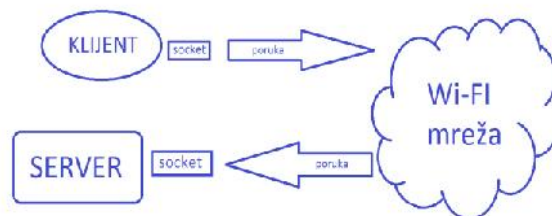
može biti svrsishodna. Pokazano je kako se sistemi za kretanje, komunikaciju i upravljanje senzora mogu projektovati i međusobno povezati tako da njihov produkt bude primenljiv i učini platformu spremnom za izvršavanje različitih funkcija i jednostavnu za održavanje i unapređenje.

### 2. OPIS SISTEMA

Komunikacija između klijenta i servera se odvija preko Wi-Fi mreže koristeći "Socket"-e. Prilikom uključivanja Raspberry Pi3 uređaja na napon, tj. prilikom podizanja operativnog sistema (NOOBS with Pixel), pokreću se dve skripte. Jedna od njih pokreće server za kretanje, dok druga pokreće server za kameru. Oba servera imaju istu IP adresu, IP adresa Raspberry Pi3 uređaja, dok je razlika u portu na kome oslušuju.

Klijent unosi IP adresu servera, i na taj način se javlja serveru i zahteva da ostvare konekciju kao što je prikazano na slici 1. Različitim komandama se zahteva povezivanje na različite servere. Potrebno je da se povezivanje izvrši u redosledu: server za kretanje, server za kameru.

Kada se sve konekcije uspostave, klijenti šalju poruke serverima na koje oni odreaguju ili odgovore nekom akcijom. Uglavnom poruke upravljaju stanjem GPIO pinova Raspberry Pi3 uređaja kojima se kontrolišu GATE-ovi MOSFET tranzistora.



Slika 1. Dijagram konekcije

### 3. HARDVERSKA REALIZACIJA

Za konstruisanje vozila korišćene su sledeće komponente:

- IRF 4095 MOSFET
- LED
- DC 3-6V Gear Motor
- 621D012 Relay DPDT

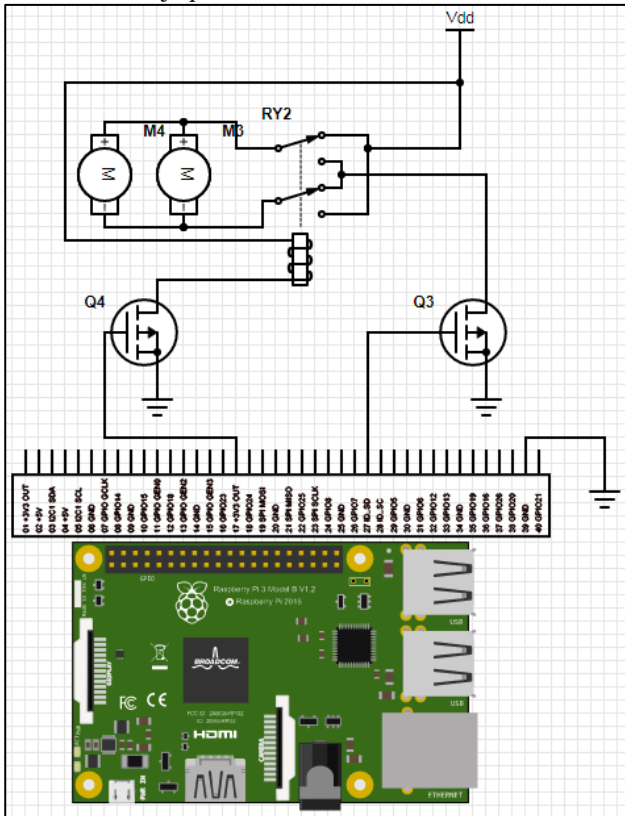


- 28BYJ-48-5V, Stepper Motor
- LDR Sensor Module
- IR Encoder Speed Motion Sensor Module
- Logitech Webcam C210
- Raspberry Pi3
- Baterije 1,5V - Napon napajanja

Na platformi su postavljena četiri točka koja se okreću pomoću DC motora koji su povezani na MOSFET tranzistore i releje. Sve komponente se napajaju sa redno vezanim baterijama od  $V_{dd} = 9\text{ V}$ .

Moguće je softverski upravljati motorima u oba smera preko Raspberry Pi3 uz pomoć releja, tako što se dovede napon od 6V na njegovim ulazima. Ovo dovodi do toga da se promeni smer struje koja prolazi kroz DC motor, a samim tim se promeni i smer okretanja točka.

Dovode se po dva signala sa Raspberry Pi3, jedan signal za pogon, drugi signal za okretanje smeru točkova na levoj strani vozila, i još dva takva signala za desnu stranu vozila, kao što je prikazano na slici 2.



Slika 2. Šematski prikaz upravljanja dva DC motora

Na ploči Raspberry Pi3 se nalaze četiri USB porta, što daje znatno lakšu komunikaciju sa drugim uređajima. Takva komunikacija ostvarena je web kamerom koja nam daje sliku u realnom vremenu prilikom upravljanja vozila. Kamera je postavljena na step motor koji omogućava okretanje kamere po uglu skretanja.

Na pinove step motora se naizmenično dovode signali sa Raspberry Pi3 i na taj način se upravlja radom step motora, što je prikazano na slici 3.

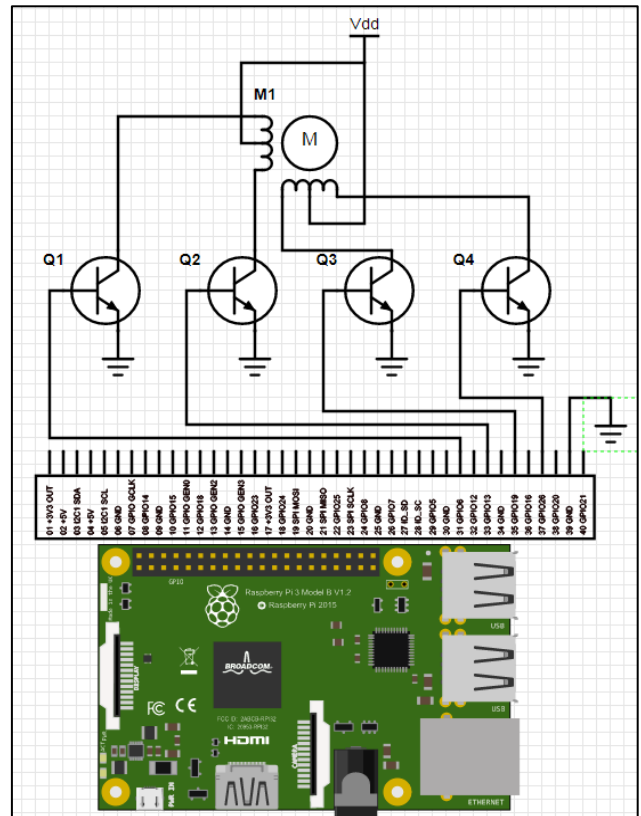
Na jedan točak koji pokreće vozilo ugrađen je IR Encoder Speed Motion Sensor Module i enkoder.



a) b)

Slika 4. Senzor moduli: a) IR Encoder Speed Motion Sensor Module, b) LDR Sensor Module

Kada se vozilo pokrene, enkoder se zajedno sa točkom okreće i njegovo okretanje registruje IR Encoder Speed Motion Sensor Module čije se dalje informacije obrađuju softverski i kao rezultat se dobija brzina kojom se kreće vozilo. Informacija o brzini vozila koristi se za automatsko kretanje vozila na određenu koordinatu koju zadaje korisnik.



Slika 3. Šematski prikaz upravljanja step motora

Na vozilo su ugrađeni senzor moduli prikazani na slici 4:

LDR Sensor Module je ugrađen na vozilo i povezan sa LED koje predstavljaju farove na vozilu. U slučaju da u prostoriji gde se vozilo nalazi nema dovoljno svetlosti LDR Sensor Module generiše struju LE diodama koje proizvode svetlost. Ovim je obezbeđeno uspešno upravljanje vozila i u noćnim uslovima.





Slika 5. Slika vozila sa uključenim farovima

#### 4. SOFTVERSKA REALIZACIJA

Softver korišćen za funkcionisanje vozila je pisan u Java programskom jeziku. Komunikacija između klijenta, programa na računaru ili smart telefonu, i servera, programa na Raspberry Pi3 uređaju, se obavlja preko "Socket-a". Komunikacija se izvršava tako što klijenti šalju poruke oblika "\_\_\_poruka\_\_\_" serveru.

Na Raspberry Pi3 uređaju se nalaze dva servera. Jedan je zadužen za primanje komandi koje se tiču kretanja, a drugi je zadužen za komunikaciju sa posebnom niti klijenta koja služi za prikazivanje kadra koji hvata kamera na vozilu. Server koji je zadužen za kretanje zapravo predstavlja beskonačnu petlju koja na početku svog izvršavanja proverava da li je pristigla neka poruka. Ukoliko nije, glavna nit servera se blokira sve dok poruka ne pristigne. Ukoliko je poruka stigla, server nastavlja dalje sa njenom obradom.

Postoji 7 osnovnih komandi za kretanje:

- napred
- nazad
- levo
- desno
- rotacija ulevo
- rotacija udesno
- zaustavi

Svaka od njih aktivira ili deaktivira određene GPIO pinove na Raspberry Pi3 uređaju. Pored ovih osnovnih komandi, postoje još dve dodatne komande za kontrolisanje step motora koji služi za pokretanje kamere, i još jedna komanda koja pokreće vozilo za zadati broj centimetara unapred.

Obradivanje komandi koje kontrolišu kretanje step motora funkcioniše tako što postoji posebna nit koja na zadatu komandu, npr. okreni nalevo ili okreni nadesno, pali i gasi određene GPIO pinove sa zadatim vremenskim razmakom, i na taj način podstiče kretanje step motora. Postoji i komanda koja zaustavlja kretanje step motora.

Obradivanje komande koja pokreće vozilo za zadati broj centimetara unapred koristi podatke koje očitava senzor za brzinu. Svakih 10 ms se proverava brzina vozila, i na osnovu tih podataka se ažurira predjeni put. Postoji posebna nit koja konstantno proverava brzinu vozila. Ovaj

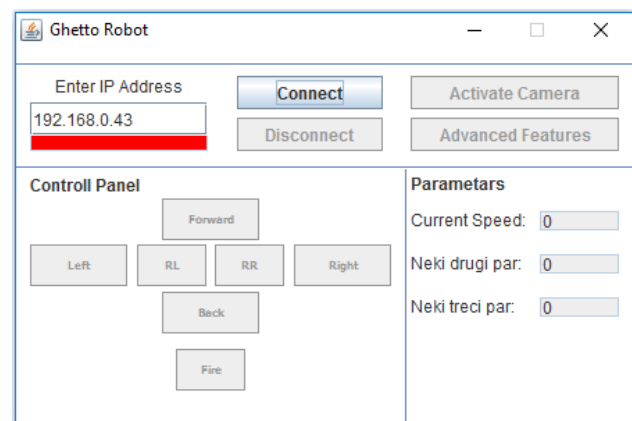
proces se ponavlja sve dok se pređeni put ne izjednači sa zadatim putem.

Za kontrolisanje GPIO pinova je korišćena biblioteka "Pi4Java" koja apstrahuje korišćenje pinova na visokom nivou. Ukoliko se želi aktivacija ili deaktivacija pina potrebno je samo napisati "broj\_pina.high()" ili "broj\_pina.low()".

Server za kameru je program koji šalje frejm po frejm klijentu. Slanje se izvršava tako što se prvo dohvati slika sa kamere u vidu matrice. Nakon toga se dobijena matrica pretvori u niz bajtova. Niz bajtova se deli na 5 manjih nizova odnosno blokova, veličine po 30000 bajtova, upakuje u vidu objekta, i šalje klijentu. Nakon toga se čeka odgovor klijenta da je primio blok bajtova i pošalje odgovor da je primio blok. Onda server šalje sledeći blok podataka, i ovakav protokol se sprovodi za svih 5 blokova nakon čega server ponovo prima sledeći frejm sa kamere i ponavlja prethodne korake.

Na klijentskoj strani se nalazi GUI prikazan na slici 6 sa sledećim funkcionalnostima :

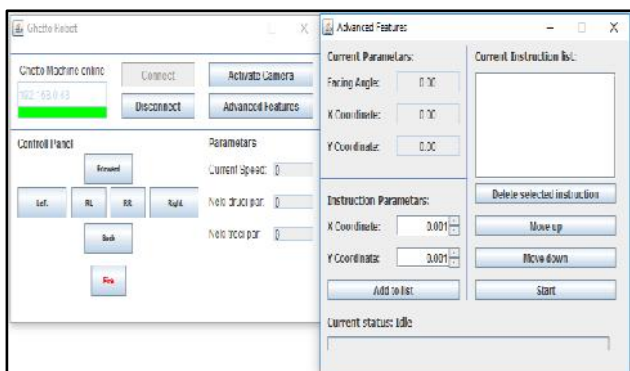
- tekstualno polje za IP adresu servera
- dugme CONNECT
- dugme DISCONNECT
- dugme za kretanje napred
- dugme za kretanje nazad
- dugme za kretanje levo
- dugme za kretanje desno
- dugme za rotiranje nalevo
- dugme za rotiranje nadesno
- dugme za napredne funkcionalnosti
- dugme za aktivaciju kamere



Slika 6. Glavni prozor GUI-a

Dugme CONNECT uspostavlja vezu sa serverom za kretanje, dok dugme DISCONNECT prekida vezu sa serverom. Svako dugme za kretanje, kao što su: napred, nazad, levo, desno, rotacija u levo, rotacija u desno, funkcioniše tako što se prilikom pritiska dugmeta šalje odgovarajuća poruka: levo, desno, napred, nazad, itd, a kada se dugme otpusti onda se šalje poruka "zaustavi". Ovo omogućava da se vozilo kreće u željenom pravcu sve dok držimo dugme. Kada ga pustimo, vozilo se zaustavlja. Takođe, vozilo je osetljivo na pritisak više

dugmadi odjednom, i uvek će se izvršavati poslednja zadata komanda. Primer : pritisnuto dugme “levo”, pritisnuto dugme “napred”, otpušteno dugme “napred”, otpušteno dugme “levo” rezultiraju sledeću kretanju vozila: “levo, napred, levo, zaustavi”.

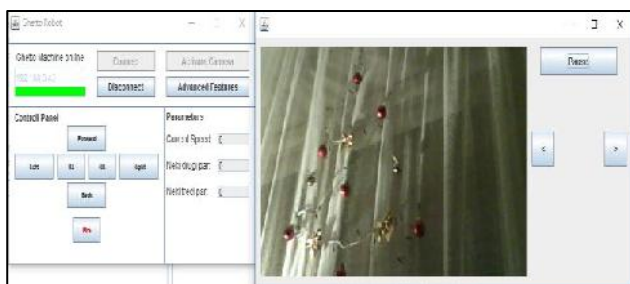


Slika 7. Glavni prozor sa prozorom za napredne funkcionalnosti

Dugme za napredne funkcionalnosti otvara novi prozor prikazan na slici 7, u kome će se nalaziti nove funkcionalnosti koje bi se ticale mapiranja prostora, pronalaženja najkraćeg puta, i još nekih tehnika vezanih za veštačku inteligenciju.

Dugme za aktivaciju kamere uspostavlja vezu sa serverom za kameru na Raspberry Pi3 uređaju. Nakon uspostavljanja veze, klijent prima blokove bajtova i šalje serveru povratne informacije o primanju bloka.

Nakon primljenih 5 blokova, klijentski program rekonstruiše matricu slike, a na osnovu nje i sliku. Slika se onda prikazuje u novom prozoru kao na slici 8. Ovi koraci se ponavljaju sve dok je uspostavljena veza sa serverom za kameru. Ona se gasi kada se isključi prozor za kameru, glavni prozor ili kada se prekine veza sa serverom za kretanje. Prenos sa kamere može da se pauzira i nastavi. Ovo se postiže tako što su i server za kameru i klijent koji prima slike servera zapravo dve niti koje mogu da se blokiraju i odblokiraju.



Slika 8. Glavni prozor sa prozorom za kameru

Na glavnom prozoru GUI-a se uvek ispisuje poslednja odrađena instrukcija ili greška u slučaju njenog postojanja.

Takođe, postoji i deo glavnog prozora GUI-a u kome se ispisuju trenutni parametri. Za sad je implementirano da se može očitavati trenutno stanje brzine kretanja vozila.

I klijentska i serverska strana koriste biblioteku “OpenCV” za primanje slike sa kamere i za predstavljanje te slike u vidu matrice.

## 5. ZAKLJUČAK

U radu je predstavljena i detaljno objašnjena upotreba Raspberry Pi3 uređaja kojim se preko Wi-Fi komunikacije uspešno daljinski upravlja mobilni robot. Primena ovako dizajniranog sistema je široka, naročito u okolnostima kada je potrebno sačuvati ljudski život.

Osnovne prednosti koje su primećene tokom rada su:

- Laka upravljivost sistema
- Jednostavna nadogradnja funkcionalnosti
- Potrebe za održavanjem su minimalne

Dok su mogući nedostaci:

- Ograničen opseg kontrole vozila u zavisnosti od dometa Wi-Fi mreže i
- Nadogradnja sistema može biti zahtevna u pogledu kapaciteta napajanja sistema

Formirani su predlozi za dalja istraživanja i unapređenja:

- Prelazak sa komunikacije putem Wi-Fi mreže na komunikaciju putem mobilne mreže, čime se znatno povećava domet upravljivosti vozila
- Obrada podataka prikupljenih kamerom
- Zamena trenutnih elektronskih komponenti kvalitetnijim i sofisticiranijim elektronskim komponentama
- Implementacija veštačke inteligencije

## LITERATURA

- [1] Ibrahim, D. (2006). *Microcontroller based applied digital control*. John Wiley & Sons.
- [2] Upton, E., & Halfacree, G. (2014). *Raspberry Pi user guide*. John Wiley & Sons.
- [3] Richardson, M., & Wallace, S. (2012). *Getting started with raspberry PI*. " O'Reilly Media, Inc."
- [4] Monk, S. (2016). *Raspberry Pi cookbook: Software and hardware problems and solutions*. " O'Reilly Media, Inc."
- [5] Maksimović, M., Vujović, V., Davidović, N., Milošević, V., & Perišić, B. (2014). *Raspberry Pi as Internet of things hardware: performances and constraints*. *design issues*, 3, 8.
- [6] Hoyo, Á., Guzmán, J. L., Moreno, J. C., & Berenguel, M. (2015). *Teaching control engineering concepts using open source tools on a Raspberry Pi board*. *IFAC-PapersOnLine*, 48(29), 99-104.
- [7] Leccese, F., Cagnetti, M., & Trinca, D. (2014). *A smart city application: A fully controlled street lighting isle based on Raspberry-Pi card, a ZigBee sensor network and WiMAX*. *Sensors*, 14(12), 24408-24424.
- [8] Bermudez-Ortega, J., Besada-Portas, E., López-Orozco, J. A., Bonache-Seco, J. A., & De la Cruz, J. M. (2015). *Remote web-based control laboratory for mobile devices based on EJS, Raspberry Pi and Node. js*. *IFAC-PapersOnLine*, 48(29), 158-163.

[9] Vujovic, V., & Maksimovic, M. (2014, May). Raspberry Pi as a Wireless Sensor node: Performances and constraints. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on* (pp. 1013-1018). IEEE.

[10] Retrieved October 15th, 2017, from <https://pi4j.com/>

[11] Retrieved October 15th, 2017, from <https://opencv.org/>

# SOFTVERSKI SISTEM ZASNOVAN NA BIOFEEDBACK METODI

## SOFTWARE SYSTEM BASED ON BIOFEEDBACK METHOD

Milana Prodanov<sup>1</sup>, Marija Punt<sup>1</sup>, Nadica Miljković<sup>1</sup>, Sanja Delčev<sup>1</sup>

*Elektrotehnički fakultet Univerziteta u Beogradu<sup>1</sup>*

**Sadržaj** - Računarska primena u oblasti medicinskog istraživanja radi poboljšanja fiziološkog stanja osobe predstavlja popularno polje u oblasti računarske tehnike i informatike. U ovom radu predstavljena je inicijalna verzija softverskog sistema čiji je cilj da primenom biofeedback metode pruži korisniku mogućnost da poboljša funkciju i aktivnost relaksacionog impulsa. Korišćenjem GSR instrumenta meri se provodnost kože, koja odražava stepen relaksiranosti korisnika. Putem simulacija računarski sistem pruža korisniku povratnu audio-vizuelnu informaciju u biofeedback sprezi. Sistem uključuje grafički prikaz vremenskog signala, koji je moguće softverski obrađivati i filtrirati, kao i niz interaktivnih simulacija čije izvršavanje direktno kontroliše korisnik.

**Abstract** - Computer applications in the field of medical research to improve the physiological condition of a person is a popular field in the area of Computer Engineering and Informatics. This paper presents initial version of a software system based on biofeedback method that aims to enhance the function and activity of a relaxation impuls. GSR instrument is used to measure the conductivity of the skin, which reflects the level of person's relaxation state. Through the use of computer simulations the system gives the user audio-visual information in a bio-feedback loop. The system includes signal view in time domain, various signal modifiers and filters, as well as a set of interactive simulations which are directly controlled by the user.

### 1. UVOD

Većina ljudi misli da nema apsolutno nikakvu kontrolu nad svojim biološkim funkcijama, kao što su krvni pritisak, temperatura kože ili mišićna napetost. Tačno je da nervni sistem vodi računa da se takve biološke stvari odvijaju automatski, međutim, istraživanja [1] pokazuju da svesnim naporom osoba može da utiče, pa i da izmeni ove ustaljene funkcije. Poznati su blagotvorni efekti meditacije kojom osoba uči da se relaksira i istovremeno povećava kontrolu nad sobom i svojim mislima, što direktno utiče na centralni nervni sistem i rad osnovnih bioloških funkcija.

Osim meditacije, postoje i druge tehnike koje mogu da pomognu u postizanju kontrole nad psihofizičkim stanjem i jedan od njih je i biofeedback metod [2]. Ovaj metod podrazumeva da osoba aktivno dobija povratnu informaciju o svom tekućem stanju u vidu audio-vizuelnih simulacija kojima direktno upravlja, što joj pomaže da nauči da kontroliše svoje emocije koje se fizički ispoljavaju ubrzanim disanjem, znojenjem i sličnim fiziološkim pokazateljima [3].

Jedan od pokazatelja stepena relaksacije korisnika je i električna osobina ljudske kože, koja ispoljava veću električnu provodnost prilikom psihičkog stanja uzbuđenosti (eng. *arousal*), odnosno odsustva relaksacije [4]. Merenja ne mogu da ukažu na to o kojoj vrsti uzbuđenosti se radi (nervoza, zabrinutost, bes, neverica, iščekivanje, itd.), već samo da je simpatetički nervni sistem aktiviran. Prema tome, smanjena uzbuđenost ukazuje da je osoba u stanju relaksacije, pa je provodnost kože jedan od bioloških signala kojim se može sprovesti biofeedback trening.

U ovom radu predstavljen je modularni softverski sistem koji može da prikuplja, obrađuje i prikazuje podatke sa senzora. Postojeći sistem može lako da se proširuje novim funkcijama i algoritmima obrade, načinima prikaza rezultata, kao i novim simulacijama. Projekat je zasnovan na biofeedback principu, gde korisnik aktivno dobija povratnu informaciju o svom tekućem stanju koje meri GSR senzorom. Komunikacija sa instrumentom je realizovana serijski, preko Arduino Uno A/D konvertora, dok je sam softverski sistem implementiran upotrebom Unity okruženja. Sistem ima okruženje za analizu signala i za biofeedback trening. Okruženje za analizu omogućava posmatranje i obradu signala u realnom vremenu, dok okruženje za trening sadrži skup različitih audio-vizuelnih simulacija čiji je cilj učenje korisnika kako da samovoljno utiče na stanje koje se meri. Softverski sistem je predviđen za upotrebu na desktop platformama.

U glavi dva predstavljen je teorijski pregled vezan za biofeedback metod i električnu provodnost kože, kao i opis postojećih instrumenata i prapratnog softvera. U glavi tri je opisan realizovani softverski sistem zasnovan na biofeedback metodi. Rezultati inicijalnog testiranja



sistema su predstavljeni u glavi četiri. U glavi pet dat je zaključak i dalji mogući pravci razvoja sistema.

## 2. OPIS PROBLEMA I POSTOJEĆA REŠENJA

Stres može da izazove reakciju tela na pretnje ili opasnosti, što je prirodan odgovor u odgovarajućim situacijama (eng. *Fight-or-Flight response*). Tokom ove reakcije, određeni hormoni poput adrenalina i kortizola se otpuštaju, što dovodi do ubrzavanja pulsa, usporavanja varenja, manevrisanja protoka krvi do velikih mišićnih grupa, kao i do promene raznih drugih funkcija autonomnog nervnog sistema [5], što dovodi do stvaranja dodatne energije i snage tela. Problem nastaje kada se stres veštački izaziva u svakodnevnim situacijama zbog saobraćaja, posla, novca i sl. Ljudski organizam je napravljen tako da se vraća u stanje normalnog funkcionisanja čim posmatrana pretnja nestane, međutim u današnje vreme hroničnog stresa, aktivacija relaksacionog impulsa se nedovoljno često dešava, što izaziva oštećenje organizma.

*Biofeedback* je metod kojim je moguće pospešiti nivo svesti o fiziološkim funkcijama, čime se otvara mogućnost da osoba utiče na samu sebe kako bi smanjila nivo stresa, odnosno kako bi poboljšala funkciju i aktivnost relaksacionog impulsa. Metod uključuje instrumente za merenje raznih bioloških signala koji su dobri pokazatelji stepena relaksacije (ili obrnuto, uzbuđenosti). Jedan od njih je svakako stepen otpornosti kože (eng. *Galvanic Skin Resistance - GSR*).

GSR je ujedno i jedan od najistraženijih bioloških indikatora i posledica je znojenja kože prilikom stanja uzbuđenosti. Znojenje kože ne mora biti vidljivo golim okom, ali se može izmeriti propuštanjem malih struja kroz elektrode postavljene na jagodicama prstiju i računanjem provodnosti (ili otpornosti) na osnovnu izmerenog napona među elektrodama. Što je osoba više uzbuđena simpatetički nervni sistem je više aktivan, što fizički rezultuje povećanim znojenjem kože. Vlažnija koža bolje provodi struju, odnosno, veća joj je provodnost [6]. Na slici 1 su prikazane znojne žlezde na kažiprstu (brazde predstavljaju otisak prsta) posmatrane pod elektronskim mikroskopom za veći i manji broj žlezda.



Slika 1. Znojne žlezde na kažiprstu

Softver i hardver za merenje provodnosti, odnosno otpornosti kože je relativno jeftin i jednostavan u poređenju sa drugim načinima poput EEG metode. U nastavku je dat opis nekih uređaja, kao i propratni softver koji ide uz njih.

### 2.1. PSYCHLAB

Ovaj GSR instrument kompanije *Contact Precision Instruments* [7], zajedno sa softverom za analizu signala, namenjen je za naučna istraživanja provodnosti kože kao posledice spoljašnjeg ili unutrašnjeg uticaja. *PsychLab* je u upotrebi još od 1986. i tada se koristio za slična istraživanja. Nudi visoku rezoluciju signala, prikaz i čuvanje vremenskih odbiraka, kao i mogućnost ručnog kreiranja proizvoljnih eksperimenata upotrebom slike, zvuka ili električnih šokova. Električno kolo za merenje provodnosti modelira kožu kao skup promenljivog broja paralelno vezanih otpornika, što je bolje rešenje od zadavanja određenog fiksnog broja otpornika, s obzirom da se broj aktivnih znojnih žlezda, a time i provodnika (ili otpornika) menja. *PsychLab* instrumentom je moguće meriti provodnost kože i unutar magnetnog polja, jer ni srebro ni srebro hlorid, od kojih su napravljene elektrode, ne menjaju osobine u takvoj okolini. S druge strane, pojačavač signala može da se lako udalji, tako da ne bude unutar Faradejevog kaveza. Sve ovo daje mogućnost upotrebe *PsychLab* GSR uređaja i MRI skenera istovremeno, čime se može pratiti više parametara u isto vreme. Na slici 2 je prikazana *PsychLab* aparatura. Gore levo su prikazani uređaji za generisanje zvučnog i električnog šoka, koji predstavljaju vrste spoljašnjih stimulatora. Gore desno su prikazane elektrode veličine 8mm koje se postavljaju na jagodične delove kažiprsta i srednjeg prsta. Mogu biti napravljene od srebra ili srebro-hlorida. Na slici 2 dole je prikazan *PsychLab* program koji ima odvojene prozore za potrebe istraživača i ispitanika.

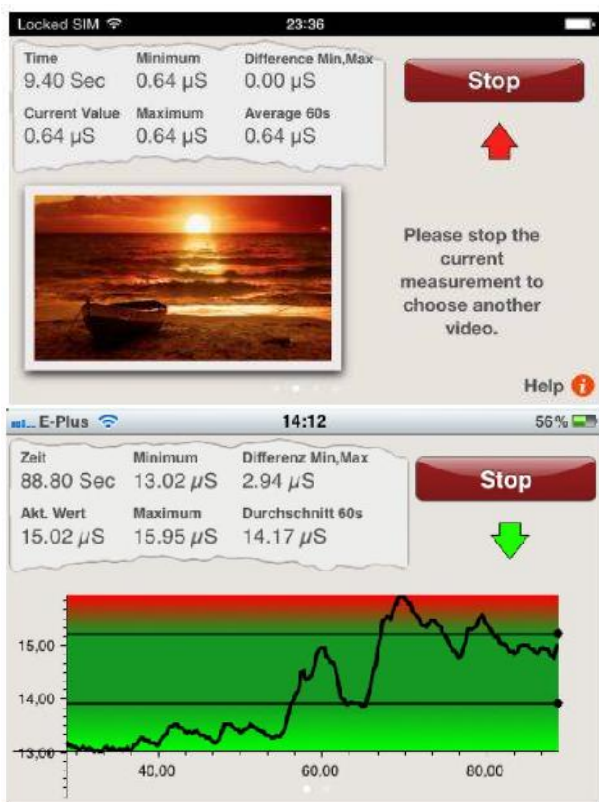


Slika 2. PsychLab oprema za merenje provodnosti kože korisnika kao odgovor na zvučne i električne stimuluse



## 2.2. MINDFIELD ESENSE SKIN RESPONSE

Ovaj GSR instrument je proizvod kompanije *Mindfield Biosystems* [8] koji meri provodnost kože ( $\mu\text{S}$ ) u realnom vremenu i koji šalje odbirke na svakih 10ms. Namenjen je korisnicima koji žele da treniraju mehanizam opuštanja zasnovan na principu biološke povratne sprege. *Mindfield* aplikacija ima mogućnost posmatranja provodnosti kože u realnom vremenu, kao i trening opuštanja. Prate se minimalna i maksimalna provodnost kože, razlika te dve vrednosti, srednja vrednost u poslednjem minutu i tekuća vrednost. Trening opuštanja uključuje vibracije uređaja, video i/ili muziku koji se pospešuju, odnosno suzbijaju u zavisnosti od nivoa uzbuđenosti, kao i stepen relaksiranosti. Ukoliko osoba smanjuje provodnost kože, efekti se pojačavaju. Video i muzika mogu proizvoljno da se biraju. Aplikacija je dostupna za Android i iOS platforme i prikazana je na slici 3 sa okruženjem za prikaz promene provodnosti kože prilikom emocionalne uzbuđenosti i okruženjem za trening koji sadrži različite simulacije koje reaguju na izmerene promene.



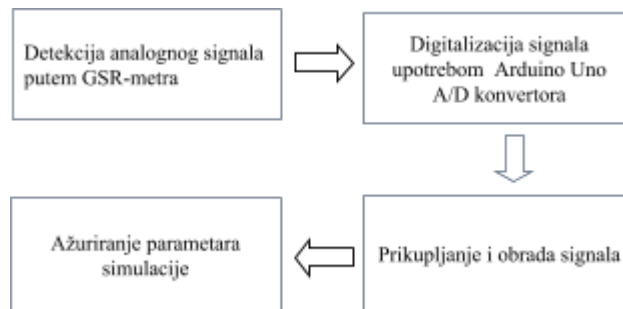
Slika 3. Merenje i prikaz provodnosti kože upotrebom Mindfield eSense Skin Response aplikacije

Elektrode *Mindfield* instrumenta se postavljaju na jagodicama prstiju i mogu da se menjaju. Merenja mogu da se obavljaju upotrebom suvih elektroda, dok elektrode sa gelom daju bolje očitavanje signala i mogućnost pozicioniranja i na druge delove tela, pa je tako recimo moguće i merenje rada srca. Uređaj se povezuje na mobilne telefone ili tablete preko ulaza za mikrofon.

## 3. REALIZACIJA I OPIS SOFTVERSKOG SISTEMA BAZIRANOG NA BIOFEEDBACK METODI

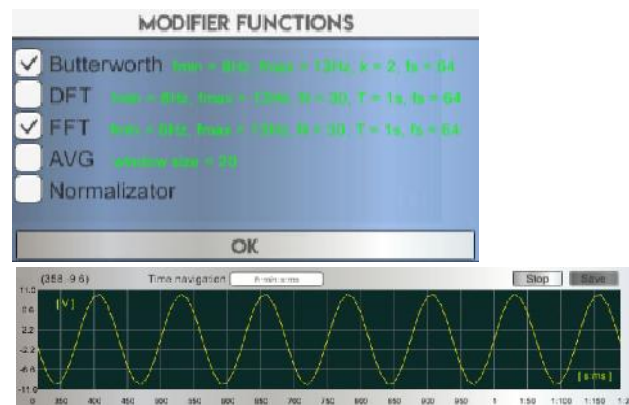
Realizovani sistem se sastoji od hardverskog i softverskog dela. Hardverski deo uključuje Arduino Uno A/D konvertor i GSR instrument za merenje provodnosti kože, dok softverski deo uključuje *biofeedback* aplikaciju. Za razvoj hardverskog dela korišćen je Arduino Web programator, dok je za razvoj softverskog sistema odabrana danas veoma popularna tehnologija Unity (verzije 2017.1.0f3). Arduino Uno je programiran u jednoj varijanti C jezika, dok su Unity skripte pisane u jeziku C#.

Na slici 4 je prikazan princip rada sistema. Analogni signal se detektuje putem GSR-metra, zatim se šalje A/D konvertoru gde se vrši digitalizacija i slanje računaru serijskom USB vezom. Računar sakuplja odbirke digitalizovanog signala, vrši zadatu obradu i koristi signal kao ulaz za ažuriranje parametara simulacije.



Slika 4. Princip rada realizovanog sistema

Softverski sistem poseduje dva okruženja - za analizu signala i za trening *biofeedback* metodom. Okruženje za analizu signala vrši prikupljanje, obradu i prikaz signala u vremenu, dok okruženje za trening sadrži skup različitih audio-vizuelnih simulacija koje pomažu korisniku da utiče na svoj stepen relaksacije.



Slika 5. Deo realizovanog sistema za prikupljanje, obradu i prikaz signala

Na slici 5 je prikazan deo okruženja za analizu signala. Grafički prikaz je interaktivan i omogućava korisniku mogućnost promene veličine prikaza i pomeranje po

vremenskoj osi. Više signala može istovremeno da se očitava, obrađuje i prikazuje sa različitih analognih ulaza A/D konvertora. Načini obrade i periode odabiranja mogu da se podešavaju za svaki od signala. Načini obrade uključuju Batervortov filtar, Furijeovu transformaciju, aritmetičku sredinu odbiraka u određenom vremenskom prozoru, kao i normalizator vrednosti. Omogućeno je i čuvanje odbiraka kako bi kasnije po potrebi mogla da se sprovede dodatna analiza izmerenog signala.

Okruženje za trening sadrži skup interaktivnih simulacija sa ugrađenim mehanizmom nagrade koje korisnika dodatno podstiču na trening. Korisnik može da se registruje, sačuva rezultat uspešnosti treninga i da prati svoju istoriju treniranja. Svojim biološkim signalom korisnik direktno utiče na promenljive parametre simulacije koji uključuju zvuk, brzinu kretanja, visinu pozicije i promenu vremenskih prilika.

Realizovane simulacije su Sneg, Pustinja, Ostrvo i Loptica. U svakoj od simulacija se korisnik kreće i sakuplja poene. Simulacija Sneg predstavlja zimski ambijent sa promenljivim parametrima: intenzitet snežnih padavina, oblačnost, brzina kretanja, visina pozicije, jačina vetra i jačina zvuka. Pustinja predstavlja monotoni ambijent sa promenljivim parametrima: oblačnost, brzina kretanja, visina pozicije i jačina zvuka. Ostrvo predstavlja letnji ambijent sa promenljivim parametrima: oblačnost, brzina kruženja oko ostrva, visina pozicije i jačina zvuka. Loptica predstavlja dinamični trening sa najmanjim brojem promenljivih parametara: brzina kotrljanja, oblačnost i jačina zvuka. Na slici 6 prikazana je simulacija Loptica.

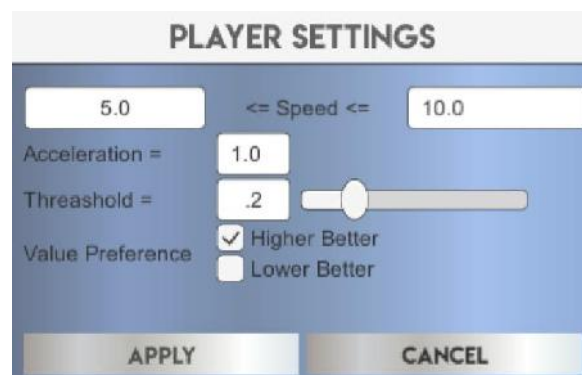


Slika 6. Interaktivna animacija u kojoj korisnik pokreće lopticu

Mereni signal može da se prikuplja i obrađuje na slične načine kao kod modula za analizu. Na slici 7 je prikazana kontrolna tabla putem koje je moguće postaviti fiksne parametre simulacije: opseg brzine, ubrzanje, težina simulacije, kao i način tumačenja signala.

Prilikom korišćenja sistema može da se javi problem u treningu ukoliko se javi šum velike amplitude. Tada normalizator signala pamti veštačku maksimalnu vrednost, koja je dosta veća od maksimalne provodnosti kože, čime se smanjuje kontrola korisnika nad simulacijom. Taj problem je lako uočljiv tokom treniranja

i u tom slučaju je potrebno ručno resetovati vrednosti normalizatora.



Slika 7. Kontrolna tabla za postavljanje parametara treninga

#### 4. INICIJALNO TESTIRANJE SISTEMA

Realizovani softverski sistem je inicijalno testiran od strane tri korisnika u cilj sticanja utiska o daljem mogućem pravcu razvoja novih simulacija koje bi imale najveći uticaj na stanja opuštenosti korisnika. Prilikom testiranja prikupljeni su parametri iz simulacija i zabeleženi subjektivni utisci. Prikupljeni parametri iz simulacija su: naziv simulacije, naziv korisnika, korišćeni obrađivači signala, težina simulacije, broj sakupljenih poena i celokupna uspešnost treninga koja se meri po formuli  $\frac{\text{poeni} \cdot 100}{\text{trajanjeSimulacije}}$ . Svaka simulacija je trajala 5 minuta. Prikaz sakupljenih parametara je dat u tabeli 1.

Tabela 1. Rezultati tri ispitanika za četiri simulacije merenjem provodnosti kože

simulacija	korisnik	obrađivači	težina	poeni	uspešnost
Pustinja	Korisnik1	Normalizator	0.5	7	2.33
Loptica	Korisnik1	Normalizator	0.5	61	20.33
Sneg	Korisnik 1	Normalizator	0.5	1	0.33
Ostrvo	Korisnik 1	Normalizator	0.5	5	1.67
Pustinja	Korisnik 2	Normalizator	0.5	6	2
Loptica	Korisnik 2	Normalizator	0.5	62	20.67
Sneg	Korisnik 2	Normalizator	0.5	8	2.67
Ostrvo	Korisnik 2	Normalizator	0.5	2	0.67
Pustinja	Korisnik 3	Normalizator	0.5	7	2.33
Loptica	Korisnik 3	Normalizator	0.5	56	18.67
Sneg	Korisnik 3	Normalizator	0.5	8	2.67
Ostrvo	Korisnik 3	Normalizator	0.5	0	0

Rezultati uspešnosti prikazani u tabeli su se u većini slučajeva poklopili sa subjektivnim doživljajem testiranih korisnika. Korisnik je osećao bolju kontrolu kod simulacija sa manjim brojem promenljivih parametara i sa većom dinamikom kretanja, što je direktno uticalo na stepen relaksacije. Korisnicima se najviše svidela simulacija Loptica, koja ima svega tri promenljiva parametra i koja je imala najdinamičnije kretanje i muziku. Po subjektivnoj oceni korisnika simulacija Sneg

je imala previše parametara, Pustinja je izazivala pospanost zbog monotonog ambijenta i zvuka u pozadini, dok je Ostrvo kod nekih izazivalo osećaj mučnine zbog konstantnog kruženja.

## 5. ZAKLJUČAK

U ovom radu predstavljen je realizovani sistem zasnovan na *biofeedback* konceptu. Realizovane su četiri različite simulacije i skup različitih obrađivača signala. Kao ulazni signal se koristila električna osobina ljudske kože kao direktni pokazatelj psihofizičkog stanja uzbuđenosti. Krajnji cilj realizovanih simulacija je da pruže zanimljiv i udoban audio-vizuelni doživljaj krajnjem korisniku koji želi da pospeši ulazak i trajanje stanja relaksacije.

Sproveden je inicijalni test nad korisnicima, koji je imao za cilj da pomogne u daljem razvoju sistema. Prilikom testiranja prikupljeni su parametri iz simulacija i zabeleženi su subjektivni utisci korisnika. Iskustva korisnika su pokazala da dinamične i jednostavne simulacije sa malim brojem parametara na koje se utiče povećavaju osećaj kontrole, što dalje utiče na stepen zadovoljstva i relaksacije.

Moguća poboljšanja postojećeg sistema uključuju dva pravca. Prvi pravac se odnosi na povećavanje broja senzora koji simultano mogu da mere različite biološke parametre (temperatura, frekvencija disanja, EKG, itd.) i dodavanje novih načina obrade signala. Drugi pravac se odnosi na dodavanje novih promenljivih parametara u simulacijama, kao i mogućnost da korisnik samostalno kreira scenu za trening po sopstvenoj potrebi. Nakon proširenja, planirano je da se sistem testira nad većim brojem korisnika za duži vremenski period i da se obavi analiza *biofeedback* uticaja na nivo relaksacije.

## ZAHVALNICA

Rad na ovom projektu je delimično bio finansiran od strane Ministarstva prosvete i nauke Republike Srbije (III44009, OS175016 i TR 32047). Autori zahvaljuju na finansijskoj podršci.

## LITERATURA

- [1] Critchley, H. D., "Brain activity during biofeedback relaxation: A functional neuroimaging investigation", *Brain*, 124.5: 1003-1012, 2001.
- [2] Denis, P., "Methodology of biofeedback", *European Journal of Gastroenterology & Hepatology*, 8(6):530-533, 1996.
- [3] Bersak, D., McDarby, G., Augenblick, N., McDarby, P., McDonnell, D., McDonald, B., & Karkun, R., "Intelligent Biofeedback using an Immersive Competitive Environment", *Designing Ubiquitous Computing Games Workshop at UbiComp 2001*, Atlanta, GA, USA, 1-6, 2001.
- [4] Lazarus, Richard S., Joseph C. Speisman, Arnold M. Mordkoff, "The relationship between autonomic indicators of psychological stress: Heart rate and skin conductance", *Psychosomatic Medicine*, 25(1), 19-30, 1963.
- [5] Boucsein W., "Electrodermal Activity", Springer Science & Business Media, 1-25, 2012.
- [6] Miljković N., "Merenje impedanse u kliničkom inženjerstvu", *Predavanja sa smera za Biomedicinsko inženjerstvo*, 9-15, 27-30, 2017.
- [7] Psychlab, Contact Precision Instruments, [Online]:[http://www.psychlab.com/hardware\\_skin\\_Conduct.html](http://www.psychlab.com/hardware_skin_Conduct.html), pristupano septembar 2017.
- [8] Mindfield Biosystems eSense Skin Response, [Online]:<https://www.mindfield.de/en/Biofeedback/Products/Mindfield%C2%AE-eSense-Skin-Response.html>, pristupano septembar 2017.

# PREGLED KORIŠĆENJA INTELIGENTNIH ŽELEZNIČKIH SISTEMA

## APPLICATION OVERVIEW OF THE INTELLIGENT RAILWAY SYSTEMS

Dr Dragica Jovanovic<sup>1</sup>, MSc Marko Bursac<sup>1</sup>, Dr Zoran Bundalo<sup>1</sup>  
*Visoka železnička škola strukovnih studija<sup>1</sup>*

**Sadržaj** – Upravljanje saobraćajem je veliki problem širom sveta. Moderni železnički saobraćajni sistemi moraju da ispune zahteve u vezi pouzdanosti i raspoloživosti. Takođe, visoki zahtevi za velikom bezbednošću i velikom brzinom železničkih mreža u 21. veku, određuju Inteligentne železničke sisteme (IRS) kao jedan od mogućih načina za ostvarenje toga.

IRS je integrisani sistem koji primenjuje širok spektar komunikacionih, kontrolnih, senzorskih i elektronskih tehnologija za rešavanje i upravljanje saobraćajnim problemima. IRS se koristi u razvijenim zemljama protekle dve decenije, ali je i dalje novi koncept kada se radi o zemljama u razvoju. Ovaj rad uvodi značajne koncepte Inteligentnih železničkih sistema, uključujući zašto su oni potrebni i kako se mogu razvijati i primenjivati u svetu. Različiti primeri upotrebe IRS su prezentovani i analizirani.

**Abstract** - Traffic management is a major problem around the world. Modern rail transport systems must meet the reliability and availability requirements. Also, the high demands for high security and high speed rail networks in the 21st century determine Intelligent Rail Systems (IRS) as one of the ways to achieve this.

The IRS is an integrated system that employs a wide range of communication, control, sensor and electronic technologies for solving and managing traffic problems. The IRS has been used in developed countries over the past two decades, but is still a new concept when it comes to developing countries. This paper introduces significant concepts of Intelligent Rail Systems, including why they are needed and how they can be developed and applied globally. Various examples of IRS use have been presented and analyzed.

### 1. UVOD

Inteligentni železnički sistemi (Intelligent Rail System - IRS) su nova generacija transportnih sistema razvijena integracijom telekomunikacionih, elektronskih, navigacionih, upravljačkih, automatičkih tehnologija, kao i tehnologija za donošenje odluka. Ove tehnologije omogućavaju optimalno korišćenje svih raspoloživih fiksnih i mobilnih resursa, vremena, prostora i ljudskih resursa u železnici, sa ciljem poboljšanja efikasnosti transporta, povećanja bezbednosti transporta kao i kvaliteta usluge, uz minimalni trošak. Tehnologije uključuju GIS (Geografski informacioni sistem), GPS (Globalni pozicioni sistem), GSM (uključujući GPRS) i ostale računarske tehnologije. Ove tehnologije će ultimativno

rezultirati u sledećem: povećanju efikasnosti, bezbednosti ili kvaliteta usluga.

IRS obuhvata: Menadžment saobraćajem i tranzitom, Saobraćajne signalne sisteme, Globalni Pozicioni Sistem, Informacioni Sistem o vremenu i drugom, Elektronsko plaćanje (Clearance) i Informisanje putnika u realnom vremenu. Najznačajniji aspekti IRS su:

- Poboljšanje produktivnosti kroz napredne tehnologije i upravljačke tehnike,
- Efikasniji rad postojećih programa,
- Integrisanje sistema i
- Obezbeđivanje putničkih informacija.

#### 1.1. Povezani radovi

Osnovni principi za upravljanje železničkim saobraćajem su dati u [1]. Ovo uključuje upotrebu blokiranja, upravljanje resursima i podelu železničkih mreža na različite delove. Novi trendovi kontrole železničkog saobraćaja i upravljanja datiraju još od 1997 [2]. Pojedinačno kašnjenje jednog voza može izazvati domino efekat kašnjenja na celoj železničkoj mreži, što predstavlja glavnu brigu planera i dispečera, pa je *algoritam za planiranje železničkog saobraćaja* opisan u [3].

Projekat [4], podržan od strane *Swedish National Rail Administration* and *Vinnova, Swedish Agency for Innovation Systems*, navodi funkcionalnosti automatskog sistema za izvršavanje i podršku, koji mora biti raspoloživ u železničkim sistemima upravljanja saobraćajem:

- automatsko izvršavanje kontinuiranog ažuriranja saobraćajnog plana,
- automatsko testiranje planiranih vozničkih trasa i
- automatsko blokiranje testiranih trasa voza u skladu sa planom i nalogima za signalizaciju.

Primer sistema za podršku dispečerstvu za korišćenje u železničkom operacionom upravljačkom sistemu, kao i korišćenje ekspertskog znanja i fazi pravila su dati u [5].

Sitemska arhitektura bazirana na korisnikovim zahtevima za planiranje, definisanje i integrisanje inteligentnih transportnih sistema, koja obezbeđuje logički okvir za kompleksan menadžment, upravljanje i servis prihvatanja podatka koji su podržani preko ITS, predstavljena je u [6]. Standardi za Inteligentne transportne sisteme i pravila bezbednosti su navedena u [7], [8].

## 2. INTILIGENTNI TRANSPORTNI SISTEMI (ITS)

ITS je integrisani sistem koji primenjuje širok spektar komunikacionih, kontrolnih, senzorskih i elektronskih tehnologija za pomoć u praćenju i upravljanju protokom saobraćaja, smanjenju zagušenja, pružanju optimalnih puteva putnicima, povećanju produktivnosti sistema i uštedi života, vremena i novca.

Tehnička nota Svetske banke pod nazivom "ITS za zemlje u razvoju" govori o stanju ITS-a u zemljama u razvoju i diskutuje o dugoročnim, društvenim prednostima koje ITS može pružiti i načinima na koje ITS može pružiti neposrednije koristi pojedincima pomažući da se površinski transport učini dostupnijim, pouzdanijim i efikasnijim. Navodi se da je ITS koristan na sledeći način:

- poboljšava mobilnost za ljudi i teret,
- veća kompatibilnost površinskog transporta sa okolinom,
- manje smrtnosti i povrede vezane za saobraćaj,
- bolje upravljanje sistemom transporta i
- omogućava bolje planirano, brže i jeftinije putovanje.

ITS pokriva i poboljšava gotovo sve aspekte transportnog inženjerstva. Prema [9], ITS je podeljen u četiri glavne grane bazirane na njihovoj implementaciji u različitim aspektima upravljanja transportom tj. Napredni putnički informacioni sistem (ATIS), Napredni sistem upravljanja saobraćajem (ATMS), Napredni sistem javnog prevoza (APTS) i Sistem za upravljanje vanrednim situacijama (EMS).

Napredni putnički informacioni sistem (ATIS) primenjuje širok spektar tehnologija, kao što su internet, telefoni, mobilni telefoni, televizija, radio itd. kako bi putnicima i vozačima pomogli u donošenju odluka u vezi sa optimalnim rutama i dostupnim načinima putovanja. ATIS obezbeđuje informacije za vozače kako na putu tako tako i pre putovanja. Dostupnost informacija pre odlaska povećava samouverenost vozača pri korišćenju autoputeva i omogućava putnicima da izaberu bolje tranzitne rute [10]. Singh i Kumar [16] su razvili napredni informacioni sistem za informisanje putnika u gradu Hiderabad, Indija, u ArcView GIS okruženju. U sistem su uključeni moduli sa mogućnošću GIS-a za najkraće putanje, najbliži objekti i autobuske linije. Zhang et al. [11] u svojoj studiji razvili su i testirali generički multimodalni model transportne mreže za ATIS aplikacije.

ATMS je jedna od najistaknutijih i korišćenih grana ITS-a. Prema [12] su uključili upotrebu tehnika veštačke inteligencije u upravljanju saobraćajem i dali multiagentnu arhitekturu za inteligentne sisteme upravljanja saobraćajem. Zhang i dr. [11] su proučavali efikasnost Pekingskog sistema inteligentnog upravljanja saobraćajem (ITMS) i pokazali da je ITS poboljšao ukupnu efikasnost transporta u Pekingu.

Na polju APTMS-a [13]: opisuje arhitekturu računarskog sistema koji prati ideju inteligentnog sistema zasnovanog na znanju za upravljanje javnim prevozom. Hatem i dr. [14] su predložili sistem koji integriše Radio Frekvenci Identification (RFID) u Vireless Sensor Network (VSN) za upravljanje javnim prevozom. Ganeshkumar i Ramesh [15]

su dizajnirali sistem upravljanja i informisanja za hitne reakcije (ERMIS) za grad Madurai, Tamil Nadu.

## 3. PRIMERI UPOTREBE INTELIGENTNIH ŽELEZNIČKIH SISTEMA

U ovom radu smo istražili široku primenu Inteligentnih železničkih sistema, analizirali njihov način implementacije, kao i prednosti koje oni donose. Naveli devet različitih načina korišćenja Inteligentnih železničkih sistema u praksi.

### 3.1. Evropski sistem za upravljanje železničkim saobraćajem

Danas su evropski vozovi opremljeni sa 6 različitim navigacionih sistema koji su ekstremno skupi i okupiraju veliki prostor u kabini. Prilikom prelaska granica, mora se menjati sistem koji se koristi što dovodi do dodatnog utroška vremena i novca. Stoga su evropske zemlje odlučile da sve nekompatibilne sigurnosne sisteme (trenutno ih ima 14) zamene jednim sistemom. Evropski sistem za upravljanje vozovima (European Train Control System – ETCS) je podeljen na različite funkcionalne i nivoe opremljenosti. Definicija nivoa zavisi od toga kako je deonica opremljena i načina na koji se prenosi informacija do voza. U osnovi, dozvola za kretanje i odgovarajuće informacije o deonici se prenose do voza i prikazuju se u kabini vozača.

Evropski železnički sistemi za upravljanje obuhvataju sledeće oblasti [17]:

1. Evropski sistem za upravljanje železničkim saobraćajem (European Railway Traffic Managements System (ERTMS)) - zajednički sistem za signalizaciju i komunikaciju,
2. Evropski sistem za upravljanje vozovima (European Train Control System (ETCS) )
3. GSM za železnicu (GSM for Railways (GSM-R))
4. GSM-R – ETCS interfejs (GSM-R – ETCS Interfaces)
5. Regionalni ERTMS (ERTMS-Regional (ERTMS-R))
6. Implementaciju evropskog sistema za upravljanje vozovima (Implementing the European Train Control System).

Evropske železnice sadrže najmanje šest tipova železničke elektrifikacije i oko 20 različitih železničkih upravljačko-komandnih sistema. Evropska komisija je definisala GSM za železnice (GSM for Railways, GSM-R) kao novi digitalni radio sistema za interni prenos glasa i prenos podataka, kao i evropskog upravljačkog sistema za vozove (European Train Control System - ETCS) kao novog upravljačko-komandnog sistema [17].

Kombinacija ETCS i GSM-R čini novi signalni i komunikacioni sistem, nazvan Evropski menadžment sistem za železnički saobraćaj (European Railway Traffic Management System - ERTMS), slika 2. ERTMS sistem obuhvata dva glavna funkcionalna aspekta:

- upravljanje i komandovanje vozom radi obezbeđenja operacija vozova u mreži i



- menadžment saobraćajem radi optimizovanja kapaciteta železnica koristeći napredni saobraćajni i infrastrukturni menadžment.

ERTMS je automatski sistem za zaštitu vozova (Automatic Train Protection system - ATP) koji kontinuirano nadzire kretanje vozova uz pružanje kabinske signalizacije. Kabinska signalizacija (cab signaling) obezbeđuje neophodne informacije osobama koje nadgledaju sigurnost voza. Više ATP sistema se trenutno koristi u Evropi [18].

### 3.1.1. Evropski sistem za upravljanje vozom

ETCS sistem za upravljanje i komandovanje vozom je specificiran od strane *International Union of Railways* (UIC) u kooperaciji sa železničkom signalnom industrijom i železničkim operatorima. ETCS nudi jedinstveni signalni sistem i otvara put za besprekorne prekogranične operacije (seamless cross-border operations) za vozove velikih brzina i konvencionalne vozove, kao i za teretne vozove. Ovaj sistem pravi vitalni doprinos efikasnosti železničkih mreža preko optimizacije bezbednosti i povećanja maksimalnog kapaciteta na železničkim linijama.

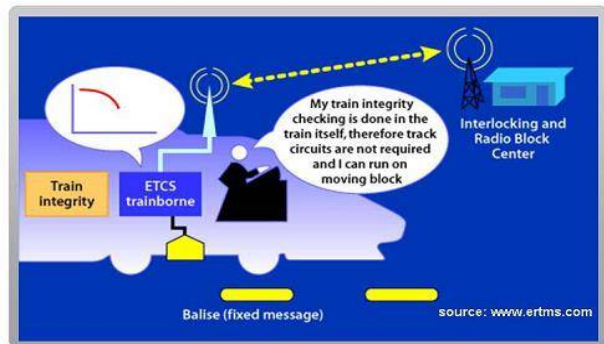


Slika 1. ERTMS[17]

Na slici 1 su prikazani gradivni blokovi Evropskog železničkog sistema za upravljanje koji uohvata sledeće blokove: Signalizaciju, Telekomunikacije, Upravljanje saobraćajem i Ostale savremene tehnološke blokove.

ETCS nivo3 je prikazan na slici 2. Na ovom nivou ETCS prevazilazi funkciju čiste zaštite voza sa implementacijom radio pozicioniranja. Kako se signal pozicije voza neprestano prenosi do radio centra, moguće je utvrditi koje tačke na deonici je voz bezbedno prešao, te se na taj način može narednom vozu dati dozvola za prelaz novih tačaka. Na taj način deonice se ne dele na fiksne sekcije na kojima se trenutno može nalaziti smo jedan voz, već računar lokomotive prati potrebnu dužinu zaustavnog puta voza u odnosu na voz ispred sebe.

U okviru ovog sistema upravljanje deonicama i skretnicama se obavlja centralizovano. Komande se prenose bežičnim putem, prati se položaj voza u svakom trenutku, prate se trenutna ograničenja brzina kako trajna tako i privremena. Takođe ovaj sistem ima mogućnost optimizacije energetskog bilansa, praćnja sporednih sistema, prijavljivanja trenutnih parametara u samoj lokomotivi i konačno daljinsko upravljanje lokomotivom iz dispečerskog centra.



Slika 2: ETCS Level 3 [17]

Svaki voz prijavljuje svoju poziciju kontrolnom centru bežičnim putem. Logički sistemi kontrolnog centra prikupljaju ove podatke, zatim ih obrađuju i kao povratnu informaciju vozovima šalju podatak o ograničenju brzine, vodeći pri tome računa o bezbednom razmaku između vozova. Računar u lokomotivi prati ograničenja brzine i poziciju i upoređuje ih sa trenutnim vrednostima i proračunava potencijalna i trenutna nebezbedna stanja. Ukoliko dođe do prekoračenja brzine prvo se upozorava mašinovođa, od koga se očekuje da preduzme određene akcije a ako one izostanu aktivira se sistem za prinudno zaustavljanje voza. Takođe računar prati vitalne sisteme u lokomotivi kao što su vučna snaga, kočnice i te informacije predaje kontrolnom centru.

### 3.1.2. GSM za železnice (GSM-R)

GSM-R obezbeđuje platformu za glasovnu i podatkovnu komunikaciju između operativnog osoblja železničkih kompanija, uključujući vozače, dispečere, članove timova, železničke inženjere, i kontrolore na stanicama. On isporučuje napredne mogućnosti, kao što su grupni pozivi, glasovni broadcast, konekcije bazirane na lokaciji i pozive (*call pre-emption*) u slučaju hitnosti.

GSM-R se bazira na javnom GSM-u. Arhitektonski okvir ponuđenih servisa od strane GSM-R mreže je:

- Standardne GSM opcije kao što su glas od tačke do tačke i Servis kratkih poruka (Short Messaging Service - SMS) između radija u kabini, ručnih radija unutar voza, signalizera, kontrolera, i ostalih radnika. Dodatno, ova platforma može takođe podržati suplemantarne servise kao što su poziv na čekanju, prosleđivanje poziva i drugo,
- Napredne opcije poziva (Advanced Call Speech Items - ASCI): Call Pre-emption, Voice Group Calling Service, Voice Broadcast Service,
- Specifične železničke opcije: Funkcionalno adresiranje, Pristupna matrica i Adresiranje bazirano na lokaciji.

ETCS koridori presecaju Evropu sa severa na jug is a istoka na zapad i to su, ETCS koridori velikih brzina:

- Madrid - Paris/Zurich/Milan,
- Paris - Luxembourg/Mannheim/Zurich,
- Paris - London/Brussels - Amsterdam/Cologne,
- Zurich/Geneva/Munich - Naples.

ETCS konvencionalni koridori:

- Rotterdam - Milan/Genova,
- Antwerp - Basle,
- Hamburg - Malmö,

- Berlin - Bukarest/Constanta,
- Milan - Budapest,
- Munich/ Budapest - Belgrade,
- Bar/Thessaloniki - Istanbul.

### 3.2. ILTIS – Železničko upravljanje saobraćajem

ILTIS je centralizovani sistem za upravljanje saobraćajem razvijen inicijalno za švajcarsku nacionalnu železnicu (Swiss National Railways) [19]. Proteklih godina su zahtevi za automatizacijom rasli širom sveta. ILTIS upravljački i informacioni sistem omogućava efikasan automatski operacioni menadžment za glavne linije, kao i za privatne železnice. On pokriva celokupno operaciono polje železničkog upravljanja, od lokalnog i remote upravljanja do upravljanja individualnim blokiranjem, kao i automatizacije cele železničke mreže. ILTIS obezbeđuje upravljanje sigurnosno – kritičnim operacijama blokiranja. ILTIS ispunjava sledeće uslove u vezi železničkih zahteva:

- ILTIS mora biti u funkciji 24 sata dnevno, 7 dana u nedelji. Nisu dozvoljeni ni kratki prekidi servisa.
- Kvalitet i raspoloživost su takođe preduslovi za bilo koji švajcarski CTC.
- ILTIS sistem sadrži preko 4 miliona linija koda, i zahteva se njegovo lako održavanje.

### 3.3. Pregled automatskog nadzora za SPICA-železnički program

Upravljanje železničkim saobraćajem predstavlja ultimativnu soluciju za rešavanje potencijalno opasnih situacija [20]. Studije i eksperimenti o ponašanju operatera su sprovedene na University of Technology of Compiègne (UTC) korišćenjem platforme za nadzor “SPICA-Rail” bazirane na Alstom-ovom proizvodu ICONIS™. Ovaj proizvod je generisan za nadzor železnica baziran na Sistemima za upravljanje i prikupljanje podataka (Supervisory Control and Data Acquisition - SCADA). Ova oprema uključuje “*simulator okruženja*” omogućavajući eksperimentalnu platformu za testiranje “*as if*” opcija koje se realno mogu desiti u železničkoj mreži.

SPICA-Rail može simulirati upravljanje i nadzor celokupne mreže, integrišući funkcije upravljanja saobraćajem kao i nadzor signalizacije, definisanje ruta, praćenje vozova i menadžment reda vožnje. Osnovni interes predstavlja mogućnost za laboratorijsko kreiranje scenarija nesreća i konfrontiranja operatera sa ovim situacijama, sa ciljem analiziranja njihovog ponašanja i odluka.

### 3.4. Saobraćajni kontrolni centar i informacioni sistem savremene železničke mreže u Pekingu

Singapurska kompanija Technologies Electronics Limited, u partnerstvu sa kompanijom Tsing Hua Tong Fang, sklopila je ugovor u 2006-oj, o isporučivanju Integriranog Informacionog Sistema (IIS) za Saobraćajni Kontrolni Centar (TCC) [21], koji upravlja urbanom železničkom mrežom u Pekingu. Sistem je dizajniran da koordinira železničkim saobraćajnim sistemom glatko i efikasno, omogućavajući da putnici stignu na svoje destinacije, bezbedno i na vreme.

IIS obezbeđuje centralizovan i lokalizovan nadzor električnih i mehaničkih podistema različitih železničkih pruga. Podsystemi uključuju: napajanje energijom, kontrolu životne sredine, automatizaciju objekata, signalizaciju, video nadzor, prikaz informacija o putnicima, automatizovane prolazne kapije, glavni sat, požarne alarme itd.

IIS obuhvata i mnoge druge podsysteme kao što su: Integrirani nadzorni sistem (ISS), Operativni sistem za informisanje putnika (OPIS), Dispečerski poslovni informacioni sistem (BIDS), Sistem nadzora video kamerama (CCTV), Podrška sistema za baze podataka (DSSDB) Linijska procena opreme sistema (LEAS), Održavanje sistema za upravljanje (MMS) itd.

Funkcije glavnog sistema su:

1. Nadzor nad kombinacijom sledećih sistema
  - Sistem napajanja, Sistem protivpožarne zaštite,
  - Sistem kontrole životne sredine,
  - Sistem signalizacije, Sistem kontrole troškova,
  - Sistem za informisanje putnika,
  - Sistem naplate usluga i
  - Obračunski centar (*Account Clearing Centre*).
2. Sistem upravljanja i kontrole operativnih informacija (OIS), Dispečerski poslovni informacioni sistem (BIDS).
3. Praćenje i kontrola CCTV podistema.
4. Deljenje informacija i koordinacija za normalno funkcionisanje železnice, i revizija linijske opreme.
5. Deljenje podataka i informacija za komandu i kontrolu Pekingškog železničkog saobraćaja tokom vanrednih situacija.

Komponente IIS sistema su:

- Integrirani informacioni sistem (IIS), Glavni kompjuterski sistem lociran je u XiaoYing-u.
- IIS Centar za razvoj i testiranje, lociran u XiaoYing-u.
- CCTV sistem, takođe lociran u XiaoYing-u.
- Lokalana komunikacija velike brzine i upravljanje mrežom locirane u XiaoYing-u.
- IIS (Backup) Kompjuterski sistem i komunikaciona mreža, locirani u XiZhiMen-u.

### 3.5. Inteligentni železnički transportni sistemi Indije

Indijske železnice su druge najveće železničke mreže na svetu. Redosled putničkih i teretnih vozova, praćenje i sprovođenje sigurnosnih standarda sigurno predstavlja veliki izazov. Više od 14 miliona putnika i preko milion tona tereta se transportuje svaki dan.

U radu [22] istražuju se tehnologije koje mogu poslužiti za poboljšanje putničkih i teretnih železničkih usluga. Takve tehnologije uključuju Geografske informacione sisteme, Sistem za globalno pozicioniranje, GPRS, RFID itd. Pomenuta studija obuhvata tehnologije i potrebne promene, čiji je cilj povećanje efikasnosti, kvaliteta usluga i bezbednosti, kako je navedeno:

1. Povećanje efikasnosti
  - Inteligentni teretni operativni sistemi
  - Inteligentni sistemi za upravljanje vozilima
2. Povećanje kvaliteta usluga
  - Inteligentni E-biznis sistemi

- Inteligentni korisnički informacijski sistemi
3. Povećanje sigurnosti
- Sigurnosni i Kontrolni Inteligentni sistemi.

### 3.6. Sprečavanje nezgoda koristeći inteligentni sistem kontrole za železnički saobraćaj

Ljudski faktor igra značajnu ulogu u kontroli železničkih sistema. U poslednje tri godine dogodilo se nekoliko nezgoda sa smrtnim ishodom u Letoniji. Glavni razlog je nepažnja vozača i prolazak kroz crveno svetlo, a glavni zadatak je smanjiti takve nezgode izazvane ljudskim faktorom. Metoda za sprečavanje takvih nezgoda objašnjena je u radu [23]. Kontroler veštačkih neuronskih mreža zadužen je za kontrolu kretanja vozila u voznom parku, kao i za izračunavanje vremena koje je potrebno za bezbedno zauzastavljanje vozila pre kritične tačke. Rezultati ovakvog eksperimenta pokazuju mogućnost korišćenja neuronske mreže za kontrolu brzine vozila u zavisnosti od distance za zaustavljanje. Rezultati pokazuju da je pomoću inteligentnih dijagnostičkih sistema i uređaja za koordinaciju moguće sprečiti nezgode i izbeći različite probleme. Neuronske mreže se mogu koristiti za sprečavanje havarija i nezgoda i kao takvu vrstu kontrolera neophodno je integrisati u radnu infrastrukturu za optimalnu kontrolu brzine železničkog saobraćaja. Postoje tri nivo sigurnosti u transportnim sistemima. Prvi je bezbednost sistema **mehatronike** voza. Što znači da je potrebno odvojiti inteligentni dijagnostički sistem senzora za vanredne i kritične situacije. **Drugi nivo je bezbednost mehatroničkog sistema voznog parka.** Jedan od primarnih zadataka je inteligentna kontrola brzine vozova, koristeći multi-kriterijume donošenja odluka, uzimajući u obzir matematičke modele voznih parkova i algoritme za sprečavanje nezgoda.

### 3.7. Distribuirani raspored u realnom vremenu za Železnički saobraćaj

Povećanje efikasnosti i fleksibilnosti u železničkom saobraćaju zahteva uvođenje novih metoda u realnom vremenu. Distribuirani metod za raspored vozova je prikazan u radu [24]. Vozovi imaju svoja vremenska ograničenja za susret, unapred utvrđene rute sa stanicama i potrebnim vremenom dolaska. Rute sadrže blok sekcije, od jedne stanice do druge, dinamički raspoređene, tako da ne može doći do zastoja. Red vožnje baziran je na: Inteligentnim kontrolerima kolovoza [25], Heurističkoj metodi, kao što su genetski algoritmi [26], Interaktivnom rasporedu [22], Korišćenjem GPS-a i bežične komunikacije između motora u vozu i kontrolnog centra [23].

### 3.8. Železnički sistem kontrole signala optičkim LAN-om i pojednostavljenim dizajnom

Poboljšanje železničkog sistema promenom kontrolne logike i spoljnih signalnih uređaja rezultuje boljim uslugama koje zadovoljavaju potrebe korisnika, povećanju saobraćajnih kapaciteta i proširenje direktnih operacija preko više linija. Železnički sistem za kontrolu signala optičkim LAN-om i njegov razvoj je predstavljen u radu [24]. Takođe, u radu [24] predstavljen je sistem koji opisuje mreže prenosa, bezbednosne komunikacije i softversku konfiguraciju sistema. Zamena železničkih sigurnosnih

uređaja zahteva i veliki broj signalnih kablova i instalacija, kao i redizajniranje kontrolne jedinice. Kompanija East Japan Railway, rešila je ovaj problem izradom novog sistema kontrole signala baziranom na IP-mreži.

### 3.9. Tehnika detekcije bezbednosnih incidenata za višestepene Inteligentne Upravljačke Sisteme u železničkom transportu u Rusiji

Sistemi za kontrolu bezbednosti i upravljanje incidentima postali su glavni fokus istraživanja u oblasti inteligentnih upravljačkih sistema železnice. Intenzivan razvoj ITS-a dovodi do neophodnosti značajnih napora da se obezbedi potreban nivo integrisane sigurnosti objekata koji su kritični za misiju na železnici. ITS ima intenzivnu mrežnu razmenu u smislu "velikih podataka", pa su sistemi analize i predviđanja saobraćaja tema naučnih istraživanja [25], kao i razvoja proizvoda [26]. Jedna komponenta ITS-a je *sigurnosno praćenje i upravljanje sigurnosnim informacijama i događajima (SIEM)* [27].

U [28] se razmatra sistemski arhitektura multilevel inteligentnog sistema kontrole u ruskom železničkom transportu i detaljno je objašnjen problem i zadatak sistema obrzbrđnja sigurnosti informacija i upravljanja događajima, kao važnim delom inteligentnog kontrolnog sistema na više nivoa. Glavni rezultat se sastoji u razvoju jednostavnih i brzih sigurnosnih detekcija na osnovu teorije *grubih skupova*. Spomenuta infrastruktura ruske železničke omogućava izvođenje razvoja i postavljanja inteligentnih upravljačkih sistema na više nivoa (MICS) unutar ITS-a. U skladu sa međunarodnim standardom (ISA-95) za razvoj automatizovanog interfejsa između preduzeća i upravljačkih sistema, hijerarhija automatizovanih kontrolnih sistema industrijskog preduzeća podeljena je na četiri nivoa, formirajući funkcionalnu piramidu:

- Poslovna inteligencija (BI)
- Planiranje resursa preduzeća (ERP)
- Proizvodni sistem izvršenja (MES)
- Nadzorna kontrola i prikupljanje podataka SCADA).

Osim toga, [28] pokazuje da je moguće razlikovati zlonamerne aktivnosti unutar SIEM-a posmatrajući deo *nenormalne* sekvencije. Takođe, predložena tehnika će biti korisna za rad SIEM-a u online modusima.

## 4. ZAKLJUČAK

Inteligentni železnički sistemi omogućuju napredovanje na polju bezbednosti transporta i mobilnosti, povećavaju produktivnost kroz upotrebu naprednih komunikacionih tehnologija i integraciju u saobraćajnu infrastrukturu. Sistemi su bezbedniji, efikasniji i pouzdaniji. Ovi sistemi obuhvataju širok spektar bežične i žične komunikacije zasnovane na informatičkoj i elektronskoj tehnologiji. Inteligentni železnički sistemi obuhvataju razne tehnologije kao što su: Informatika, Komunikacije, Telekomunikacije, Elektronska trgovina itd. Na osnovu izloženog, zaključujemo da primena IRS-a doprinosi: 1) Povećanju efikasnosti železničkih usluga, 2) Upravljanju železnicom, 3) Nadgledanju saobraćajne kontrole uključujući cirkulaciju i regulaciju saobraćaja, 4) Kontrolu rasporeda u realnom

vremenu, 5) Smanjenju troškova u železničkom saobraćaju, 6) Povećanju protoka saobraćaja, 7) Sistemima bezbednosti, 8) Smanjenju negativnih efekata rasporeda vožnje, 9) Održavanju pruga.

Glavna prednost korišćenja inteligentnih upravljačkih sistema je mogućnost koordiniranja akcija svih učesnika u transportnom železničkom sistemu i realizovanje multi-kriterijumskog donošenja odluka u upravljanju, dijagnostici i raspoređivanju (scheduling) elektrificiranog transporta. Inteligentni uređaji su kontroleri, koji imaju interfejs da rade u globalnim mrežama kao i bežičnim mrežama, i programirani su da koriste metode veštačke inteligencije. Inteligentni uređaji imaju mogućnost da saraduju jedan sa drugim i da koordiniraju njihov rad radi donošenja boljih odluka.

## LITERATURA

- [1] Pacht J., "Railway Operation and Control," VTD Rail Publishing, Mountlake Terrace WA 98043 USA, 2004.
- [2] Shoji S., Igarashi A., "New trends of train control and management systems with real-time and non-real-time properties," Proceedings of the 3rd International Symposium on Autonomous Decentralized Systems (ISADS'97), 1997, pp. 319–326.
- [3] Goverde R. M. P., "A delay propagation algorithm for large-scale scheduled rail traffic," Preprints of 11th IFAC Symposium on Control in Transportation Systems, Delft, Netherlands, 2006, pp. 169–175.
- [4] Kauppi A., Wikström J., Hellström P., "Future train traffic control, control by re-planning," [www.it.uu.se/research/hci](http://www.it.uu.se/research/hci)
- [5] Fay A., "A fuzzy knowledge-based system for railway traffic control," Engineering Applications of Artificial Intelligence, 2000., pp. 719-729
- [6] Jarasuniene A., "Estimation of Importance of Intelligent Transportation Systems (ITS) Architecture", The 8 International Conference "RELIABILITY and STATISTICS in TRANSPORTATION and COMMUNICATION - 2008"
- [7] Williams B., "Intelligent Transport Systems Standards", ARTECH HOUSE, 2008., INC., ISBN-13: 978-1-59693-291-3
- [8] European Transport Safety Council, "Intelligent Transportation Systems and Road safety", ISBN: 90-76024-05-7
- [9] Bhupendra Singh, Ankit Gupta, "Recent trends in intelligent transportation systems: a review", Journal of Transport Literature, 9(2), 30-34, Apr. 2015.
- [10] Campbell, J. L., Carney, C., & Kantowitz, B. H. (2003). Human Factors Design Guidelines for Advanced Traveler Information Systems (ATIS) and Commercial Vehicle Operation (CVO). Federal Highway Admin., McLean, VA, Rep. FHWA-RD-98-057-2.
- [11] Zhang, J., Liaoa, F., Arentzea, T., & Timmermansaa H. (2011). A Multimodal Transport Network Model for Advanced Traveler Information Systems. Procedia Computer Science, 912-919.
- [12] Hernandez, J.Z., Ossowski, S., & Garcya-Serrano A. (2002). Multiagent Architectures for Intelligent Traffic Management Systems, Transportation Research Part C, 10, 473–506. ITS for Developing Countries
- [13] Molina, M. (2005). An Intelligent Assistant for Public Transport Management. Proc. International Conference on Intelligent Computing (ICIC 2005), Part II, LNCS 3645, 199-208.
- [14] Hatem, B. A., & Habib, H. (2009). Bus Management System Using RFID In WSN in the proceedings of European and Mediterranean Conference on Information Systems (EMCIS), April 12-13 2009, Abu Dhabi, UAE.
- [15] Ganeshkumar, B., & Ramesh, D., (2010). Emergency Response Management and Information System (ERMIS) – A GIS Based Software to Resolve the Emergency Recovery Challenges in Madurai City, Tamil Nadu. Int. Journal of Geomatics and Geosciences, 1(1), 1-13. Growth Resuming, Dangers Remain, (2012). World Economic Outlook, Report of International Monetary Fund (IMF), United Nations, Washington, DC, USA.
- [16] Singh, V. & Kumar, P. (2011). Web-Based Advanced Traveler Information System for Developing Countries. Journal of Transportation Engineering, 136(9), 836-845.
- [17] ERTMS White Paper, "European Railway Traffic Management System", GSM-R Core Marketing, Document Date: August 2005, Document Version:2.5, [www.ertms.com](http://www.ertms.com)
- [18] Bueno M. Á., "A Standardized System for Railway Traffic Control", INECO, 23th October 2009, [www.era.europa.eu](http://www.era.europa.eu)
- [19] Aonix Case Study, "ILTIS - Railway Traffic Control, Siemens Switzerland Transportation Systems", [www.aonix.co.uk](http://www.aonix.co.uk)
- [20] Belmonte F., Boulanger J-L., Schön W., Berkani K., Heudiasyc, "Automatic Supervision Survey for SPICA-RAIL Program", Université de Technologie de Compiègne, France
- [21] Singapore Technologies Electronics Limited, "Traffic Control Centre (TCC) Integrated Information System for Beijing Urban Raikway Network", Regn. No.: 196900084E, SINGAPORE, [www.stee.stengg.com](http://www.stee.stengg.com),
- [22] IIM – IDEA Telecom Centre of Excellence, "India - Intelligent Rail Transport Systems", Suresh K. 28-Dec-08
- [23] Gorobet M., Ribickis L., Balckars P., Greivulis J., Levchenkov A., "Method of Accident Prevention Using Intelligent Control System for Railway Transport", Proceedings of the 6 International Scientific Conference TRANSBALTICA 2009
- [24] Letia T., Hulea M., Miron R., "Distributed Scheduling for Real-Time Railway Traffic Control", Proceedings of the International Multiconference on Computer Science and Information Technology pp. 679–685, ISBN 978-83-60810-14-9 ISSN 1896-7094
- [25] Tao T., "A train control system for low-density lines based on intelligent autonomous decentralized system (IADS)," Proceedings of the Sixth International Symposium on Autonomous Decentralized Systems, 2003.
- [26] Higgins A., Kozan E., "Heuristics techniques for single line train scheduling," Journal of Heuristics, 3, Kluwer Academic Publishers, 1997, pp. 43–62.
- [27] Lova A., Tormas P., Barber F., Ingolotti L., Salido M. A., Abril M., "Intelligent train scheduling on high-loaded railway network," Algorithmic Methods for Railway Optimization, Springer, Berlin, 2007.
- [28] Zimmermann A., Hommel G., "A train control system case study in model-based real-time system design," Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'03), Nice, France, 2003, p118b.
- [29] Kunifuji T., Nishiyama J., Sugahara H., Okada T, Fukuta Y., Matsumoto M., Railway Signal Control System by Optical LAN and Design Simplification, JOURNAL OF NETWORKS, VOL. 3, NO. 7, JULY 2008
- [30] Yisheng Lv; Yanjie Duan; Wenwen Kang; Zhengxi Li; Fei-Yue Wang, "Traffic Flow Prediction With Big Data: A Deep Learning Approach," in Intelligent Transportation Systems, IEEE Transactions on , vol.16, no.2, pp.865-873, April 2015.
- [31] Omar Santos, Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security. 1nd ed. Indianapolis, IN: Cisco Press, 2015.
- [32] Miller, D.; Harris, S.; Harper, A.; VanDyke, S.; Blask, C. Security Information and Event Management (SIEM) Implementation; McGraw-Hill Companies: Columbus, OH, USA, 2011.
- [33] Andrey V. Chernov, Maria A. Butakova, Ekaterina V. Karpenko, "Security Incident Detection Technique for Multilevel Intelligent Control Systems on Railway Transport in Russia", TELFOR 2015, Beograd

# SOFTVERSKA INTEGRACIJA CFP MODULA U NMS SISTEM SUNCE-O ZA OTN/DWDM PLATFORMU OTP100G IRITEL

## SOFTWARE INTEGRATION OF CFP MODULES IN NMS SUNCE-O FOR OTN / DWDM PLATFORM OTP100G IRITEL

Marko Radivojević<sup>1</sup>, Petar Knežević<sup>1</sup>, Branislav Tomić<sup>1</sup>, Mihailo Stanić<sup>1</sup>, Dejan Drajić<sup>1,2</sup>

*IRITEL a.d. Beograd<sup>1</sup>*  
*Elektrotehnički fakultet, Beograd<sup>2</sup>*

**Sadržaj** – U ovom radu je opisana softverska integracija CFP optičkog primopredajnika u postojeći NMS sistem SUNCE-O koji služi za upravljanje OTN/DWDM platformom OTP100G IRITEL. Prikazano rešenje je bazirano na modifikaciji postojećeg SNMP agenta (podagenta) koji se izvršava na svakom uređaju OTP100G, modifikaciji SNMP menadžera koji se izvršava na serveru kao i proširenju baze upravljačkih informacija (MIB) tako da se omoguće sve funkcije koje su neophodne za rad CFP modula. Takođe su prikazane grafičke forme korisničkog interfejsa za pristup realizovanim funkcionalnostima.

**Abstract** - This paper describes the software integration of the CFP optical transceivers into the existing SUNCE-O NMS system, which is used to manage OTN / DWDM platform OTP100G IRITEL. The presented solution is based on the modification of the existing SNMP agent (subagent) that is executed on each OTP100G device, the modification of the SNMP manager executed on the server, and the extension of the MIB information base, so that all the functions necessary for the operation of the CFP module are enabled. Graphical user interface forms for access to implemented functionalities are also presented.

### 1. UVOD

OTP100G je multifunkcionalna optička transportna platforma visokih performansi i velike skalabilnosti [1]. Pogodna je za primenu u lokalnim, metro, regionalnim i magistralnim mrežama za povezivanje različitih telekomunikacionih centara i mreža preko optičkih kablova (vlakana). Brzina prenosa (protok) OTN (*Optical Transport Network*) signala u okviru mreže OTP100G IRITEL je 100Gbit/s što u kombinaciji sa DWDM (*Dense Wavelength Division Multiplexing*) multipleksiranjem 80 kanala, omogućuje protok od 8 Tbit/s po paru optičkih vlakana. Pomoću NMS (*Network Management System*) sistema SUNCE-O upravlja se uređajima (mrežnim elementima) čiji broj može da varira od nekoliko uređaja, do nekoliko desetina, stotina ili čak nekoliko hiljada u istoj mreži.

Kao optički primopredajnici za protok 100 Gbit/s se koriste CFP (*C form-factor pluggable*) izmenljivi moduli u kojima su realizovane složene funkcije analognog koherentnog optičkog primopredajnika i digitalne kompenzacije disperzije optičkog signala.

Softverska integracija CFP modula u postojeći NMS sistem SUNCE-O zahtevala je modifikaciju SNMP (*Simple Network Management Protocol*) agenta (podagenta) koji se izvršava na svakom uređaju OTP100G, modifikaciju SNMP menadžera koji se izvršava na serveru kao i proširenje baze upravljačkih informacija (MIB – *Management Information Base*) tako da se omogući rad svih funkcija koje spadaju u kategoriju konfigurisanje, alarmiranje i performanse.

U drugom poglavlju ovog rada dat je kratak opis NMS sistema za upravljanje SUNCE-O, u trećem poglavlju je je opisan princip komunikacije upravljačkog agenta na uređaju i NMS sistema za upravljanje koji se izvršava na serveru. Opis implementacije rešenja integracije CFP modula u postojeći NMS sistem je prikazan u četvrtom poglavlju. Posle zaključka i zahvalnice dat je spisak korišćene literature.

### 2. OPIS NMS SISTEMA SUNCE-O

Softverski sistem SUNCE-O namenjen je upravljanju pojedinačnim uređajima OTP10G i OTP100G Iritel (*EMS – Element Management software*) kao i upravljanju celokupnom mrežom koju čine uređaji OTP10G i OTP100G Iritel (*NMS – Network Management software*) (Slika 1) [2].

Sistem se koristi u eksploataciji i održavanju, tako što omogućava praćenje ispravnosti rada pojedinačnih uređaja, mreže, kvaliteta i pouzdanosti realizovanih servisa i promenu načina korišćenja kapaciteta mreže. Može se koristiti i za poslove planiranja mreže na osnovu podataka o slobodnim transportnim kapacitetima. Podaci u sistemu prikazuju se kroz odgovarajuće menije, prozore i izveštaje.

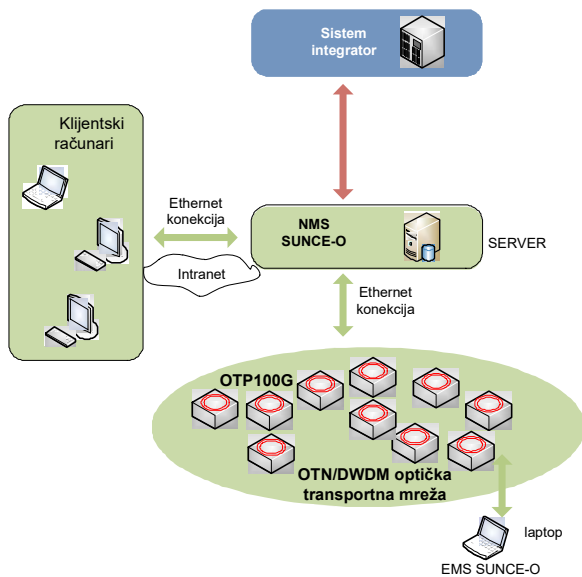
Softverski sistem SUNCE-O omogućava upravljanje OTN/DWDM transportnom mrežom: upravljanje greškama (alarmiranje), konfiguracijom, performansama i sigurnošću.

Sistem je dizajniran u klijent-server arhitekturi. Serverske komponente sistema isporučuju se preinstalirane na računaru za obradu, uz mogućnost istovremenog rada glavnog i rezervnog računara sa serverskim komponentama.

Nadgledanje i upravljanje grupom uređaja u mreži vrši se slanjem SNMP poruka sa jednog ili više administrativnih računara koji se nazivaju menadžeri [3]. Osnovne



komponente mreže upravljane SNMP protokolom su upravljani uređaj, softver koji se izvršava na upravljanoj uređaju odnosno agent i softver koji se izvršava na menadžeru odnosno NMS (*Network management station*). Činjenica da *SNMP* koristi samo proste tipove podataka da predstavi objekte upravljanja nije pogodna za opis složenih sistema sa mnogo parametara ali način formiranja identifikatora *SNMP* objekata ima osobine koje omogućavaju grupisanje objekata u tabele. Pojam tabele poznat je samo menadžeru dok agent prepoznaje samo pojedinačne objekte.



Slika 1. Upravljanje platformom OTP100G IRITEL pomoću NMS sistema Sunce-O

### 3. KOMUNIKACIJA UPRAVLJAČKOG AGENTA I NMS SISTEMA ZA UPRAVLJANJE

Komunikacija upravljačkog agenta na uređaju i sistema za upravljanje se odvija razmenom *SNMP* poruka tako što sistem za upravljanje šalje menadžeru zahtev za čitanje (*snmpget* ili *snmptable*) ili za podešavanje (*snmpset*) određenog objekta upravljanja. Menadžer dalje prosleđuje zahtev agentu koji je prijavio obradu tog objekta upravljanja. Agent dobija informacije o tome da li se radi o čitanju ili podešavanju, da li se očitava tabela ili pojedinačan objekat upravljanja, kao i *OID* (*object identifier*) tog objekta upravljanja. Ukoliko se radi o tabeli agent treba da prosleđuje menadžeru jedan po jedan pojedinačan objekat upravljanja iz te tabele. Sistem za upravljanje dobija kao odgovor informaciju o tome da li je zahtev prihvaćen i traženu vrednost ako jeste.

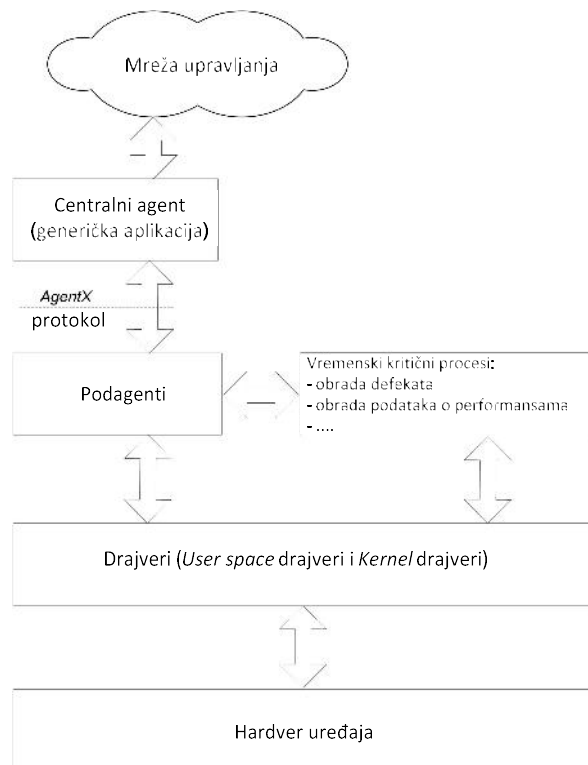
*MIB* (*Management Information Base*) ili baza upravljačkih informacija je baza podataka koja se koristi za upravljanje svim objektima od interesa u mreži. Svi objekti u mreži kojima se može upravljati su organizovani u strukturu stabla a ime objekta se formira na osnovu

putanje kroz stablo, od korena do objekta. Ime objekta na osnovu putanje kroz stablo naziva se *OID*.

### 4. OPIS IMPLEMENTACIJE

*Net-SNMP* je besplatni softverski paket koji obuhvata implementaciju sve tri verzije *SNMP* protokola. Koristi se za implementaciju *SNMP* agenta (*snmpd*) i predviđen je za izvršavanje na *UNIX* operativnim sistemima, ali može se koristiti i na *Microsoft Windows*-u, podržava i *IPv4* i *IPv6* verzije internet protokola. Pored implementacije agenta *Net-SNMP* pruža mogućnost i menadžerskih operacija koje očitavaju ili menjaju vrednosti parametara upravljanog uređaja. Očitavanje se može obaviti ili pojedinačnim zahtevima *snmpget*, *snmpgetnext* ili višestrukim zahtevima *snmpwalk*, *snmptable*, *snmpdelta*, a konfigurisanje *snmpset* zahtevom. Implementira pozadinski proces koji prima *SNMP* notifikacije (*snmptrapd*) koje mogu biti zabeležene, poslate drugom *SNMP* sistemu upravljanja ili nekoj drugoj aplikaciji.

U implementaciju agenta spadaju i biblioteke sa *C* i *Perl* *API*-jima koje omogućavaju proširivanje agenta na centralnog i jednog ili više podagenata korišćenjem *AgentX* protokola. Centralni agent obavlja funkcionalnosti samog *SNMP* protokola a podagent deo koji je specifičan za konkretan uređaj. Na slici 2. je prikazana blok šema komunikacije centralnog agenta i podagenta i veze agenta sa ostalim blokovima u uređaju OTP100G [5].



Slika 2. Komunikacija centralnog agenta i podagenta u uređaju OTP100G IRITEL

Na ovaj način, omogućena je integracija CFP modula u postojeći NMS sistem modifikacijom samo podagenta.

Modifikacijom su obuhvaćeni:

- Konfigurisanje CFP modula: uključivanje/isključivanje, podešavanje predajne snage i podešavanje talasne dužine rada optičkog predajnika;
- Upravljanje performansama koje se obavlja čitanjem brojača performansi CFP modula, merenim na intervalu od 24 časa i intervalu od 15 minuta;
- Alarmi CFP modula koji se mogu pratiti periodičnim očitavanjem tabele alarma, a svaka promena alarma prouzrokuje i slanje *snmptrapd* poruke uređaja prema NMS-u, sa informacijom o kom alarmu se radi.

Objekti upravljanja CFP modula su opisati u bazi upravljačkih informacija (MIB), i to tako da budu pregledni i pogodni za eventualna proširenja kod različitih verzija CFP modula. S obzirom da CFP moduli mogu imati različit broj mrežnih traka (*network lanes*) pogodno je sve objekte upravljanja koji zavise od broja traka smestiti u posebnu tabelu u kojoj svaka traka, nekog CFP modula u uređaju, predstavlja zasebnu kolonu.

Ono po čemu se CFP modul razlikuje od prethodnih OTN modula je i mogućnost kontrole predajne snage pa se objekti upravljanja koji se odnose na kontrolu predajne snage mogu smestiti u zasebnu tabelu. Zasebnu tabelu čine i dijagnostički parametri koji se odnose na predajnu i prijemnu snagu, struju polarizacije lasera (*laser bias*), struja polarizacije poluprovodničkog optičkog pojačavača (*semiconductor optical amplifier bias*), temperatura primopredajnika, napon napajanja kao i sve granične vrednosti za upozorenja i alarme ovih parametara.

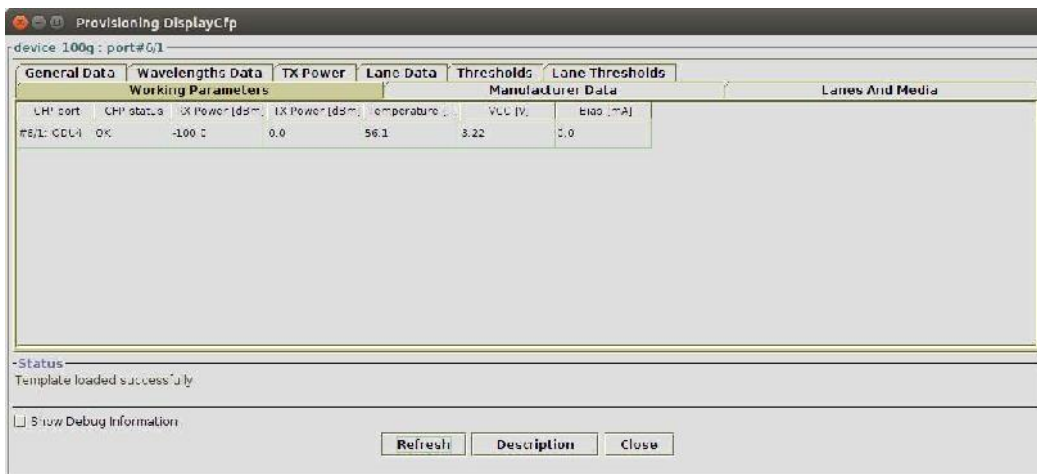
Ukoliko je sam modul podesiv (*tunable*) može mu se podešavati talasna dužina odnosno kanal po kojem radi. Agent, nezavisno od modula, u fajl sistemu čuva informacije o tome koji je kanal podešen, da li je predajna snaga kontrolisana i kolika je predajna snaga programirana tako da je konfiguracija modula moguća i pre priključivanja modula u uređaj. To takođe omogućava i konzistentan rad modula prilikom njegovog reseta ili reseta uređaja.

Konfiguraciju modula je moguće i sačuvati i učitati na drugi modul. Implementirano je uključivanje i isključivanje modula softverskim putem tj. slanjem odgovarajuće SNMP poruke.

Na klijentskoj aplikaciji u okviru postojećeg NMS sistema SUNCE-O implementirane su forme koje omogućavaju nadgledanje i upravljanje CFP modulom. Klijentske forme komuniciraju sa serverom na udaljenom racunaru koji ima ulogu menadžera u organizaciji mreže upravljane SNMP protokolom. U okviru servera napravljen je poseban NMS modul zadužen za komunikaciju sa implementiranim formama.

Na Slici 3. prikazan je izgled forme za prikaz parametara rada CFP modula. Prikaz parametara je grupisan na različitim tabovima. Tekuće vrednosti ovih parametara se očitavaju sa uređaja pri otvaranju forme ili sa forme na zahtev pritiskom na dugme *Refresh*.

Na Slici 4. je prikazana grafička forma na kojoj se vide samo neki od alarma koji se mogu pojaviti pri radu CFP modula (npr. CFP-Rx-LOS označava gubitak optičkog signala na ulazu u prijemnik)

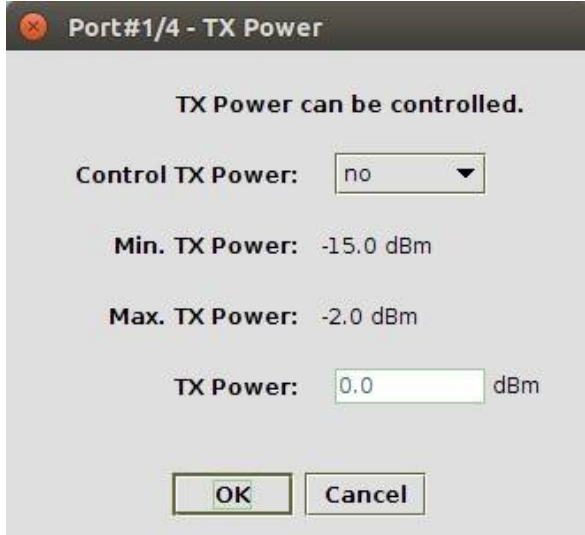


Slika 3. Grafička forma za prikaz parametara rada CFP modula



Slika 4. Grafička forma za prikaz alarma CFP modula

Na slici 5. je prikazano podešavanje minimalne i maksimalne izlazne snage iz CFP modula.



Slika 5. Grafička forma za podešavanje predajne snage

## 5. ZAKLJUČAK

Softverska integracija CFP modula u postojeći NMS sistem SUNCE-O je urađena tako što je proširen SNMP agent (podagent) koji se izvršava na uređajima OTP100G IRITEL, modifikovan menadžer na NMS serveru i tako što je proširena baza upravljačkih informacija (MIB).

Grafičke forme korisničkog interfejsa su omogućile klijentski pristup realizovanim funkcionalnostima CFP modula. Sve funkcionalnosti su uspešno testirane i implementirane u komercijalnoj verziji NMS sistema SUNCE-O Ver. 3.0 i u komercijalno dostupnoj optičkoj transportnoj platformi OTP100G IRITEL. Takođe, svi budući tipovi CFP modula se mogu lako integrisati u NMS sistem.

## NAPOMENA (ZAHVALNICA)

Ministarstvu prosvete, nauke i tehnološkog razvoja Republike Srbije koje je delimično finansiralo rad na projektu TR32007 "Multiservisna optička transportna platforma OTN10/40/100 Gbps sa DWDM/ROADM i Carrier Ethernet funkcionalnostima"

## LITERATURA

- [1] OTP100G IRITEL, Tehnička dokumentacija: opis, instalacija i rukovanje, IRITEL, Beograd, 2017.
- [2] NMS SUNCE-O, Tehnička dokumentacija: opis, instalacija i rad sa softverom, IRITEL, Beograd, 2017.
- [3] Essential SNMP, By Douglas Mauro, Kevin Schmidt
- [4] <http://www.net-snmp.org/>
- [5] Petar Knežević, Upravljanje multiservisnim SDH uređajima pomoću SNMP protokola, Magistarski rad, Elektrotehnički fakultet Beograd, Januar 2006.

# IMPLEMENTACIJA SISTEMA ZA PRIKUPLJANJE PODATAKA, GENERISANJE KLASTERA I PREPORUKA POMOĆU MAŠINSKOG UČENJA

## IMPLEMENTATION OF WEB CRAWLER AND GENERATING CLUSTERS AND RECOMMENDATIONS USING MACHINE LEARNING

Dražen Drašković<sup>1</sup>, Nemanja Kojić<sup>1</sup>, Marko Mićović<sup>1</sup>, Uroš Radenković<sup>1</sup>

*Elektrotehnički fakultet Univerziteta u Beogradu<sup>1</sup>*

**Sadržaj** - U ovom istraživanju analiziran je sadržaj jednog veb sajta sa velikom količinom podataka o muzičkim albumima. Za prikupljanje informacija o albumima, pesmama, žanrovima, stilovima, izvođačima i autorima korišćene su tehnike veb-indeksiranja i veb-parsiranja. Dobijeni podaci su zatim analizirani pomoću metode k-srednjih vrednosti koja pripada algoritmima mašinskog učenja. Cilj istraživanja bio je da se implementira softverski sistem koji će moći da generiše klasterne i preporuke korisnicima sistema.

**Abstract** - This research analyzed the content of a web site with a big data of music albums and songs. Web-crawling and web-scraping techniques were used to collect information about albums, songs, genres, styles, artists and authors. The obtained data were analyzed using machine learning algorithm k-means clustering, one of the simplest unsupervised learning algorithms. The aim of the research was to implement a software system that would be able to generate clusters and recommendations to system users.

**Ključne reči** - web crawling, web scraping, mašinsko učenje, k-means klasteri

### 1. UVOD

Razvojem Interneta, implementacijom mnogih portala i veb sajtova sa velikom količinom informacija i uvođenjem društvenih mreža, količina podataka oko nas povećava se eksponencijalno. Prema podacima iz 2016. godine u svetu postoji više od jedne milijarde Internet sajtova, ali vrlo mali procenat tih sajtova sadrži sveobuhvatnu kolekciju podataka.

Za potrebe ovog istraživanja izabran je jedan od veb sajtova sa velikom kolekcijom podataka iz oblasti muzike. Platforma sadrži nešto manje od 9 miliona muzičkih naslova, koji obuhvataju brojne naslove izdate na gramofonskim pločama, kasetama, kompaktnim diskovima i u drugim formatima. Gramofonske ploče čine oko polovine korpusa. Naslovi se mogu pretraživati po žanru i stilu muzike, formatu, zemlji i dekadi u kojoj su izdati. Pretragom se dobijaju nazivi albuma i njihovi izvođači, a odabirom određenog naslova prikazuju se detalji o albumu, pesme koje sadrži, autori, mišljenja korisnika, dostupnost i statistike o albumu. Pored pretrage albuma,

na veb sajtu je moguće videti detalje o izvođačima i njihova ostala izdanja.

Nedostatak ove platforme je što ona ne daje preporuke korisniku o sličnim albumima i autorima. Zato smo odlučili da sa platforme prikupimo podatke metodom veb-indeksiranja i da ih smestimo u bazu, a zatim da dobijene podatke klasterizujemo pomoću mašinskog učenja, metodom k-srednjih vrednosti. Na osnovu dobijenih klastera, korisniku koji je izabrao određeni album preporučili bi se slični albumi.

Istraživanje je obuhvatilo oko 50 000 albuma izdatih na prostorima Srbije i bivše Jugoslavije. Raznovrsnost podataka koji su prikupljeni je velika - od albuma sa samo jednom pesmom, do komplikacija koje sadrže više albuma u sebi. Albumi mogu imati jednog ili više autora, ali i svaka pesma može imati posebne autore sa različitim ulogama - kompozitor, tekstopisac, aranžer, i drugi. Album može pripadati jednom ili više žanrova i stilova, takođe može imati izdavačku kuću, ali i ne mora. Zato je pravljenje relacije baze podataka u ovom istraživanju bilo poseban izazov. Dobro predstavljanje relacija između žanrova, autora, albuma i pesama, bilo je neophodno da bi se omogućilo što bolje pretraživanje prikupljenih podataka.

Preporučivanje sadržaja korisniku je verovatno jedan od najzastupljenijih problema današnjice, koji još uvek nije adekvatno rešen. Postoje različite metode koje se mogu koristiti i mnogo promenljivih koje treba odrediti kako bi se dobio dobar rezultat. U ovom istraživanju je korišćen algoritam k-srednjih vrednosti (eng. *k-means*), koji pripada algoritmima za mašinsko učenje koji se ne treniraju skupovima sa poznatim ulazima i izlazima (eng. *unsupervised learning*), već on samo na osnovu ulaznih podataka određuje sličnost elemenata i tako ih deli u grupe. Kako bi ovaj algoritam što bolje radio, potrebno je definisati ulazne parametre i odrediti koji ulazni podaci su bitni da bi se dobio odgovarajući izlaz.

U nastavku ovog rada, data je kratka analiza problema veb indeksiranja i veb parsiranja i zahtevi koje smo postavili pri realizaciji softverskog sistema. U radu je prikazan opis svih implementiranih funkcionalnosti i arhitektura sistema. Na kraju rada dat je zaključak.

## 2. ANALIZA PROBLEMA

Veb-indeksler (eng. *web crawler*) služi za pretraživanje i obilazak veb strana na Internetu. Njegov cilj je da se poveže na određenu veb stranu i da preuzme njen sadržaj. Parsiranjem date strane mogu da se nađu linkovi, koji vode na neke druge strane na koje veb-indeksler ponovo može da uđe i da ponovi celu proceduru. Pored otkrivanja linkova, parser može da prepozna i druge sadržaje koje strana ima. U ovom sistemu pronalazimo informacije o autorima, albumima, imenima žanrova, stilova, zemlji porekla muzičkog izdanja, i mnoge druge.

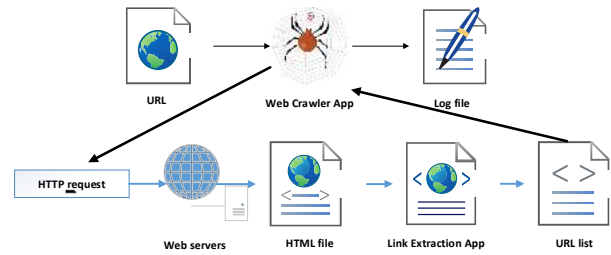
Tehnika veb indeksiranja je široko rasprostranjena i koriste je svi, od najvećih svetskih pretraživača veb sadržaja do manjih veb sajtova koji na taj način dolaze do podataka. Kako bi se sprečila krađa podataka ili usporavanje servera, mnoge platforme su razvile načine da spreče veb indeksiranje njihove platforme. Zato pravljenje veb-indeksera koji može da preuzme veliku količinu podataka bez problema zahteva analizu mnogih implementacionih detalja i uvid tokom procesa obrade sadržaja.

Implementacija veb-indeksera podrazumeva da se postave odgovarajuća zaglavlja koja veb sajt očekuje da prihvati pri pozivu. Koriste se GET ili POST pozivi, koji sadrže listu svih parametara sa odgovarajućim nazivima. Prilikom poziva veb strane može se desiti da ona bude nedostupna u kratkom periodu i u tom slučaju je neophodno da veb-indeksler ima ugrađenu mogućnost ponavljanja poziva stranice, bez bacanja greške. Vreme između ponavljanja ne sme biti previše kratko, kako bi server koji treba da odgovori imao vremena da se oporavi, ali ni previše dugo, jer svako čekanje usporava proces preuzimanja podataka.

Još jedan bitan parametar o kome se vodilo računa je vreme između dva poziva sajta. Vreme koje se čeka između dva zahteva zavisi od sledećih okolnosti:

- broja paralelnih procesa koji će biti pokrenuti u isto vreme;
- kapaciteta sistema koji treba da vrati stranu;
- broja drugih korisnika koji paralelno sa našim veb-indekslerom koristi sistem;
- strukture tog sistema i broja zahteva koji on može da primi;
- posla koji taj zahtev treba da uradi kako bi vratio veb stranicu.

Pošto najčešće treba prikupljati veliku količinu podataka, treba raditi veb indeksiranje koristeći paralelne procese, pogotovo zato što dobijene podatke treba obraditi i smestiti u bazu. To znači da jedan proces ne radi sve vreme pozivanja platforme, pa je zbog toga moguće imati više različitih procesa.



Slika 1 - Veb-indeksler i veb-parser

Postoje različite implementacije veb-indeksera pisane za sledeće programske jezike: C, C++, C#, Javu, Python, Perl, PHP i druge. Postoji preko 50 rešenja otvorenog koda, od kojih su najpoznatiji: crawler4j, Heritrix, Nutch, Scrapy, PHP-Crawler. Rešenje se najčešće bira prema zahtevima i parametrima prilikom pretraživanja podataka. U ovom istraživanju realizovana je sopstvena implementacija veb-indeksera.

Uloga veb-parsera je da otkrije potreban sadržaj sa primljenih veb strana. Pri tome je potrebno odrediti i značenje sadržaja kako bi se baza podataka popunila tačnim podacima. U ovom istraživanju korišćena je biblioteka jsoup, koja veb stranu parsira kao stablo elemenata, pamteći za svaki element njegove atribute i vrednosti atributa.

Veb-parser može da se koristi i bez veb-indeksera ukoliko imamo već fajlove koje treba analizirati, dok veb-indeksler uvek koristi veb-parser. Najčešće tehnike koje se koriste pri implementiranju veb-parsera su: HTML parser, DOM parser, tehnika regularnih izraza koji izdavaju potreban sadržaj i tehnika prepoznavanja semantičkih anotacija, odnosno meta-podataka.

Metoda k-srednjih vrednosti spada u metode mašinskog učenja kod kojih algoritam ne dobija ni primere izlaza, već uči samo iz ulaznih podataka. Cilj algoritma je da grupiše ulaze u K klastera, pri čemu svaki ulaz mora da pripada jednom od klastera i ulazi unutar jednog klastera su najslabiji između sebe. Algoritam se ne trenira kako bi shvatio šta su dobri, a šta su loši izlazi, već on to sam određuje na osnovu ulaza i ulaznih parametara.

Metoda k-srednjih vrednosti je algoritam iterativne klasterizacije. On je nedeterministički u polinomijalnom vremenu (NP težak problem), ali postoje efikasniji heuristički algoritmi koji se često primenjuju i brzo konvergiraju ka lokalnom optimumu.

Ako je dat set observacija  $(x_1, x_2, \dots, x_n)$ , gde je svaka observacija d-dimenzionalan realan vektor, metoda k-srednjih vrednosti deli n observacija u k setova  $(k \leq n)$ ,  $S = \{S_1, S_2, \dots, S_k\}$ , tako da minimizuje sumu kvadrata unutar klastera. Bitno je istaći da su skupovi  $S_1, S_2, \dots, S_k$  međusobno disjunktni i njihova unija je skup S. Rastojanje između klastera može se predstaviti sledećom formulom:





gde je  $\mu_i$  centar skupa  $S_i$ . Skupovi  $S_i$  su zapravo d-dimenzionalne lopte oko centra  $\mu_i$ .

Algoritmu je dakle potrebno zadati  $k$ , broj d-dimenzionalnih lopti, i skup ulaza  $S$ , pri čemu svaki element skupa  $S$  ima d-dimenzija. Sve dimenzije moraju biti brojevi kako bi bile uporedive i s toga se kaže da je algoritmu potrebno zadati  $n$  d-dimenzionalnih vektora. Broj  $k$  zavisi od upotrebe izlaza algoritma i utiče značajno na sličnost izlaza. Što je veće  $k$ , elementi unutar jednog podskupa  $S_i$  su sličniji.

Ovo je NP-težak problem, tako da se rešava heurističkim algoritmima. Najčešće se koristi Lojzdov iterativni algoritam koji se zove i metod k-srednjih vrednosti. Njegova složenost je  $O(nkd)$ , gde je  $n$  - broj ulaza,  $d$  - dimenzionalnost ulaza,  $k$  - broj klastera i  $i$  - broj iteracija potrebnih da bi izlaz konvergirao ka  $k$  klastera. Broj iteracija je najčešće mali, jer algoritam vrlo brzo konvergira i svakom sledećom iteracijom tačnost se minimalno poboljšava. Međutim, iako je broj iteracija mali, a samim tim i vreme izvršavanja kraće, za svaku iteraciju potrebno je izračunati rastojanja između svih centara i  $n$  ulaza. Ovo dodatno uvećava vreme izvršavanja, zato je implementacija algoritma jako bitna za njegovu brzinu. Treba iskoristiti činjenicu da su već posle nekoliko iteracija ulazi prilično dobro raspoređeni između klastera.

### 3. ZAHTEVI ZA REALIZACIJOM SISTEMA

U ovoj sekciji je dat opis strukture analiziranog veb sajta, kao i zahtevi za implementacijom algoritama za prikupljanje podataka, analizu podataka pomoću mašinskog učenja i preporučivanje sadržaja korisniku.

#### 3.1 Struktura veb sajta

Za potrebe istraživanja korišćeni su podaci sa veb sajta Discogs. To je jedna od najvećih baza podataka o muzičkim albumima na svetu. Izabrana je zato što pored naziva albuma sadrži veliku količinu detalja o njima i njihovim autorima. Takođe, podaci su vrlo lepo struktuirani, odnosno postoji konačan skup žanrova, stilova, autora, albuma, izvođača i zamlaja i imena dva ista entiteta se ne razlikuju.

Početna strana sadrži formu za prijavljivanje i registraciju novih korisnika, mogućnost pretrage bez prijavljivanja i listu svih postojećih unosa, koja obuhvata preko 9 miliona zapisa. Moguće je izabrati između 15 različitih žanrova, 477 stilova, 187 formata, 267 zemalja i 17 dekada. U ovom istraživanju uzeti su podaci koji filtriraju samo naslove iz Srbije, preko 8 hiljada naslova, i Jugoslavije, sa oko 43 hiljade naslova.

Veb strana sa albumom se sastoji iz više sekcija, koje su dinamičke, što znači da mogu, ali ne moraju da budu prikazane u zavisnosti od podataka o albumima koji su uneti. Centralni deo strane sadrži osnovne informacije o

albumu, zatim listu pesama, kompanije, zasluge, dodatne informacije, druge verzije i mišljenja korisnika. Albumi mogu da sadrže samo osnovne informacije o albumu i listu pesama, pa do svih navedenih detaljnih informacija.

Sekcija osnovne informacije o albumu sadrži imena izvođača kojih može biti jedan ili više, a vrlo često se dešava da za neke albume postoji neka izvođačka grupa koja se kasnije podelila ili ujedinila sa nekom drugom. U tom slučaju stari i novi izvođači se smatraju kao zasebni entiteti. Pored imena izvođača nalazi se slika prednje strane albuma i ime albuma, a unutar sekcije su i labela, format, zemlja, godina ili datum izlaska, žanrovi i stilovi.

Lista pesama uglavnom sadrži broj pesme na albumu i naziv pesme, često dodatne autore na pesmi, a ponekad i trajanje pesme u formatu MM:SS. Broj pesme na albumu često nije broj već može biti i slovnna oznaka. Dodatni autori na pesmi imaju svoje uloge i link na stranu koja sadrži više informacija i autoru ili izvođaču. Uloge su različite: glavni vokal, ostali vokali, kompozitor, orkestar, tekstopisac, aranžer, gostujući izvođači i druge uloge.

#### 3.2 Prikupljanje podataka

Prikupljanje podataka je implementirano u programskom jeziku Java korišćenjem biblioteke za dovlačenje i parsiranje veb strana - jsoup. Zbog dinamičkog prikaza informacija na stranama o albumima, u velikoj meri je korišćena struktura drveta koja se dobija parsiranjem veb strane, kako bi se sekcije i informacije pravilno prepoznale. Pošto u većini slučajeva nije bilo moguće prepoznati sekciju na osnovu detalja u njoj, jer su u kodu korišćeni isti elementi i stilske klase kao za druge sekcije, korišćena je struktura stabla, da bi se iz svake sekcije pročitali svi njeni elementi i da se na taj način dobije informacija o tome koji elementi pripadaju kojoj sekciji.

#### 3.3 Analiza podataka pomoću mašinskog učenja i preporuke

Kako bi se podaci obradili pomoću metode k-srednjih vrednosti, potrebno je napraviti vektore koji mogu da služe kao ulazni podaci. Takođe, treba odrediti broj dimenzija koje želimo da koristimo i broj klastera koje želimo da proizvedemo. Imajući u vidu da koristimo podatke samo iz Srbije/Jugoslavije, najrelevantniji parametri koji su dostupni u svim albumima su žanrovi i stilovi, kao i godina izdanja.

Urađena je analiza pomoću k-srednjih vrednosti koja uključuje prostor sa većim brojem dimenzija: svi žanrovi (15 dimenzija), stilovi (477 dimenzija) i dekade (17 dimenzija). Cilj je da izlazi budu što sličniji albumi, te je stoga broj klastera veliki ( $k=5000$  za oko 51 000 ulaza). Dobijeno je da je prosečan broj albuma po klasteru 10. Urađene su analize i za drugi broj klastera ( $k=100$ ,  $k=500$  i  $k=1000$ ).

Druga analiza, koja bi bila interesantna je da se sa datim podacima i sa manjim brojem dimenzija (3 dimenzije), imala bi za cilj da se albumi prikažu vizuelno u prostoru. Kao dimenzije mogu se uzeti dekada izdavanja, prvi stil i prvi žanr izlistani na strani albuma. Broj klastera treba da bude manji (mogu se probati vrednosti  $k=5$ ,  $k=10$  ili  $k=20$ ). Rezultati metode k-srednjih vrednosti sa ovakvim

ulaznim parametrima mogu se lepo prikazati jednim trodimenzionalnim grafom, na kome se može videti raspored albuma i njihovo grupisanje. Rezultati te analize mogu da pokažu koji su najzastupljeniji žanrovi i stilovi na prostorima Srbije i bivše Jugoslavije, kao i kako se situacija menjala kroz godine. Ovu analizu je moguće uraditi pomoću istog algoritma koji smo upotrebili za preporučivanje uz ulazne podatke koji su navedeni.

Konačni rezultat ovog istraživanja ke da korisnik pretražuje sadržaj veb sajta po raznim kriterijumima i da za izabrani album dobije preporuke o njemu sličnim albumima. Pošto korisnik nema korisnički profil i ne čuva se istorija pregleda albuma od strane korisnika, preporuke mogu da se vrše samo na osnovu trenutno stanja, odnosno albuma koji trenutno gleda. Ovaj način preporučivanja se zove prepouka bazirana na proizvodu.

#### 4. OPIS SISTEMA

Da bi se prikazali rezultati i analiza ovog istraživanja, napravljena je softverski sistem - veb aplikacija u Javinim veb tehnologijama, pomoću tehnologija Java Server Faces i biblioteke PrimeFaces. Ulaskom na prvu stranu korisnik dobija listu svih albuma koji su dostupni u bazi podataka, a iznad nje formu pomoću koje može da pretražuje albume po raznim kriterijumima. Izborom nekog albuma iz liste korisnik dobija mogućnost da pregleda detalje o albumu i kao rezultat rada algoritma za preporuke, dobija sugestije o sličnim albumima koje može da pogleda. Sistem je realizovan kao MVC (Model-View-Controller) veb aplikacija.

##### 4.1 Pregled sadržaja

Izborom albuma iz osnovne liste ili liste koju je dobio pretraživanjem, korisniku se otvara strana sa detaljima o albumu. Cilj ove veb strane je da prikaže sve bitne informacije o albumu koje se nalaze i na originalnom sajtu sa muzičkim albumima. Svaki album ima svoj naslov, izdavačku kuću, format izdanja, kategoriju izdanja, zemlju izdavanja albuma, godinu (ili datum) izdavanja, listu žanrova, odvojenih zarezima, listu stilova, odvojenih takođe zarezima, listu autora, koji su autori na celom albumu i listu kompanija, koji su saradivali u izradi albuma. Ispod ovih osnovnih informacija o albumu, prikazuje se lista pesama na tom albumu, sa dostupnim informacijama: pozicija na albumu (broj, slovo ili broj i slovo), naziv pesme, tabela sa autorima i trajanje.

##### 4.2 Pretraživanje sadržaja

Forma za pretragu nalazi se na vrhu veb strane i ima veći broj opcija za pretraživanje. Korisnik može odabrati da li želi da dobije uniju ili presek elemenata koji zadovoljavaju njegovu pretragu. Ukoliko korisnik želi uniju svojih kriterijuma, prikazaće mu se svi albumi koji zadovoljavaju bar jedan od podataka unetih u formi za pretragu. Ukoliko izabere presek, prikazaće se samo albumi koji sadrže sve kriterijume pretrage.

Na izvornom sajtu prilikom pretraživanja prikazuje se samo presek kriterijuma zadatih u pretrazi, što nam omogućava da lakše suzimo izbor albuma, ali nam ne onemogućava da se na primer nađu albumi kod kojih nismo sigurni za određene podatke. Recimo ako tražimo muzički album za koji ne znamo da li je nastao krajem

70-ih, u 80-im ili početkom 90-ih godina, na izvornom sajtu moramo da izvršimo tri pretrage kako bismo proverili da li je album koji nas interesuju unutar baze podataka. Sličan problem je i ako pretragu vršimo po stilovima ili po žanrovima.

Uvođenjem mogućnosti da se pretrage prikazuje na osnovu unije, ovo istraživanje omogućava da se razreše navedeni problemi i da se korisniku omogući kvalitetnija pretraga. Prikaz forme za pretragu dat je na slici 2.

Choose method:	<input checked="" type="radio"/> Union <input type="radio"/> Section
Song Name:	Ajde Da Li Znaeš, Milice Ako Ako Ako Dođeš Ti Ako Se Ikada Dogodi Ako Ti Se Još Momkuje
Author Name:	A. Nikolić A. Putarek A. Sarlevski A. Todorović Krnjevac A. Tomošević
Album Name:	Dođi Dom Za Vešanje (Muzika Iz Filma E Donesi Vina, Krčmarice Dođe Vreme Da Se Ženim / Frulo M Dođi
Country:	Serbia Yugoslavia
Released:	1965 1966 1967 1969 .....
Format:	CD CDr Cassette File Flv, mp3

Slika 2 - Prikaz dela forme za pretragu u realizovanom sistemu

Pretraživanje je moguće po imenu nekog od autora, imenu albuma, imenu neke od pesama, zemlji porekla albuma, datumu/godini, imenu neke kompanije koja je učestvovala u izradi, stilu, žanru i formatu. Sve moguće opcije ponuđene su korisniku u vidu listi i padajućih menija. Kada korisnik pritisne dugme "Pretraži", pretražiće se baza podataka i dobiće se rezultati koji odgovaraju njegovoj pretrazi. Ukoliko korisnik nije uneo nijedan parametar pretrage, lista će sadržati sve postojeće albume iz Srbije i bivše Jugoslavije. Podaci se prikazuju tabelarno, uz uključenu paginaciju od 20 rezultata po veb strani, kao što je prikazano na slici 3. Izborom određene stavke u tabeli, odnosno naziva albuma, prelazi se na stranu sa detaljima o tom albumu.

Album title	Format	Country	Released time
Amala	Vinyl	Yugoslavia	1967
Kola	Vinyl	Yugoslavia	1969
Kola	Vinyl	Yugoslavia	1971
Kola	Vinyl	Yugoslavia	1971
Kola	Vinyl	Yugoslavia	1970
18 Zlatnih Hitova iva Robića	Vinyl	Yugoslavia	1977
Yemenite Songs	Cassette	Yugoslavia	1968
Primosten, Najpisa Misto / Primosten, Mote I II	Vinyl	Yugoslavia	1962
No Need To Argue	Cassette	Yugoslavia	
Before We Were So Rudely Interrupted	Vinyl	Yugoslavia	
Hendrix In The West	Vinyl	Yugoslavia	1971
Орнејум: Чајноскијама Орејби '87	Vinyl	Yugoslavia	1967
Narcini Cocktail	Cassette	Yugoslavia	1962
Hitka No. 1 - Hitovi, Hitovi	Cassette	Yugoslavia	1990
Krapina '85 - Festival Krapinske Pijevke	Cassette	Yugoslavia	1988
Ozogene	Cassette	Yugoslavia	1976
Stobodan Latic	Vinyl	Yugoslavia	1964
Labinške Konji Tenci - Narodne Pjesme I Piosovi Labinšine - Folk Songs And Dances Of The Region Of Labin	Cassette	Yugoslavia	1963
Narodna Kola Na Svesotaru	Vinyl	Yugoslavia	1962
Navika Sam Na Tebe	Cassette	Yugoslavia	1967

Slika 3 - Rezultati pretrage

### 4.3 Preporučivanje sadržaja

Preporučivanje sadržaja korisnicima vrši se samo na nivou albuma, odnosno korisniku koji gleda album treba da se prikažu preporuke drugih albuma. Sistem se vrlo lako može proširiti dodavanjem funkcionalnosti preporuka na osnovu autora ili glavnog izvođača.

Preporučivanje se vrši na osnovu sličnosti albuma koji korisnik gleda u datom trenutku. Koristi se algoritam mašinskog učenja metoda k-srednjih vrednosti, koji deli sup svih albuma u podskupove. Kada korisnik učita određeni album iz baze podataka se traže svi albumi koji su u istom podskupu u kome se nalazi dati album i ti albumi se prikazuju kao slični. Broj takvih albuma može biti od 0 do 50 hiljada, ali je zbog korišćenih ulaznih parametara najverovatniji broj preporučenih rezultata oko 10.

Ukoliko ne postoji nijedan preporučeni album, korisniku će se ispisati poruka da sličnih albuma trenutno nema u bazi. Ako je algoritam pronašao neke slične albume, korisniku će se prikazati tabela sa albumima, slične tabelarne strukture kao lista albuma prilikom pretrage na glavnoj veb strani aplikacije.

## 5. REALIZACIJA SISTEMA

Realizovani sistem se sastoji od četiri komponente: (1) veb-indeksersa veb-parserom; (2) relacione baze podataka; (3) algoritma za klasterizaciju, implementiranog u Javi; (4) veb aplikacije za prikaz, pretragu i preporučivanje, realizovanu koristećih tehnologiju JSF i biblioteku PrimeFaces.

Veb-indeksiranje je urađeno posle detaljne analize jednog muzičkog sajta kako bi se njegova struktura iskoristila za što lakše parsiranje veb strana i što brži obilazak, tj. slanje što manje poziva. U ovom istraživanju analizirali smo samo podatke o albumima iz zemlje Srbija/Jugoslavija. Korišćena je metoda GET, odnosno podaci su samo preuzimani slanjem odgovarajućih parametara koji selektuju odgovarajuću stranu direktno u pozivu. Nisu popunjavane forme koje se nalaze na sajtu, niti je svrha

bilo kog poziva bila da utiče negativno na platformu ili da ometa rad analiziranog sajta.

Prikupljanje podataka je izvršeno brzo time što je broj poziva optimizovan i iznosi oko jedan poziv po albumu. Na mnogim platformama ovo nije moguće uraditi, ali ovde je takva struktura bila moguća, jer je redosled albuma i njihovom pregledu za isti filter uvek isti i podatak kojim se poziva određeni album uvek je imao istu strukturu.

U istraživanju je implementiran eksponencijalni *back-off* algoritam čija je svrha da ukoliko od primljenog odgovora dobije informaciju da je strana koja se traži nedostupna, ponovo pozove tu stranu nakon jedne sekunde. Ukoliko je strana dva puta bila nedostupna, pozvaće se i treći put nakon 2 sekunde, a nakon tri neuspešna pokušaja prikazaće se greška.

Eksponencijalni *back-off* algoritam se često koristi u današnjim veb-indekserima, međutim nije deo biblioteke jsoup, tako da je ovde implementiran dodatno. Postoje biblioteke u Javi koje rade ovaj posao, međutim u ovom istraživanju one nisu korišćene. Ovde je algoritam implementiran pomoću sleep metode koja se pozove na odgovarajući broj milisekundi.

U paraleli se izvršava 10 procesa koji se bave preuzimanjem podataka o različitim albumima. Vreme potrebno za preuzimanje svih 50 hiljada nslova bilo je oko 2 sata. Kada bi se preuzimala veća količina podataka, trebalo bi pokušati sa većim brojem paralelnih poziva od kojih bi neki išli preko proxy servera. U ovom istraživanju nije bilo potrebno koristiti tu mogućnost, pošto su podaci preuzeti u konačnom intervalu.

Posle preuzimanja podataka, najveći problem je bio kako na odgovarajući način parsirati veb strane sa detaljima o albumima koje imaju dinamički sadržaj. Prikazuju se samo sekcije koje sadrže podatke i svaki album ima različite sekcije. Takođe, atributi, stilovi i elementi koji su korišćeni slični su za sve sekcije, tako da nije moguće uvek prepoznati koja je sekcija ili element u pitanju, i samim tim nismo sigurni da uzimamo potreban podatak. U slučajevima kada nije bilo moguće okriti o kojoj sekciji se radi, polazilo se od korena sekcije u stablu, pa su se prolaskom kroz njeno podstablo nalazile odgovarajuće informacije.

Podaci se čuvaju u relacionoj bazi podataka koja je granulirana na manje tabele, kako bi podržala različite odnose između entiteta. Jaki entiteti su album, pesma, žanr, stil, autor i kompanija. Većina relacija unutar baze je tipa više prema više (eng. *many-to-many*).

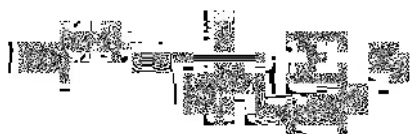
Kako bi se podaci o albumima podelili u klastere implementirana je metoda k-srednjih vrednosti. Svaki ulaz ima 509 dimenzija (17 za dekade, 15 za žanrove i 477 za stilove). Album može za svaku dimenziju da ima 1 ili 0 kao vrednost, pri čemu je vrednost 1 ukoliko je album nastao te dekade (za neku od 17 dimenzija dekade), ima taj žanr (za neki od 15 žanrova) ili ima taj stil (za neki od 477 stilova). Album ivek ima samo jednu dekadu, ali najčešće ima nekoliko žanrova i stilova.

Implementiran je iterativni algoritam za metodu k-srednjih vrednosti, poznat još i kao Lojgov algoritam. Prvo se izabere K slučajnih vrednosti koje se nalaze unutar kocke koja ima 509 dimenzija sa ivicama u (0,0; 0,1; 1,0; 1,1), a zatim algoritam iterativno ponavlja sledeće korake:

1. Dodela observacija nekom od k-klastera (koji su nastali na osnovu K slučajno generisanih vrednosti). Dodela se vrši tako što se nađe klaster koji je najbliži toj observaciji, što se računa prema formuli:

$$S_i^{(t)} = \{x_p : \|x_p - m_i^{(t)}\| \leq \|x_p - m_j^{(t)}\| \forall 1 \leq j \leq k\}$$

2. Ažuriranje centara klastera koje se računa tako da je novi centar svakog klastera tačka koja je minimalno udaljena od svih tačaka u klasteru:



Algoritam se završava kada u koraku dodele observacije nijedna observacija ne promeni svoj klaster. Izlaz algoritma je lista observacija sa brojem klastera kojoj pripadaju. Pripadnost klasterima se čuva u tabeli kako bi mogla da se prikaže korisniku tokom prikaza preporuka.

## 6. ZAKLJUČAK

Cilj ovog istraživanja je da se objedini nekoliko tehnika za prikupljanje i obradu podataka kako bi se korisniku omogućila bolja vrednost dobijenih informacija i preporuka na osnovu raspoloživih podataka.

Podaci su preuzeti sa muzičkog sajta čija je primarna svrha čuvanje i razmena gramofonskih ploča, dok su podržani i drugi formati kao što su kasete, kompakt diskovi i drugi. Platforma sadrži oko 9 miliona naslova, među kojima se može nalaziti više naslova za jedno isto izdanje. Sajt se može pretraživati po nekoliko kategorija: zemlja, dekada i godina nastanka albuma, žanrovi, stilovi i formati. Kao rezultat pretraživanja uvek se vraća presek unetih pretraga. Izborom nekog albuma otvara se veb strana koja prikazuje dinamički generisane dostupne detalje o tom albumu.

U ovom istraživanju prikupljeni su podaci o svim albumima čija je zemlja porekla Srbija/Jugoslavija, što predstavlja korpus od oko 50 hiljada naslova. Za svaki album, prikupljeni su detaljni podaci i napravljena je baza podataka koja podržava različite relacije među entitetima. Veb-indeks i veb-parser koji su korišćeni za preuzimanje i parsiranje podataka, implementirani su u programskom jeziku Java uz pomoć biblioteke jsoup. Bilo je potrebno podesiti odgovarajuće parametre i postaviti zaglavlja kako bi se veb indeksiranje odvijalo što brže. Takođe, zahvaljujući strukturi sajta, smanjen je broj pristupa platformi na skoro 1 pristup po albumu, što značajno utiče na brzinu prikupljanja podataka.

Nakon što su podaci prikupljeni i smešteni u bazu, izvršena je analiza pomoću mašinskog učenja, korišćenjem algoritma k-srednjih vrednosti. Algoritam je implementiran koristeći Lojgov iterativni pristup. Početni

centri klastera su slučajno generisani unutar mogućeg polja rešenja. Ulaz u algoritam predstavlja nešto više od 50 hiljada vektora koji imaju 509 dimenzija (dekade, stilovi i žanrovi). Svaki album ima vrednost 0 ili 1 za svaku od dimenzija u zavisnosti od toga da li sadrži tu dimenziju ili ne.

Dobijeni klasteri služe kako bi se na portalu prikazale preporuke korisniku. Preporuke se generišu samo na osnovu albuma koji korisnik trenutno gleda. U daljem istraživanju moguće je čuvati istoriju korisnika, pomoću koje se može napraviti kompleksniji sistem za preporuku albuma. Moguće je implementirati i hibridne metode koje se baziraju na korisnicima i proizvodima.

## ZAHVALNICA

Ovaj rad je napisan u okviru projekata TR-32047 kod Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

## LITERATURA

- [1] C. Olston, M. Najork, "Web Crawling," Foundations and Trends in Information Retrieval, Vol. 4, No. 3, pp. 175-246, 2010.
- [2] B. Bahmani et al. "Scalable K-Means++," Journal Proceeding of the VLBD Endowment, Vol. 5, No. 7, pp. 622-633, March 2012.
- [3] M. Abu Kausar et al. "Web Crawler: A Review," International Journal of Computer Applications, Vol. 63, No. 2, pp. 31-36, February 2013.
- [4] T. Udupure et al. "Study of Web Crawler and its Different Types," IOSR Journal of Computer Engineering, Vol. 16, No. 1, pp. 1-5, February 2014.
- [5] S. Guliani, A. Rajoriya, "An Enhanced Clustering Algorithm by Comparative Study on K-Means Algorithm," International Journal of Engineering Research and Technology, Vol. 4, No. 6, June 2015.
- [6] T. Kanungo et al. "An Efficient k-Means Clustering Algorithm: Analysis and Implementation," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 7, July 2002.
- [7] E. Liberty et al. "An Algorithm for Online K-Means Clustering," Proceedings of the 18th Workshop on Algorithm Engineering and Experiments, 2016.
- [8] P. Cording, "Algorithms for Web Scraping", available on: [http://www2.imm.dtu.dk/pubdb/views/edoc\\_download.php/6183/pdf/imm6183.pdf](http://www2.imm.dtu.dk/pubdb/views/edoc_download.php/6183/pdf/imm6183.pdf)

# KOMPARATIVNA ANALIZA KOMPLEKSNIH UPITA NAD BAZOM PODATAKA I SKLADIŠTEM PODATAKA

## COMPARATIVE ANALYSIS OF COMPLEX REQUIREMENTS BASED ON DATA BASE AND DATA COLLECTION

Atanasijević Jordan<sup>1</sup>, Stanković Nevena<sup>2</sup>  
Generalštab Vojske Srbije<sup>1</sup>, GARDA, Beograd  
ZU AP „Oaza zdravlja“<sup>2</sup>, Beograd

**Sadržaj** - Skladištenje podataka i poslovna inteligencija su tehnike koje obezbeđuju poslovnim ljudima informacije i alate koji su im potrebni za donošenje odluka o operativnom i strateškom poslovanju. Odluke najčešće zahtevaju jedinstveni podskup informacija, koji u osnovi nije predodređen. Potrebno je da se izgradi informaciona infrastruktura koja integriše podatke iz cele organizacije i potencijalno izvan organizacije, a zatim čisti, ispravlja i restruktuirira podatke da budu fleksibilni i upotrebljivi što je više moguće. Dok većina modula transakcionog sistema radi sa jednim tipom informacija, kao što su fakture, nalozi ili potraživanja, DW/BI sistem mora da ih integriše sve zajedno. DW/BI sistem zahteva tehnički sofisticirano upravljanje i prikupljanje podataka iz različitih izvora, a najčešće ih generiše iz baza podataka.

Ono što su konkretna očekivanja u vezi rezultata istraživanja to je da se kroz implementaciju skladišta podataka pokaže da će se dobiti bolje performanse u vremenu izvršavanja upita i generisanja izveštaja u odnosu na one koje su dobijene za te iste upite i izveštaje ali nad bazom podataka iz koje je kasnije razvijeno skladište podataka.

**Abstract** - Data storage and business intelligence are techniques that provide business people with information and tools they need to make decisions about operational and strategic business. Decisions often require a single subset of information, which is basically not predetermined. It is necessary to build an information infrastructure that integrates data from the whole organization and potentially outside the organization, and then cleans, rectifies and restructure data to be flexible and usable as much as possible. While most transaction system modules work with one type of information, such as invoices, orders or receivables, the DW/BI system must integrate them all together. The DW/BI system requires a technically sophisticated management and collection of data from a variety of sources, and most often generates them from the database.

What is specific to the expectations regarding research results is that through the implementation of the data record it will show that better performance will be obtained at the time of query execution and generating reports than those obtained for those same queries and reports, but over the database from which was later developed a data warehouse.

### 1. UVOD

Globalni trendovi i ekspanzija informacionih tehnologija, doveli su do potrebe da se iznađe rešenje za nadolazeću plimu podataka koju treba akumulirati i obraditi. U ovom trenutku sistemi su dosta raznoliki i skladište podatke u različitim i obično nekompatibilnim formatima, što dovodi do toga da celokupno poslovanje funkcioniše u fragmentima. To je dovelo do „pat“ pozicije između efikasnog odlučivanja i razbacanih izvora informacija. Savremeno poslovanje zahteva donošenje odluka u najkraćem vremenu.

Skladištenje podataka je realizovano integracijom staromodnih informacionih sistema, koji su bili odvojeni od procesa donošenja poslovnih odluka čime se podaci pretvaraju u profitabilna informaciona sredstva [2]. Skladištenje podataka drastično skraćuje vreme koje je bilo potrebno za pristup podacima.

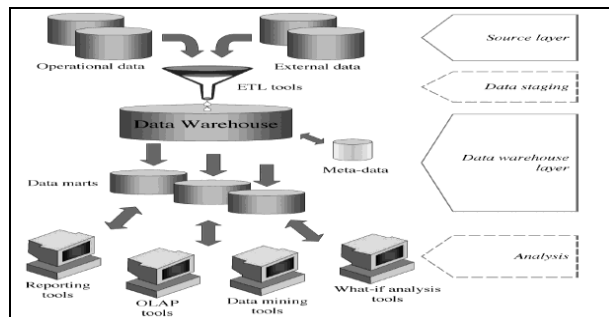
U proteklim godinama, BI i sistemi za skladištenje podataka su evoluirali u odnosu na svoj početni oblik kojim su podsećali na sisteme koji su orijentisani ka gomilanju podataka koji su bili korišćeni za jednostavno izveštavanje, postavljanje upita i analize od strane neke manje i već unapred definisane grupe korisnika. Danas su mnogi od njih veliki sistemi koji vrše obradu mnoštva različitih upita i moraju biti u kontinuitetu dostupni različitim grupama korisnika. Iz tog razloga se nametnula potreba za razmatranjem načina na koji bi se moglo izvesti unapređenje skladišta podataka u cilju efikasnije obrade upita koji se nad njim izvršavaju.



Podaci u bazi podataka su dinamični, neprestano se menjaju, dok se skladišta podataka najčešće projektuju za čitanje i analizu podataka [3].

Pored toga, skladišta podataka su dizajnirana na takav način da preuzimaju podatke, vrše izmene na već postojećim podacima, održavaju integritet i upravljaju transakcijama što je brže moguće. Skladišta se dizajniraju, najčešće za veliki broj podataka iz kojih se dobijaju kratki izveštaji sa ključnim podacima.

U samom procesu izrade skladišta podataka, korišćena je dvoslojna arhitektura, koju karakterišu [1]:



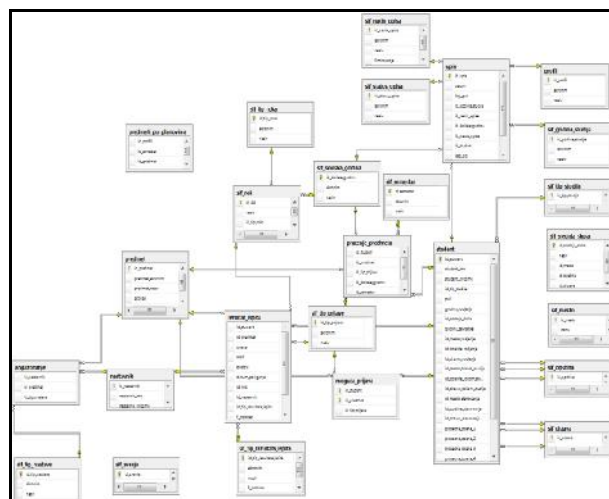
Slika 1. Dvoslojna arhitektura

## 2. ANALIZA ZAHTEVA

U radu je projektovano skladišta podataka iz postojeće test baze podataka studentske službe FON-a, a u cilju poboljšanja performansi pri dobijanju odgovora na postavljene upite, u odnosu na bazu podataka. Za razvoj skladišta podataka korišćen je SQL Server 2012 Integration Services (SSIS) koji omogućava izdvajanje, transformaciju i učitavanje podataka, tj razvoj ETL sistema. Cilj je da se podaci iz postojeće baze podataka transformišu i prilagode novim konzistentnim i odgovarajućim formatima, fokusiraju na određene interesne grupe koje predstavljaju subjekte (student, profesor, predmet, ocena,...), i da se vežu za određeni vremenski period. Na kraju, merenjem vremena dobijanja odgovora na postavljene kompleksne upite, treba prikazati prednost korišćenja skladišta podataka u odnosu na transakcionu bazu podataka.

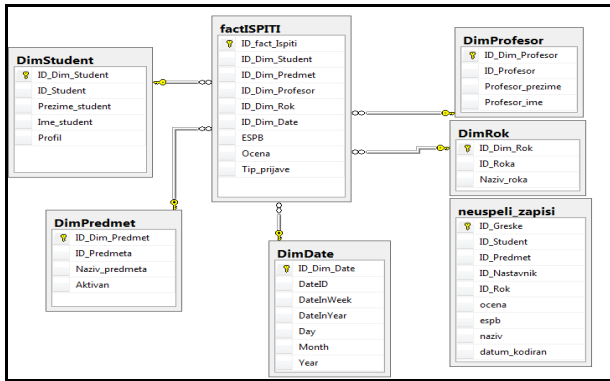
## 3. DIZAJN REŠENJA

Za potrebe rada korišćena je test baza podataka studentske službe FON-a i iz nje je kreirano skladište podataka, sa neophodnim tabelama za dobijanje odgovora na najčešće postavljene upite. Na naredne dve slike (slika 2 i slika 3) su prikazani dijagrami podataka baze podataka i skladišta podataka.



Slika 2. Dijagram podataka baze podataka

Arhitekturna razlika između skladišta podataka i data-marts svakako treba biti jasno izražena. Komponenta označena kao skladište podataka na slici 1, se takođe često naziva primarnim skladištem podataka ili korporativnim skladištem podataka.



Slika 3. Dijagram podataka skladišta podataka

Za implementaciju skladišta podataka korišćena je šema zvezde.

Šema zvezde skladišti sve informacije o dimenziji u jednu tabelu. Svaki nivo hijerarhije predstavljen je kolonom ili skupom kolona u tabeli dimenzija. Dimenzionalni objekat se može koristiti za definisanje hijerarhijskog odnosa između dve kolone (ili skupa kolona). Bez dimenzionalnih objekata, hijerarhijski odnosi su definisani samo u metapodacima. Atributi se nalaze u kolonama tabela dimenzija. Dimenzione tabele sadrže opisne tekstualne informacije. Atributi dimenzionih tabela se koriste kao ograničenja pri zadavanju upita. Svaka dimenzionalna tabela ima svoj primarni ključ, a svi oni učestvuju u stvaranju primarnog ključa tabele činjenica [6].

Tabele činjenica se koriste za čuvanje mera i sadrže podatke koji su, najčešće, numeričkog tipa i mogu sadržati veliki broj zapisa. Tabele činjenica sadrže kompozitni primarni ključ, koji se sastoji od nekoliko spoljnih ključeva (jedan za svaku tabelu dimenzija) i kolone za svaku meru koja koristi ove dimenzije.

U sledećem koraku izvršena je ekstrakcija, transformacija i upisivanje podataka u skladište podataka.

U narednom delu biće prikazan način implementacije jedne od najvažnijih dimenzija skladišta podataka, a to je dimenzija vremena. Postupak implementacije ostalih dimenzija je sličan prikazanom, sa razlikama u procedurama za ekstrakciju podataka, izvorištima i određivanjima.

Prvi korak u implementaciji dimenzije vremena je raskidanje veze između fact tabele ispiti i tabele DimDate koja predstavlja dimenziju vremena (slika 4). To se radi zbog pravila referencijalnog integriteta, jer u suprotnom sistem za upravljanje bazom podataka ne bi dozvolio brisanje podataka iz tabele DimDate. Nakon raskidanja veze između tabele, tabela DimDate se briše i ponovo kreira, sa istim kolonama, atributima, tipovima podataka i ograničenjima. Na taj način se brišu svi predhodni

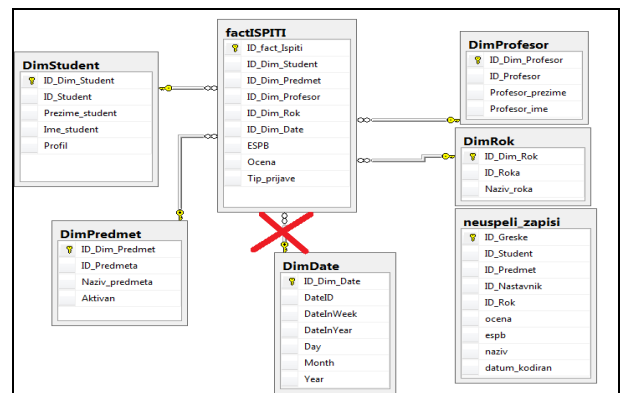
podaci i tabela je spremna za upisivanje najvažnijeg stanja iz izvorišne baze podataka.

U daljem tekstu naveden je programski kod, koji prati predhodno opisani postupak.

```

IF EXISTS (SELECT * FROM
INFORMATION_SCHEMA.REFERENTIAL_CONSTR
AINTS WHERE CONSTRAINT_NAME =
'FK_factISPITI_DimDate')
BEGIN
ALTER TABLE [dbo].[factISPITI] DROP
CONSTRAINT [FK_factISPITI_DimDate]
END
IF EXISTS (SELECT * FROM sysobjects
WHERE id = OBJECT_ID(N'DimDate'))
BEGIN
DROP TABLE [dbo].[DimDate]
CREATE TABLE [dbo].[DimDate](
[ID_Dim_Date] [int] IDENTITY(1,1) NOT
NULL,
[DateID] [int] NOT NULL,
[DateInWeek] [int] NOT NULL,
[DateInYear] [int] NOT NULL,
[Day] [int] NOT NULL,
[Month] [int] NOT NULL,
[Year] [int] NOT NULL,
CONSTRAINT [PK_DimDate] PRIMARY KEY
CLUSTERED ( [ID_Dim_Date] ASC
)WITH (PAD_INDEX = OFF,
STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON) ON
[PRIMARY]
) ON [PRIMARY]
END

```

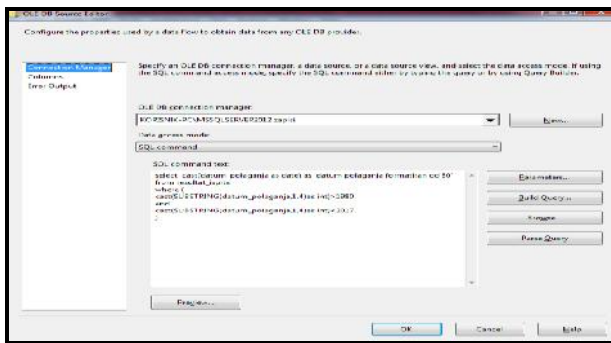


Slika 4. Brisanje veze između fact tabele i tabele koja predstavlja dimenziju

Sledeći korak je obrada podataka iz baze podataka i njihovo učitavanje, po određenom kriterijumu. U ovom delu se mogu zadati kriterijumi po kojima se podaci čitaju iz baze podataka. U konkretnom primeru (slika 5) izabrani su datumi u periodu 01.01.1981 do 31.12.2016.

U daljem tekstu naveden je programski kod, koji prati predhodno opisani postupak.

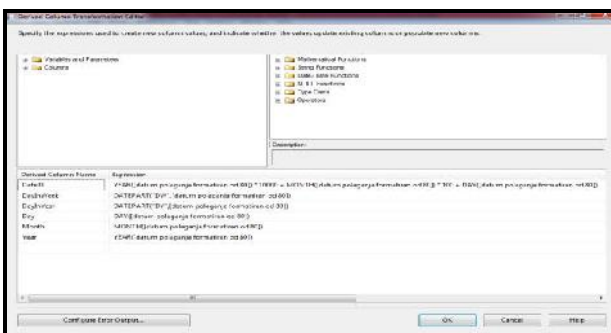
```
select cast(datum_polaganja as date) as 'datum polaganja
formatiran od 80' from rezultat_ispita where (
cast(SUBSTRING(datum_polaganja,1,4)as int)>1980
and
cast(SUBSTRING(datum_polaganja,1,4)as int)<2017
)
```



Slika 5. Obrada podataka iz baze podataka i njihovo učitavanje, po određenom kriterijumu

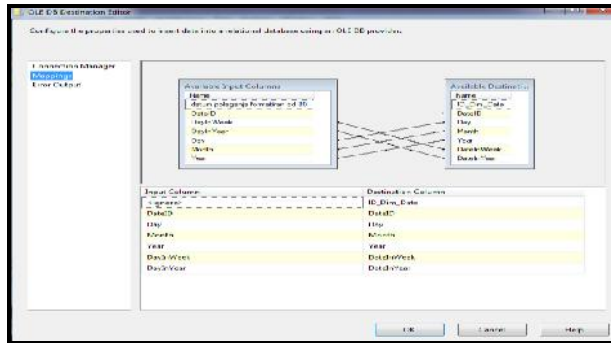
Nakon toga, na osnovu dobijene vrednosti iz baze podataka, sledi konvertovanje podataka po kolonama (slika 6 ) tabele *DimDate* u skladištu podataka. Kolone od interesa su *DayID*, *DayInWeek*, *DayInYear*, *Day*, *Month*, *Year*. Kolona *DayID* koristi se kao primarni ključ i kreirana je na sledeći način:

```
YEAR([datum polaganja formatiran od 80]) * 10000 +
MONTH([datum polaganja formatiran od 80]) * 100 +
DAY([datum polaganja formatiran od 80])
DayID od 25.11.1993 je 19931125. Na ovaj način povećane su performanse pri sortiranju.
```

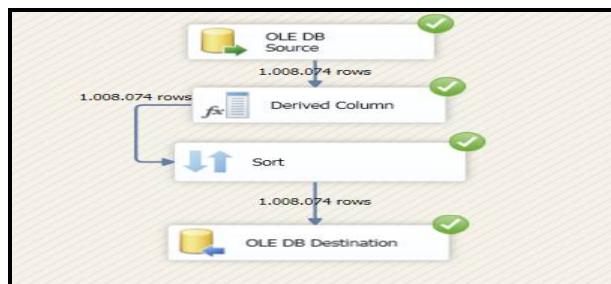


Slika 6. Konvertovanje podataka po kolonama tabele *DimDate* u skladištu podataka

Nakon predhodne aktivnosti sledi sortiranje kolona po *DayID* (slika 7) i upisivanje podataka u željeno odredište, a to je tabela *DimDay* u skladištu podataka (slika 8).

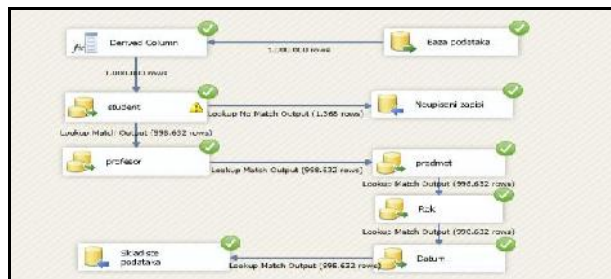


Slika 7. Sortiranje podataka po određenom kriterijumu



Slika 8. Proces učitavanja, transformacije i upisivanja podataka

Na ovaj način implementirana je dimenzija vezana za vreme. Određeno je izvoriste, razvijena je procedura za transformaciju podataka i određeno je odredište za upisivanje podataka, čime su podaci pripremljeni za dalje korišćenje. Na slici 9, prikazan je proces učitavanja podataka iz baze podataka u skladište podataka.



Slika 9. Učitavanje podataka iz baze podataka u skladište podataka

## 4. IMPLEMENTACIJA

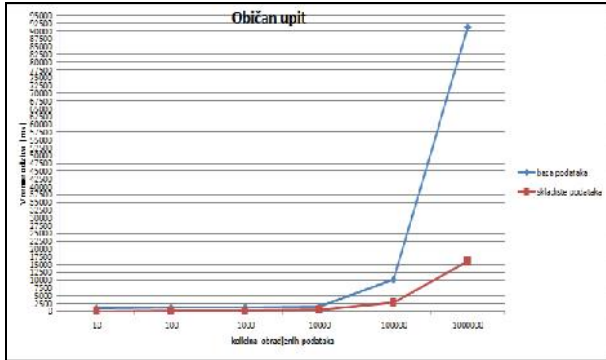
### 4.1 Običan upit

Nad bazom podataka i nad skladištem podataka postavljen je upit koji treba da vrati prezime i ime studenta, studijski program kojem pripada, naziv predmeta koji je polagao, ocenu koju je dobio, datum polaganja, kao i prezime i ime profesora kod koga je polagao ispit.

Merenjima vremena dobijanja odgovora na upit, po različitom broju zapisa, došlo se do sledećih rezultata:

broj podataka	vreme odziva[ms]	
	baza podataka	skladište podataka
10	1017	3
100	1113	83
1 000	1267	276
10 000	1556	528
100 000	10056	2811
1 000 000	91298	16073

Tabela 1. Rezultati dobijanja odgovora na običan u bazi podataka i u skladištu podataka, nad različitim brojem zapisa



Grafikon 1. Uporedna analiza dobijanja odgovora na običan u bazi podataka i u skladištu podataka, nad različitim brojem zapisa

#### 4.2 Upit sa uslovom

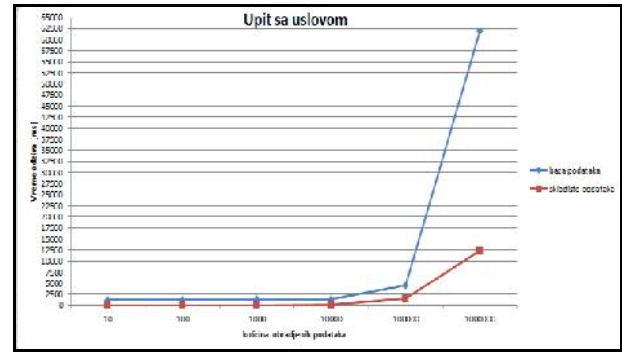
Grupisanje redova tabele se eksplicitno specificira GROUP BY klauzulom. Ona prouzrokuje dobijanje jednog rezultujućeg reda za svaku različitu vrednost kolone po kojoj se vrši grupisanje. Dejstvo GROUP BY klauzule je identično višestrukom pisanju SELECT naredbi sa različitim uslovima u WHERE klauzuli [4].

Nad bazom podataka i nad skladištem podataka postavljen je upit koji treba da vrati prezime i ime studenta, studijski program kojem pripada, pod uslovom da su položili tri i više ispita u jednom roku, sa prikazom broja tih položenih ispita i nazivom ispitnog roka.

Merenjima vremena dobijanja odgovora na upit, po različitom broju zapisa, došlo se do sledećih rezultata:

broj podataka	vreme odziva[ms]	
	baza podataka	skladište podataka
10	1130	4
100	1170	5
1 000	1317	51
10 000	1327	200
100 000	4539	1520
1 000 000	61933	12359

Tabela 2. Rezultati dobijanja odgovora na upit sa uslovom u bazi podataka i u skladištu podataka, nad različitim brojem zapisa



Grafikon 2. Uporedna analiza dobijanja odgovora na upit sa uslovom u bazi podataka i u skladištu podataka, nad različitim brojem zapisa

Kao i u slučaju postavljanja običnog upita i za upit sa uslovom vreme odziva skladišta podataka bilo je znatno manje od vremena odziva baze podataka. Razlike su veće nad manjim brojem zapisa koje treba obraditi, a sa povećanjem broja zapisa, smanjuje se i razlika u vremenu odziva. Ipak u svim slučajevima skladište podataka je pokazalo daleko bolje performanse.

#### 4.3 Upiti sa order by

Korišćenjem ORDER BY klauzule moguće je sortirati rezultujuću tabelu po jednom ili više atributa u rastućem ili opadajućem redosledu. Za specifikaciju rastućeg redosleda koristi se klauzula ASC, a za specifikaciju opadajućeg redosleda klauzula DESC. Rastući redosled se podrazumeva, pa klauzulu ASC nije neophodno navoditi, za razliku od klauzule DESC koju uvek treba navesti kada se sortira u opadajućem redosledu. ORDER BY je uvek poslednja klauzula u SELECT bloku.

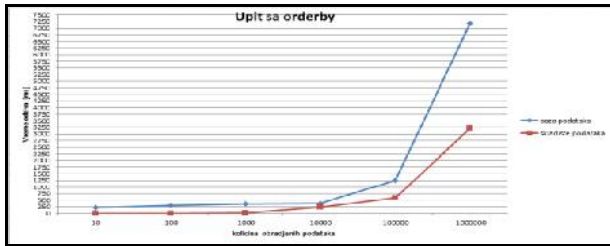
Nad bazom podataka i nad skladištem podataka postavljen je upit koji treba da vrati prezime i ime studenta, studijski program kojem pripada, naziv ispitnog roka, i broj desetki koje je student dobio u tom ispitnom roku, sortirano po prezimenu i imenu, broju desetki koje je dobio, studijskom programu kojem pripada i nazivu ispitnog roka, respektivno.

Merenjima vremena dobijanja odgovora na upit, po različitom broju zapisa, došlo se do sledećih rezultata:

broj podataka	vreme odziva[ms]	
	baza podataka	skladište podataka
10	220	2
100	303	3
1 000	359	10
10 000	377	247
100 000	1240	571
1 000 000	7182	3208

Tabela 3. Rezultati dobijanja odgovora na upit sa order by u bazi podataka i u skladištu podataka, nad različitim brojem zapisa





Grafikon 3. Uput sa orderby u bazi podataka i u skladištu podataka, nad različitim brojem zapisa

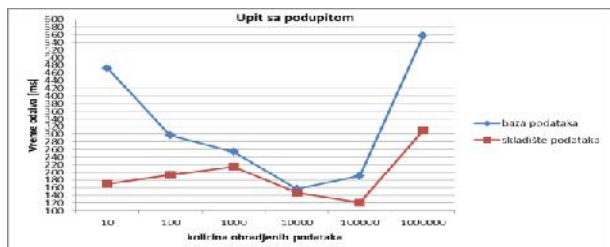
Za upit sa *ORDER BY* klauzulom nad bazom podataka i nad skladištem podataka do 10 000 zapisa, skladište podataka pokazalo je daleko bolje performanse. Nad 10 000 zapisa dobijen je odgovor na upite sa minimalnom razlikom. Nad 100 000 i nad 1 000 000 zapisa, skladište podataka je ponovo pokazalo bolje performanse, ali razlika je manja u odnosu na broj zapisa do 10 000.

#### 4.4 Upit sa podupitom

Jedan od načina realizacije upita nad više tabela je ulaganje upita nad jednom relacijom u upit nad drugom [5]. Upit koji se ulaže, odnosno upit koji je deo drugog upita, naziva se podupit, odnosno unutrašnji upit. Upit u koga se podupit ulaže naziva se spoljni upit. U implementiranom primeru korišćen je podupit koji kao rezultat vraća relaciju, i definisan je operater *NOT IN* koji testira da li se neka vrednost ne nalazi u skupu vrednosti. Nad bazom podataka i nad skladištem podataka postavljen je upit koji treba da vrati spisak predmeta, koje jos niko nije položio (ne nalaze se u evidenciji položenih ispita).

broj podataka	vreme odziva[ms]	
	baza podataka	skladište podataka
10	473	170
100	297	194
1 000	254	215
10 000	157	147
100 000	171	121
1 000 000	558	310

Tabela 4. Rezultati dobijanja odgovora na upit sa podupitom u bazi podataka i u skladištu podataka, nad različitim brojem zapisa



Grafikon 4. Uput sa podupitom u bazi podataka i u skladištu podataka, nad različitim brojem zapisa

Za upit sa podupitom nad bazom podataka i nad skladištem podataka do 1000 zapisa, skladište podataka pokazalo bolje performanse. Nad 10 000 zapisa dobijen je odgovor na upite gotovo istovremeno. Nad 100 000 i nad 1 000 000 zapisa, skladište podataka je ponovo pokazalo bolje performanse, ali razlika je manja u odnosu na broj zapisa do 1000.

## 5. ZAKLJUČAK

U svim slučajevima skladište podataka dalo je brže odgovor na postavljeni upit. Drastičnije razlike konstatovane su za obične upite i upite sa uslovom, a manje razlike za upite sa order by i upite sa podupitom. Razlike u performansama opadaju sa povećanjem broja zapisa.

Dalja istraživanja merenja performansi između baza podataka i skladišta podataka, mogu voditi u više pravaca. Jedan od pravaca je merenje performansi u savremenijim SUBP kao što su Microsoft SQL Server 2014 i Microsoft SQL Server 2016. Još jedan od mogućih pravaca daljeg istraživanja je analiza merenje performansi na server računaru koji ima bolje karakteristike po pitanju performansi u odnosu na klijentski računar, na kome je rađeno navedeno istraživanje i merenje.

## LITERATURA

- [1] Conn, S. S. (2005, April). OLTP and OLAP data integration: a review of feasible implementation methods and architectures for real time data analysis. In Proceedings. IEEE SoutheastCon, 2005. (pp. 515-520). IEEE.
- [2] Dewan, S., Aggarwal, Y., & Tanwar, S. (2014). Review on Data Warehouse, Data Mining and OLAP Technology: As Prerequisite aspect of business decision making activity.
- [3] Plattner, H. (2009, June). A common database approach for OLTP and OLAP using an in-memory column database. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data (pp. 1-2). ACM.
- [4] Antognini, C. (2014). SQL Optimization Techniques. In Troubleshooting Oracle Performance (pp. 359-418). Apress
- [5] Freedman, C., Ismert, E., & Larson, P. Å. (2014). Compilation in the Microsoft SQL Server Hekaton Engine. IEEE Data Eng. Bull., 37(1), 22-30.
- [6] Kimball R, The Data Warehouse Toolkit – Practical Techniques for Building Dimensional Data Warehouses, John Wiley & Sons, 1996. 16-17.



# GRADIJENTNA METODA ZA PROCENU USPEŠNOSTI SJEDINJAVANJA KOLOR I MONOHROMATSKIH SLIKA

## A GRADIENT METHOD FOR THE ASSESSMENT OF THE PERFORMANCE OF COLOR AND MONOCHROMATIC IMAGE FUSION

Rade Pavlović<sup>1</sup>, Vladimir Petrović<sup>2</sup>  
*Vojnotehnički institut, Ministarstvo odbrane Republike Srbije<sup>1</sup>*  
*Fakultet tehničkih nauka, Novi Sad<sup>2</sup>*

**Sadržaj** – U radu je dat pristup procene sjedinjavanja kolor i monohromatskih slika. Standardna metoda za procenu uspešnosti sjedinjavanja monohromatskih slika proširena je na procenu kolor sjedinjavanja. Metoda je zasnovana na proceni prenosa gradijenata iz ulaznih u sjedinjenu sliku. Metoda je testirana na bazi koja sadrži različite scenarije i pokazala usaglašenost sa subjektivnim testovima koji su izvedeni u okviru istraživanja.

**Abstract** - The paper presents an approach to assessing the fusion of color and monochromatic images. The standard method for assessing the success of the fusion of monochromatic images has been extended to estimate color fusion. The method is based on estimating the transfer of gradients from the input to the fused image. The method was tested on a database that contained different scenarios and showed compliance with subjective tests performed within the research.

### 1. UVOD

Napredni multisenzorski sistemi za osmatranje koriste više senzora kako bi poboljšali mogućnosti sistema za rad u različitim vremenskim uslovima, promena ciljeva i oblasti pretrage. Korišćenjem multisenzorskih sistema dobija se više informacija o sceni i objektima na njoj, ali samim tim postoji i veći broj podataka koje treba obraditi i proslediti krajnjem korisniku [1].

Multisenzorski sistemi koji koriste termovizijsku i televizijsku kameru daju informacije dobijene iz objekata koji zrače toplotnom energijom i refleksijom svetlosti. Termovizijska slika otkriva ciljeve koji imaju veći temperaturni kontrast i isto tako kamuflirane objekte [2]. Sa druge strane televizijska slika daje više visokofrekventnih informacija iz pozadine, koja je ključna u preciznom određivanju lokacije cilja i okoline. Termovizijska i televizijska slika mogu da daju informacije koje nisu zajedničke za obe jer temperaturna refleksija od objekata nije ista kao i refleksija svetlosti.

U početku razvoja algoritama za fuziju cilj je bilo sjedinjavanje monohromatskih slika u sjedinjenu sliku iz zadržavanje informacija iz ulaznih slika. Sjedinjavanjem ovih informacija povećava se kvalitet slike i samim tim i mogućnost lakšeg izvajanja ciljeva. Međutim, ako uzmemo činjenicu da ljudsko oko može da razlikuje najviše 100 nivoa sivog, rezultati dobijeni sjedinjavanjem monohromatskih slika mogu da budu veoma teški za interpretaciju a samim tim može doći i do smanjenja efekta

sjedinjavanja. Pošto ljudi mogu da razlikuju nekoliko hiljada boja definisanih kao promena intenziteta, zasićenja i osvetljenosti došlo je do razvoja algoritama za kolor mapiranje.

Međutim razvojem senzora i njihovom upotrebom u velikom broju primena dolazi do potrebe osmatranja i prikupljanja slika i videa u kolor formatu [3]. Samim time dolazi do pojave algoritama za sjedinjavanje kolor slika. Metode za sjedinjavanje kolor i monohromatskih slika zasnovane su na transformaciji kolor slike iz RGB kolor sistema u neki drugi kolor sistem (HSV, LAB,  $l\alpha\beta$ , ...) i zatim sjedinjavanju monohromatske slike sa jednim od kanala kolor slike [3]. Metoda za sjedinjavanje jednog od kolor kanala sa monohromatskom slikom je jedna od standardnih metoda za sjedinjavanje monohromatskih slika [4-6]. Uspešnost sjedinjavanja zavisi od izbora kolor sistema za sjedinjavanje i metode monohromatskog sjedinjavanja. Veći broj metoda koriste sjedinjavanje monohromatske slike sa kanalom koji predstavlja intenzitet piksela na kolor slici [7,8]. Mana ovih metoda može da bude gubitak kontrasta na sjedinjenoj slici i narušavanje prirodnog izgleda kolor slike.

Pored razvoja metoda za sjedinjavanje postoji i potreba za merama koje će da odrede uspešnost razvijenih algoritama. U poslednjih nekoliko godina samo je nekoliko algoritama za procenu uspešnosti kolor sjedinjavanja slika su razvijeni i u principu oni su ekstenzija već proverenih algoritama za monohromatske slike uključujući i kolor komponentu [9-11].

### 2. VIDEO SJEDINJAVANJE MULTISENZORSKIH SEKVENCI

Objektivna procena uspešnosti sjedinjavanja slika na bazi očuvanja ivica utemeljena je na poistovećivanju vizuelnih informacija sa ivicama ili gradijentnim informacijama u slici [12]. Opšteprihvatarena činjenica je da čulo vida raspoznaje samo promene na slici. To znači da se informacije prenose promenama pre nego apsolutnim vrednostima. Uzimajući to u obzir, cilj sjedinjavanja slika se može definisati kao prenos svih ivičnih informacija iz ulaznih u sjedinjenu sliku. Savršeno sjedinjavanje slika sadrži sve ivice koje se pojavljuju i u ulaznim slikama. Ivice se u ovom kontekstu, odnose na bilo koje promene vrednosti signala slike, poznate kao gradijent slike.

Algoritam izdvaja vizuelne informacije definisanjem parametara jačine i orijentacije ivice za svaki piksel slike. Oni se dobijaju jednostavnim Sobel operatorom, koji definišu dva 3x3 prozora. Ovi prozori mere vodoravnu i

uspravnu komponentu ivice u centralnom pikselu. Pri proceni sjedinjavanja sve tri slike:  $A$ ,  $B$  i  $F$  filtriraju se Sobel prozorima što za svaku daje još po dve slike  $s^x$  i  $s^y$  koje sadrže njihove ivične komponente u  $x$  i  $y$ -pravcu. Iz ovih komponenti jačina  $g(m,n)$  i orjentacija  $a(m,n)$  ivice dobijaju se prema jednačinama:

$$g_a(m,n) = \sqrt{s_A^x(m,n)^2 + s_A^y(m,n)^2} \quad (1)$$

$$\alpha_A(m,n) = \tan^{-1}\left(\frac{s_A^x(m,n)}{s_A^y(m,n)}\right) \quad (2)$$

gde je  $1 \leq m \leq M$  i  $1 \leq n \leq N$ , a  $M$  i  $N$  su dimenzije slika. Rasponi vrednosti jačine i orjentacije zavise od parametara normalizacije Sobelovog filtriranja i opsega  $\arctan$  funkcije.

Bilo kakav gubitak ivičnih informacija se manifestuje kroz promenu jednog ili oba ova parametra. Ovdje treba voditi računa da čulo vida ne obrađuje sve ivice podjednako. Ivice koje se ne uoče moraju se tretirati drugačije od onih koje privuku pažnju posmatrača. Informacije izdvojene iz ulaznih i sjedinjene slike nalaze se u mapama jačine i orjentacije ivica,  $[g_A(m,n), \alpha_A(m,n)]$ ,  $[g_B(m,n), \alpha_B(m,n)]$ ,  $[g_F(m,n), \alpha_F(m,n)]$ . Isprva se u obliku nezavisnih parametara  $G^{AF}$  i  $A^{AF}$  određuju promene jačine i orjentacije prema jednačinama:

$$G^{AF}(m,n) = \begin{cases} \frac{g_F(m,n)}{g_A(m,n)}, & g_A(m,n) > g_F(m,n) \\ \frac{g_A(m,n)}{g_F(m,n)}, & \text{u protivnom} \end{cases}$$

$$A^{AF}(m,n) = \frac{|\alpha_A(m,n) - \alpha_F(m,n)| - \pi/2}{\pi/2} \quad (3)$$

Kada je ulazna ivica jača od sjedinjene  $G^{AF}$  je odnos između ulazne i sjedinjene jačine (gubitak kontrasta). U suprotnom, pojačanje kontrasta je isto gubitak, odnos je obrnut, jer pojačanje kontrasta nije cilj sjedinjavanja i tretira se kao izobličenje. Izobličenja pojačanja su čest uzrok pojačanja jačine ivica. Parametar  $G^{AF}$  je 1 kada su sjedinjena i ulazna ivica iste jačine i opada linearno sa povećanjem razlike između ove dve vrednosti.

Parametri  $G^{AF}$  i  $A^{AF}$  linearno opisuju gubitak informacija prouzrokovan promenom jačine i orjentacije ivica. Reakcije bioloških sistema na različite vrste stimulusa su veoma nelinearne. Stoga se pravi gubitak informacija modeluje sigmoidnim funkcijama promene ivične jačine i orjentacije. Ove funkcije daju mere održanja ivičnih parametara  $Q_g^{AF}(m,n)$  i  $Q_\alpha^{AF}(m,n)$  prema jednačinama:

$$Q_g^{AF}(m,n) = \frac{\Gamma_g}{1 + e^{k_g(G^{AF}(m,n) - \sigma_g)}} \quad (4)$$

$$Q_\alpha^{AF}(m,n) = \frac{\Gamma_\alpha}{1 + e^{k_\alpha(A^{AF}(m,n) - \sigma_\alpha)}} \quad (5)$$

Konstante  $k_g$ ,  $\sigma_g$  i  $k_\alpha$ ,  $\sigma_\alpha$  određuju konačni oblik sigmoidnih funkcija i dobijaju se optimizacijom algoritma mere.  $\Gamma_g$  i  $\Gamma_\alpha$  osiguravaju da funkcije budu 1 kada su  $G^{AF}$  i  $A^{AF} = 1$ .

Jedinstvena mera održanja ivičnih informacija sa lokacije  $(m,n)$  ulazne slike  $A$  na odgovarajućoj lokaciji u

sjedinjenoj slici  $F$ ,  $Q^{AF}$  dobija se kao geometrijska sredina parametara održanja jačine i orjentacije  $Q_g^{AF}$  i  $Q_\alpha^{AF}$ :

$$Q^{AF}(m,n) = \sqrt{Q_g^{AF}(m,n) Q_\alpha^{AF}(m,n)} \quad (6)$$

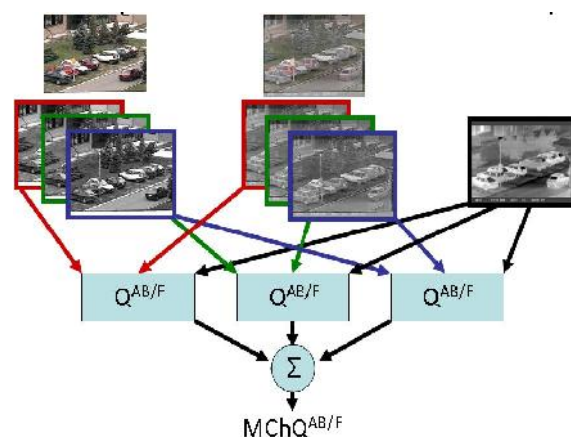
Poput  $Q_g^{AF}$  i  $Q_\alpha^{AF}$ ,  $Q^{AF}$  je takođe u opsegu od 0 do 1, gde ekstremne vrednosti i dalje imaju isto značenje. Ova procedura se primenjuje u celosti samo na uočljive gradijente.

Određivanje raspodele subjektivnog značaja dobijamo mape značaja za obe ulazne slike,  $w_A(m,n)$  i  $w_B(m,n)$ . Sveukupna uspešnost sjedinjavanja slika  $A$  i  $B$  u sliku  $F$ ,  $Q^{AB/F}$  se onda dobija moduliranim zbirom koeficijenata održanja ivica iz celog prizora.

### 3. GRADIJENTI KAO MERA ZA KOLOR SJEDINJAVANJE

Informacije koje nose kolor komponente u slici su od velikog značaja i njihova degradacija u procesu sjedinjavanja može dovesti do pojave neprirodnih objekata i same scene, što bi učinilo proces neprihvatljivim. U tom smislu od vitalnog značaja za algoritam za kolor sjedinjavanje je i njihovo zadržavanje u što većoj meri, a sam tim se i meri uspešnost svakog algoritma. Za proračun uspešnosti kolor sjedinjavanja važno je uzeti u razmatranje strukturu prenesenu iz ulaznih slika i prirodnost boja ili boje u zavisnosti od broja kolor ulaznih slika. Očuvanje gradijentnih informacija kao jedan od osnovnih modela za procenu uspešnosti sjedinjavanja monohromatskih slika može se proširiti i na kolor sjedinjavanje. Predstavljena je mera koja koristi kolor informacije iz ulazne i sjedinjene slike i zajedno sa očuvanjem strukturalnih informacija daje meru za procenu kolor sjedinjavanja.

Predloženi način u ovom radu je da se izračuna uspešnost prirodnog kolor sjedinjavanja primenom algoritma za očuvanje gradijenata monohromatskih slika za svaki kanal nezavisno u RGB kolor sistemu. Zatim se rezultati svakog kanala pojedinačno koriste za dobijanje jedinstvene mere za kolor sjedinjavanje (slika 1).



Slika 1. Mera za procenu uspešnosti kolor sjedinjavanja.

Monohromatska mera  $Q^{AB/F}$  računa se za svaki kanal ulazne kolor slike, monohromatske i kanala sjedinjene slike. Na taj način dobijaju se tri odvojene mere za procenu

uspešnosti sjedinjavanja, tj.:  $Q_R^{AB/F}$ ,  $Q_G^{AB/F}$  i  $Q_B^{AB/F}$  za svaki od R, G i B kolor kanala.

Proračuni koji se dobijaju za svaki kanal posebno mogu se jednostavno sabrati uz odgovarajuće težinske koeficijente i na taj način dobiti jedinstvenu meru za proračun sjedinjavanja kolor slika, odnosno multikanalnu  $Q^{AB/F}$ , odnosno  $MChQ^{AB/F}$ :

$$MChQ^{AB/F} = k_R Q_R^{A_B/F_R} + k_G Q_G^{A_G/B/F_G} + k_B Q_B^{A_B/F_B} \quad (7)$$

MChQAB/F proračunava očuvanje monohromatske strukture i kolor informacija u sjedinjenoj kolor slici kroz sva tri kolor kanala. Promene u boji sjedinjene slike i ulazne slike biće prikazano kroz jedan ili više kanala, što će doprineti smanjenju vrednosti u nekoj od komponenti QAB/F. Isto tako promene u intenzitetu biće prikazane kroz sva tri kanala kroz smanjenje u merama po kanalima indiciraće i smanjenje zajedničke mere MChQ<sup>AB/F</sup>.

Koristeći težinske faktore može se uticati na važnost mere po svakom kanalu i samim tim i na važnosti očuvanja svake od boja. Koristeći se iskustvima i odzivu ljudskog vizuelnog sistema može se doći do zaključka za vrednosti težinskih koeficijenata za proračun jedinstvene mere:  $[k_R, k_G, k_B] = [0.3, 0.59, 0.11]$ .

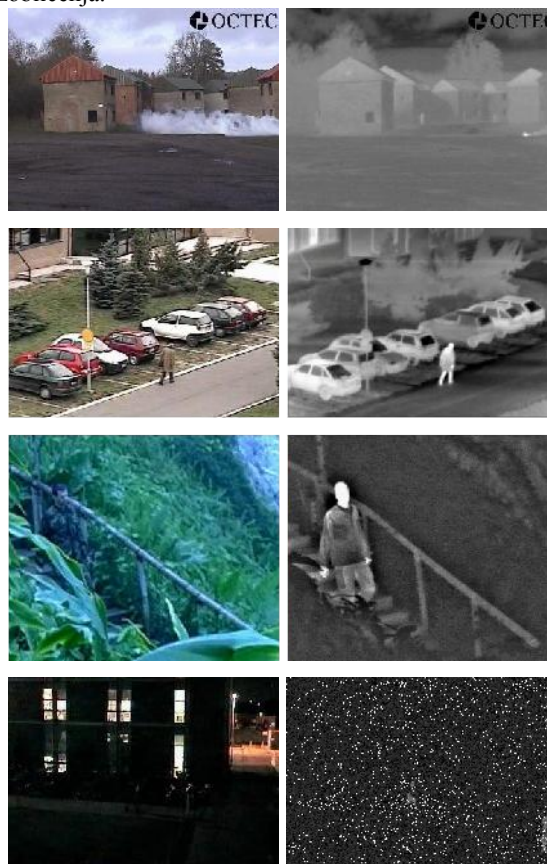
#### 4. ANALIZA REZULTATA

Za analizu mere za procenu uspešnosti sjedinjavanja kolor slika napravljena je baza od 4 različita multisenzorska scenarija (televizijska i termovizijska slika) sa po 3 slike za svaki scenario (slika 2). Baza obuhvata urbane i ruralne scenarije i različite primene sjedinjavanja kolor televizijskih i monohromatskih termovizijskih slika. Prva grupa slika (gornji red) predstavlja realnu situaciju vojnog manevra u urbanoj sredini. Termovizijska slika pokazuje objekte koji nisu vidljivi na televizijskoj slici i postoje informacije koje se ne preklapaju. Drugi red slika je iz gradske sekvence i objekti na obe slike su uočljivi i postoje preklapanja. Treći red slika su iz ruralnog područja, dok poslednji red predstavlja slike u uslovima smanjene vidljivosti sa uličnim svetlom i sa visokim nivoom šuma.

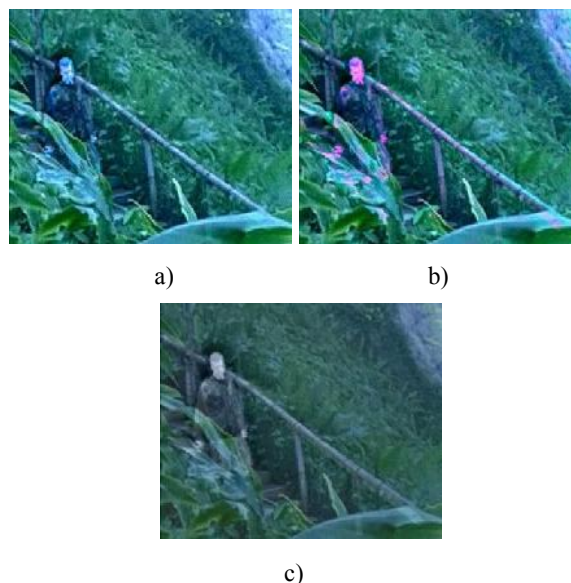
Rezultati mere testirani su na tri različite metode za kolor sjedinjavanje slika. Prva metoda je sjedinjavanje kanala intenziteta kolor slike transformisane u HSV kolor sistem (HSV) [13], druga metoda je sjedinjavanje koristeći  $\alpha\beta$  kolor sistem i sjedinjavanje monohromatske slike sa  $\beta$  kanalom ( $\beta$ ) [14] i treća je metoda jednostavnog aritmetičkog sjedinjavanja (aritm). Sjedinjenje slike za ulaznu bazu sa pomenutim metodama date su na slici 3.

U okviru istraživanja i analize rezultata izvedeni su subjektivni testovi na bazi kolor slika kako bi se uporedili rezultati mera za kolor sjedinjavanje. Ukupno 10 iskusnih posmatrača, radilo je neformalne testove na već spomenutim sekvencama i metodama. Pre početka rada svakom posmatraču je ukratko objašnjena namena testova i šta se očekuje od njih. Testovi su rađeni na 27" ekranu sa HD rezolucijom i organizovani su da se u gornjem redu prikazuju ulazne kolor i monohromatska slika, dok se u donjem redu prikazuju po tri sjedinjene slike sa slučajnim i različitim rasporedom kako bi se izbegla pristrasnost

(slika 4). Raspored ocena je bio od 0 do 5 sa korakom od 0,1, gde 0 predstavlja totalni gubitak informacija, a 5 idealno sjedinjavanje sa prenetim svim informacijama i bez izobličenja.

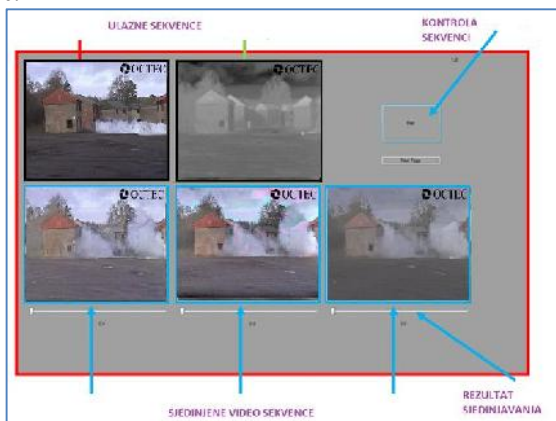


Slika 2. Baza multisenzorskih slika za sjedinjavanje i procenu uspešnosti sjedinjavanja



Slika 3. Rezultati kolor sjedinjavanja a) HSV metodom, b) sjedinjavanjem u  $\beta$  kolor kanalu i c) aritmetičko sjedinjavanje

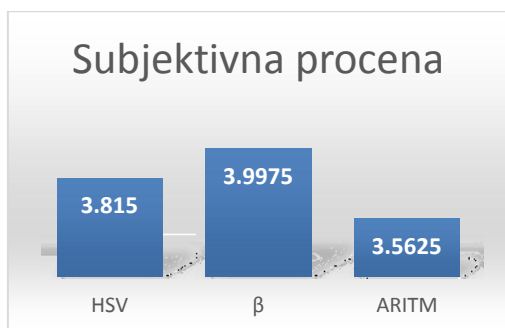
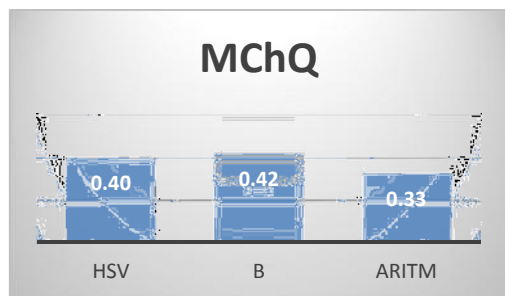
Rezultati objektivne mere i subjektivnih testova dati su u tabeli 1 i na dijagramu na slici 5. Uočava se da mera za procenu kolor sjedinjavanja rangira metode po sledećem: najuspešnije je sjedinjavanje  $\beta$  kanalom, zatim HSV kolor sjedinjavanje i na kraju metoda aritmetičkog sjedinjavanja. Treba napomenuti da je polazna gradijentna mera Q veoma osetljiva i da mala razlika u rezultatu može pokazati već značajno poboljšanje kvaliteta sjedinjavanja. U ovom slučaju to je odnos prve dve rangirane mere u korist sjedinjavanja u  $\beta$  kanalu, što potvrđuje cilj ove metode da se zadrži prirodnost kolor slike [14]. Metoda aritmetičkog usrednjavanja daje najlošije rezultate, što se vidi i sa slike 3c.



Slika 4. Vizuelni prikaz stranice za subjektivnu procenu uspešnosti sjedinjavanja.

Tabela 1. Rezultati objektivne mere i subjektivnih testova

	HSV	$\beta$	ARITM
<b>MChQ</b>	0.4025	0.42	0.3275
<b>Subjekt</b>	3.81	4.00	3.56



Slika 5. Grafički prikaz objektivnih i subjektivnih testova za sjedinjavanje kolor slika.

Rezultati subjektivnih testova pokazuju  $\beta$  metodu kao najpribližniju ispitanim subjektima po kvalitetu sjedinjavanja (prenete informacije i očuvana prirodnost), zatim HSV sjedinjavanje i kao najlošije aritmetičko sjedinjavanje. Poređenjem rezultata subjektivnih testova i objektivne mere vidi se da su po rangiranju metoda i da daju približno isti odnos za prve dve metode. Veću vrednost subjekti su jedino dali aritmetičkoj metode u odnosu na meru.

## 5. ZAKLJUČAK

Multisenzorsko osmatranje uzima sve veći značaj u velikom broju sistema kao što su besposadne letelice, borbena vozila, stacionarni sistemi osmatranja i drugo. Zbog povećanja broja senzora koje svaki od ovih sistema sadrži potrebno je izvršiti fuziju podataka kako bi se na što jednostavniji način i bez opterećenja posmatrača mogli prikazati. Sjedinjavanje slike sa kolor televizijske i monohromatske termovizijske kamere sve je zastupljenije u istraživanju i razvoju novih algoritama. Problem predstavlja složenost kolor slike, gde promene u bilo kom kanalu utiču na kompletan rezultat i dolazi do narušavanja prirodnosti slike.

Relativno mali broj metoda za procenu uspešnosti sjedinjavanja kolor slika je razvijen. Najčešće su to metode koje se oslanjaju na već postojeće metode za monohromatsko sjedinjavanje slika. U ovom radu je uzeta već proverena i ispitana metoda zasnovana na prenosu gradijenata iz ulaznih slika u sjedinjenu. Metoda razmatra sva tri kanala RGB kolor sistema i sa težinskim koeficijentima njihov zbir daje konačnu metodu za kolor procenu. Rezultati mere provereni su i sa subjektivnim testovima i pokazali su visoku korelaciju na bazi koja je korišćena u ovom radu.

## LITERATURA

- [1] Petrović V., Zrnić B., "Multisenzorsko sjedinjavanje informacija za otkrivanje, praćenje i identifikaciju ciljeva", TELFOR 2001, Beograd
- [2] Christinal, J., Jemima Jebaseeli T. "A survey on color image fusion for multi sensor night vision image." J. Adv. Res. Comput. Eng. Technol1.9 (2012): 151-155.
- [3] Xiuqiong Z., Qingli C., Tao M., "Comparison of fusion methods for the infrared and color visible images," iccsit, pp.421-424, 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009.
- [4] Burt P, Adelson E, "The Laplacian pyramid as a compact image code", IEEE Transactions on Communication, COM-31,1983, str. 532-540
- [5] Toet A., "Image fusion by a ratio of low-pass pyramid", Pattern Recognition Letters 9 North-Holland (1989) str. 245-253,
- [6] Petrović V., Xydeas C., "Computationally efficient pixel-level image fusion", Proceedings of

Eurofusion99, Stanford-upon-Avon, October 1999, str. 177-184

[7] Huang M., Leng J., Xiang C., "A study on IHS+WT and HSV+WT method for image fusion," in Proc. of International Symposium on Information Science and Engineering, Vol. 1, pp. 665-668, 2008.

[8] Kriesel M., Gat N., "True-color night vision (TCNV) fusion system using a VNIR EMCCD and a LWIR microbolometer camera", Signal Processing, Sensor Fusion, and Target Recognition XIX. Edited by Kadar, Ivan. Proceedings of the SPIE, Volume 7697, pp. 76970Z-76970Z-8 (2010).

[9] Tsagaris V., Anastassopoulos V., "Global measure for assessing image fusion methods," Optical Engineering 45(2), February 2006.

[10] Tsagaris V., "Objective evaluation of color image fusion methods," Optical Engineering 48(6), June 2009.

[11] Yuan Y., Zhang J., Chang B., Han Y., "Objective quality evaluation of visible and infrared color fusion image," Optical Engineering 50(3), March 2011.

[12] Petrović V., Xydeas C., "Objective evaluation of signal-level image fusion performance," Optical Engineering 44(8), August 2005

[13] Huang M., Leng J., Xiang C., "A study on IHS+WT and HSV+WT method for image fusion," in Proc. of International Symposium on Information Science and Engineering, Vol. 1, pp. 665-668, 2008.

[14] Pavlović, R., Petrović, V., Bondžulić, B., Fusion of Colour and Monochromatic Images with Chromacity Preservation, 15th International Conference on Information Fusion, Raffles City Convention Centre, Singapore, 9-12 July, 2012. On page(s): 1963-1969,



# ANALIZA PERFORMANSI PID REGULATORA SA FILTRIMA ŠUMA MERENJA

## PERFORMANCE ANALYSIS OF PID CONTROLLERS WITH MEASUREMENT NOISE FILTERS

Nikola Savkić<sup>1</sup>, Momir Stanković<sup>2</sup> i Stojadin Manojlović<sup>2</sup>

*Vojska Srbije<sup>1</sup>*

*Univerzitet odbrane u Beogradu, Vojna akademija<sup>2</sup>*

*Sadržaj – U radu su analizirane performanse, robusnost i osetljivost na šum merenja sistema upravljanja sa različitim strukturama PID regulatora. Opisane su modifikovane forme PID regulatora namenjene za smanjenje osetljivosti sistema na šum merenja, a stepen degradacije performansi i robusnosti koji one unose opisan je u frekvencijskom domenu. Definisane su prednosti i mane određenih struktura regulatora i izvršena je simulaciona verifikacija rezultata na sistemima sa regulatorima u diskretnoj formi u prisustvu mernog šuma na izlazu sistema.*

*Abstract – In this paper the different PID structures with filtered measurement noise are described, and the sensitivity to measurement noise, robustness and performances are analysed in the frequency domain. The main advantages and disadvantages of controllers are defined, and the results are confirmed with simulation of controllers in the discrete form.*

### 1. UVOD

Savremeni sistemi automatskog upravljanja zahtevaju primenu upravljačkih algoritama koji obezbeđuju visoke performanse u pogledu praćenja zadatih referentnih signala i potiskivanja različitih vrsta poremećaja, uz postojanje zadovoljavajuće robusnosti sistema. Pored toga, sa aspekta praktične industrijske primene, dodatni izazov predstavlja minimizacija složenosti algoritma upravljanja i što jednostavnija hardverska realizacija. Uprkos razvoju savremenih upravljačkih tehnika sa visokim performansama, kao što su optimalno, robusno, adaptivno i inteligentno upravljanje, njihova primena je često ograničena složnošću hardverske realizacije i/ili zahtevima za poznavanjem tačnog modela procesa kojim se upravlja. Shodno tome, preko 90% industrijskih upravljačkih sistema i dalje se oslanja na primenu konvencionalnih proporcionalno-integralno-diferencijalnih (PID) regulatora, pre svega zbog njihove pogodnosti za praktičnu realizaciju i malog broja parametara za podešavanje [1].

Jedan od nedostataka osnovne strukture PID regulatora je osetljivost na šum merenja, usled diferencijalnog dejstva regulatora. U cilju smanjenja uticaja šuma merenja u literaturi se mogu naći različite modifikovane strukture PID regulatora, koje najčešće podrazumevaju ugradnju filtera u strukturu regulatora, i to serijski sa celokupnom strukturom PID-a ili samo sa diferencijalnim dejstvom [2]. Međutim, primena ovakvih struktura PID regulatora dovodi do neželjenih degradacija performansi i robusnosti sistema upravljanja.

U ovom radu je sprovedena detaljna analiza performansi, robusnosti i osetljivosti na šum merenja sistema upravljanja baziranih na različitim strukturama PID regulatora. Ocena performansi sistema razmatrana je na osnovu efikasnosti potiskivanja spoljašnjeg poremećaja, dok su se kao mere robusnosti koristile margine stabilnosti. Analiza osetljivosti na šum merenja je sprovedna na osnovu odgovarajućih funkcija osetljivosti. Dobijeni rezultati su verifikovani kroz simulacionu analizu sa diskretizovanim modelima regulatora u prisustvu šuma merenja na izlazu sistema.

### 2. STRUKTURA PID REGULATORA

Osnovna struktura PID regulatora u vremenskom domenu definisana je jednačinom:

$$u(t) = k_p \cdot e(t) + k_i \cdot \int_0^t e(\tau) \cdot d\tau + k_d \cdot \frac{d}{dt} e(t) \quad (1)$$

gde su  $u(t)$  upravljački signal,  $e(t) = r(t) - y(t)$  greška koja predstavlja odstupanje referentnog signala  $r(t)$  od izlaza sistema  $y(t)$ , dok su  $k_p$ ,  $k_i$  i  $k_d$  proporcionalno, integralno i diferencijalno pojačanje respektivno. Primenom Laplasove transformacije na (1) dobijao strukturu PID regulatora u kompleksnom domenu [3]:

$$G_c(s) = k_p + \frac{k_i}{s} + k_d s \quad (2)$$

Osnovni nedostatak ovakve forme PID regulatora je velika osetljivost na šum merenja, usled uticaja diferencijalnog dejstva. Zbog toga se u praktičnoj primeni najčešće koriste modifikovane strukture PID-a [4], u kojim se filtrira izlaz regulatora:

$$G_c(s) = \frac{k_p + \frac{k_i}{s} + k_d s}{(T_f s + 1)^n}, \quad (3)$$

ili samo diferencijalno dejstvo regulatora:

$$G_c(s) = k_p + \frac{k_i}{s} + k_d s \frac{1}{(T_f s + 1)^n}. \quad (4)$$

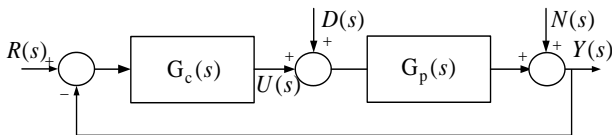
pri čemu je filter definisan vremenskom konstantom  $T_f$  i redom filtra  $n$ . Najčešće se primenjuju filteri prvog i drugog reda, imajući u vidu da sa porastom  $n$  dolazi do povećanja složenosti algoritma, kao i do smanjenja robusnosti sistema, što će biti detaljno analizirano u

narednom poglavlju rada.

### 3. FREKVENCIJSKA ANALIZA SISTEMA SA RAZLIČITIM STRUKTURAMA PID REGULATORA

U ovom poglavlju je sprovedena frekvencijska analiza performansi, robusnosti i osetljivosti na šum merenja sistema sa različitim PID regulatorima. Uporedjene su karakteristike sistema sa regulatorom (2) (u daljem tekstu označena kao PID), regulatorom (3) sa filtrima prvog i drugog reda (u daljem tekstu označeni kao PID<sub>1</sub> i PID<sub>2</sub>, respektivno) i strukturom regulatora (4) takodje sa filtrom prvog i drugog reda (u daljem tekstu označene kao PID<sub>1D</sub> i PID<sub>2D</sub>, respektivno).

Blok šema sistema upravljanja sa PID regulatorom prikazana je na Slici 1:



Slika 1. Blok šema sistema upravljanja sa PID regulatorom

gde su  $R(s)$ ,  $U(s)$ ,  $D(s)$ ,  $N(s)$  i  $Y(s)$  kompleksni likovi, referentnog signala, upravljačkog signala, signala spoljašnjeg poremećaja, šuma merenja i izlaza sistema, respektivno, dok  $G_p(s)$  predstavlja funkciju prenosa procesa kojim se upravlja. Analiza karakteristika u konkretnom slučaju je izvršena na tri karakteristična procesa:

$$G_{p1}(s) = \frac{1}{s(s+1)}, \quad (5)$$

$$G_{p2}(s) = \frac{1}{(s+1)^4}, \quad (6)$$

$$G_{p3}(s) = \frac{e^{-5s}}{(s+1)^3}. \quad (7)$$

Parametri razmatranih struktura PID regulatora su za procese (6) i (7) podešeni na osnovu optimalne metode podešavanja predložene u [5], dok su parametri regulatora za proces (5) podešeni pomoću *PID\_controller* alata programskog paketa MATLAB. Vrednosti parametara za sva tri slučaja su date u Tabeli I.

TABELA I  
PARAMETRI REGULATORA ZA RAZLIČITE PROCESSE

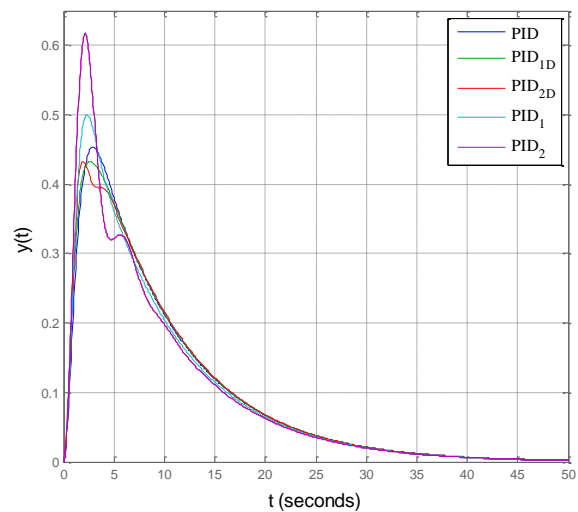
Proces	$k_p$	$k_i$	$k_d$	$T_f$
$G_{p1}(s)$	2	0.2	1.4	0.3
$G_{p2}(s)$	1.836	0.732	2.22	0.0198
$G_{p3}(s)$	0.512	0.129	1.008	0.2747

### 3.1 Analiza performansi sistema

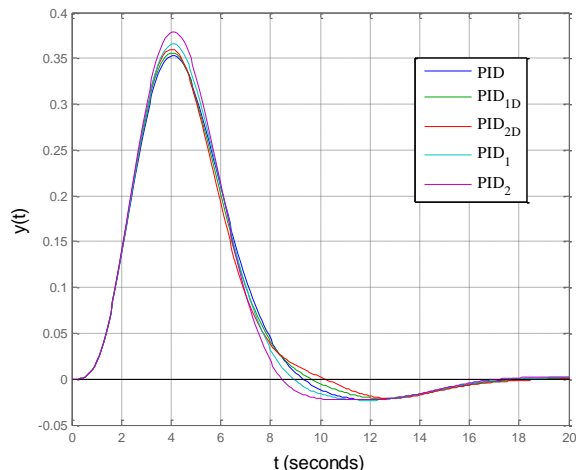
Kao kriterijum za ocenu performansi razmatrana je efikasnost potiskivanja odskočnog poremećaja  $D(s)$ . Shodno tome, za sistem prikazan na Slici 2. proračunata je funkcija prenosa od poremećaja do izlaza:

$$G_{dy}(s) = \frac{Y(s)}{D(s)} = \frac{G_p(s)}{1 + G_p(s)G_c(s)} \quad (8)$$

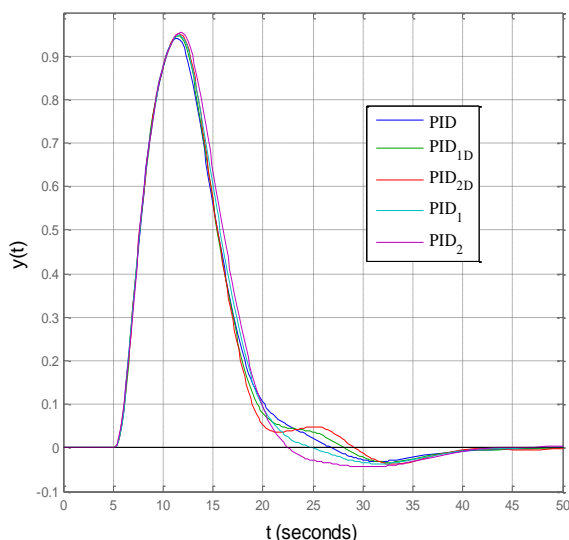
pri čemu su  $R(s) = 0$  i  $N(s) = 0$ . Na osnovu funkcije (8) dobijeni su odzivi sistema na jedinični odskočni poremećaj, koji su prikazani na slici 2., slici 3. i slici 4., za procese  $G_{p1}(s)$ ,  $G_{p2}(s)$  i  $G_{p3}(s)$ , respektivno.



Slika 2-Odzvi sistema sa različitim strukturama PID regulatora na odskočni poremećaj za proces  $G_{p1}(s)$



Slika 3-Odzvi sistema sa različitim strukturama PID regulatora na odskočni poremećaj za proces  $G_{p2}(s)$



Slika 4-Odzvi sistema sa različitim strukturama PID regulatora na odskočni poremećaj za proces  $G_{p3}(s)$

Da bi smo kvantitativno opisali odzive sistema, za svaki od njih je proračunat IAE (*Integral of the Absolute Error*) definisan kao:

$$IAE = \int_0^t |y(t)| dt \quad (9)$$

i dati su u Tabeli II:

TABELA II  
IAE ZA RAZLIČITE STRUKTURE PID REGULATORA

Struktura regulator	IAE		
	$G_{p1}(s)$	$G_{p2}(s)$	$G_{p3}(s)$
PID	4.982	1.58	8.30
PID <sub>1D</sub>	4.982	1.55	8.28
PID <sub>2D</sub>	4.982	1.54	8.27
PID <sub>1</sub>	4.982	1.60	8.47
PID <sub>2</sub>	4.982	1.62	8.81

Na osnovu rezultata iz Tabele II možemo zaključiti da za procese  $G_{p2}(s)$  i  $G_{p3}(s)$ , strukture sa filtriranim diferencijalnim dejstvom (PID<sub>1D</sub> i PID<sub>2D</sub>) bolje potiskuju poremećaj od osnovne strukture PID regulatora, te da se sa porastom reda filtra smanjuje IAE. Strukture sa filtriranim izlazom regulatora (PID<sub>1</sub> i PID<sub>2</sub>) ostvaruju lošije potiskivanje poremećaja, i sa povećanjem reda filtra raste i IAE. U slučaju procesa  $G_{p1}(s)$  IAE je isti za sve strukture jer je proces sa astatizmom prvog reda.

### 3.2 Analiza robusnosti

Analiza robusnosti je sprovedena na osnovu margina stabilnosti sistema: preteka pojačanja  $d$  i preteka faze  $\Phi_{pf}$ . Margine stabilnosti su proračunate na osnovu Nikvistovog dijagrama za funkciju povratnog prenosa sistema:

$$W(s) = G_c(s)G_p(s) \quad (10)$$

Vrednosti amplitudske i fazne rezerve stabilnosti date su u Tabeli 2.

TABELA II  
AMPLITUDSKA I FAZNA REZERVA STABILNOSTI

	$G_{p1}(s)$		$G_{p2}(s)$		$G_{p3}(s)$	
	$d$	$\Phi_{pf}$	$d$	$\Phi_{pf}$	$d$	$\Phi_{pf}$
PID	$\infty$	78.4	12.8	59.8	7.75	61.9
PID <sub>1D</sub>	$\infty$	60.8	10.4	58.4	6.99	62
PID <sub>2D</sub>	15.4	43.4	8.71	56.3	6.33	62.2
PID <sub>1</sub>	$\infty$	54.6	10.8	56.7	7.74	59.9
PID <sub>2</sub>	11	33.4	9.35	53.6	7.67	57.9

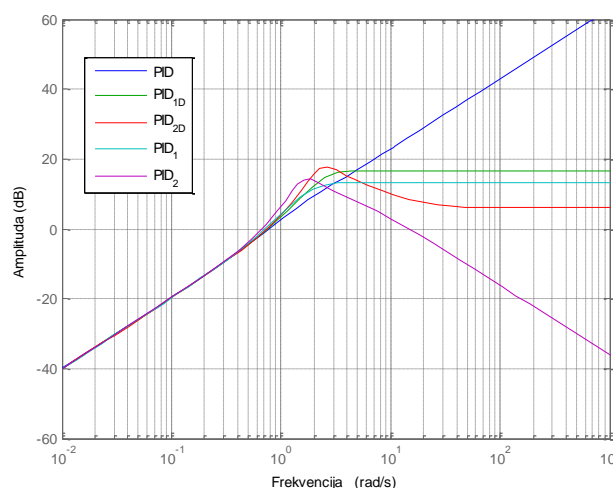
Može se uočiti da osnovna struktura PID regulatora poseduje najveće rezerve stabilnosti, što je očekivano, dok od modifikovanih struktura neznatno bolju robusnost ima struktura u kojoj se filtrira celokupni izlaz regulatora. Takođe, vidi se da se sa povećanjem reda filtera, smanjuju margine stabilnosti.

### 3.3 Analiza uticaja šuma merenja

Analiza uticaja šuma merenja je sprovedena na osnovu funkcije osetljivosti sistema na šum merenja (*noise sensitivity function*), koja je definisana kao [1]:

$$G_{un}(s) = \frac{U(s)}{N(s)} = \frac{G_c(s)}{1 + G_c(s)G_p(s)} \quad (11)$$

Frekvencijski odzivi funkcije (11) za različite strukture PID regulatora prikazani su na Slici 5, i to samo za proces  $G_{p1}(s)$ , imajući u vidu da se i za ostala dva procesa dobijaju slični rezultati.



Slika 5. Amplitudske karakteristike funkcije osetljivosti sistema na šum merenja

Imajući u vidu da je šum merenja visokofrekventni signal, jasno se uočava velika osetljivost na šum osnovne strukture PID regulatora, jer je nagib karakteristike na

visokim učestanostima +20 dB po dekadi. Kod struktura kod kojih se filtrira diferencijalno dejstvo PID<sub>1D</sub>, PID<sub>2D</sub> nagib je konstantan, i sa povećanjem reda filtera se smanjuje, dok kod struktura sa filtriranim izlazom regulatora, nagib karakteristike opada sa  $-(n-1) \cdot 20$  dB po dekadi. Može se zaključiti da najbolje performanse u potiskivanju šuma poseduje PID<sub>2</sub> regulator kod koga karakteristika  $G_{un}(s)$  na visokim učestanostima opada 20 dB po dekadi.

#### 4. SIMULACIONA ANALIZA

Simulaciona analiza je sprovedena sa diskretnim modelima razmatranih PID regulatora u prisustvu šuma merenja na izlazu sistema. Primenom Ojlerovog metoda diferenciranja unazad [6], dobijaju se diskretne forme regulatora:

standardni PID

$$u(k) = u(k-1) + (k_p + k_i \cdot T_s + \frac{k_d}{T_s})e(k) + (-k_p - \frac{2 \cdot k_d}{T_s})e(k-1) + \frac{k_d}{T_s}e(k-2), \quad (12)$$

PID<sub>1D</sub> i PID<sub>2D</sub>

$$u(k) = u(k-1) + (k_p + k_i \cdot T_s)e(k) + (-k_p)e(k-1) + \frac{k_d}{T_s}(p_n(k) + p_n(k-2)) + (-2 \cdot \frac{k_d}{T_s})p_n(k-1), \quad (13)$$

PID<sub>1</sub> i PID<sub>2</sub>

$$u(k) = [u(k-1) + (k_p + k_i \cdot T_s + \frac{k_d}{T_s})e(k) + (-k_p - \frac{2 \cdot k_d}{T_s})e(k-1) + \frac{k_d}{T_s}e(k-2)] \cdot p_n(k), \quad (14)$$

gde je  $T_s$  perioda odabiranja. NF filter je predstavljen sa  $p_n(k)$  i za  $n=1$  se dobija:

$$p_1(k) = \frac{T_f}{T_f + T_s} p_1(k-1) + \frac{T_s}{T_f + T_s} e(k), \quad (15)$$

dok je za  $n=2$ :

$$p_2(k) = \frac{2 \cdot T_f (T_s + 1)}{T_s^2 + 2 \cdot T_f \cdot T_s + T_f^2} p_2(k-1) - \frac{T_f}{T_s^2 + 2 \cdot T_f \cdot T_s + T_f^2} p_2(k-2) + \frac{T_s^2}{T_s^2 + 2 \cdot T_f \cdot T_s + T_f^2} e(k). \quad (16)$$

Simulaciona analiza je sprovedena na modelu troosne platforme didaktičkog radara, odnosno modelu kretanja

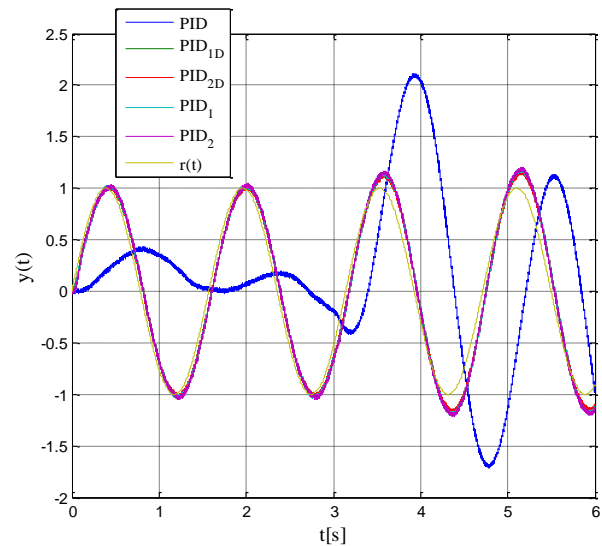
platforme po osi azimuta koji je opisan funkcijom prenosa [7]:

$$G_p(s) = \frac{6.75}{s(s+11)}. \quad (17)$$

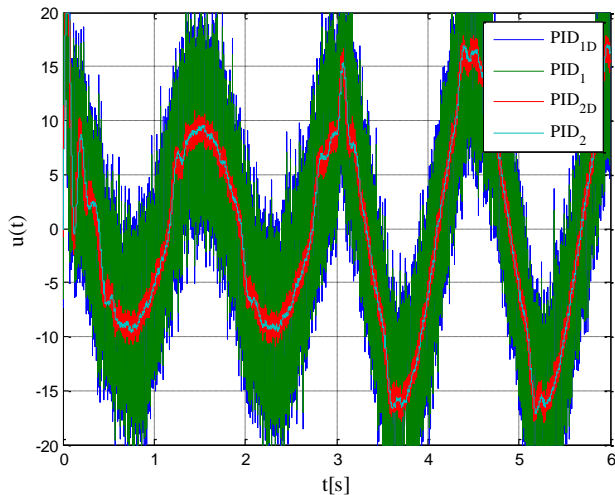
Parametri diskretnih regulatora su podešeni prema sledećem  $k_p = 63,17$ ,  $k_i = 85$ ,  $k_d = 8.78$  i  $T_f = 0.0169$ . Da bi simulacioni rezultati bili što verniji eksperimentalnim, u model su uvedene nelinearnosti tipa ograničenja upravljačkog signala  $u_{\max} = |20|V$  i "mrtve" zone motora jednosmerne struje od  $u_{\min} = |2|V$ . Za periodu diskretizacije usvojeno je  $T_s = 0.0001$ , dok je šum merenja simuliran kao Gausov beli šum varijanse  $\delta = 5 \cdot 10^{-5}$ .

Imajući u vidu da pomenuta platforma radi u režimu kružnog skeniranja koji zahteva prostoperiodično kretanje platforme po osi azimuta, analizirane su karakteristike sistema praćenja prostoperiodične reference  $r(t)$  u prisustvu poremećaja  $d(t)$ , koji se pojavljuje nakon treće sekunde.

Na slikama 6 i 7 prikazani su odzivi sistema i upravljački signali regulatora, respektivno, kada je  $r(t) = \sin(8\pi t)$  rad i  $d(t) = 0.1 \sin(8\pi t)$  Nm.



Slika 6-Odzivi sistema na sinusnu referencu u prisustvu šuma merenja i spoljašnjeg poremećaja



Slika 7- Vrednosti upravljačkih signala

Sa Slike 6 se jasno uočava da sistem sa osnovnom strukturom PID regulatora ne uspeva da prati referencu naročito nakon uključivanja poremećaja u trećoj sekundi, zbog prevelikog uticaja šuma merenja. Vrednosti upravljačkog signala u tom slučaju nisu prikazani na slici 7, zbog velike zašumljenosti. Što se tiče modifikovanih struktura regulatora, primećuje se da u pogledu performansi praćenja sve ostavruju približno iste rezultate, dok uticaj šuma merenja na upravljački signal značajno opada sa povećanjem reda filtra, što se vidi na slici 7.

## 5. ZAKLJUČAK

U radu je pokazano da modifikacije PID regulatora u cilju smanjenja uticaja mernog šuma utiču na performanse i robusnost sistema, tako da se pri izboru odgovarajuće strukture mora praviti kompromis. Pored toga, treba imati u vidu i praktičnu implementaciju složenijih struktura regulatora, što je veoma važno za industrijsku primenu.

## LITERATURA

- [1] Åström, K.J. and Häggglund, T., 2001. The future of PID control. *Control engineering practice*, 9(11), pp.1163-1175.
- [2] Åström, K.J., 2002. Control system design lecture notes for me 155a. *Department of Mechanical and Environmental Engineering University of California Santa Barbara*, p.333.
- [3] Basilio, J.C. and Matos, S.R., 2002. Design of PI and PID controllers with transient performance specification. *IEEE Transactions on education*, 45(4), pp.364-370.
- [4] Bucz, Š. and Kozáková, A., 2012. PID controller design for specified performance. *Introduction to PID Controllers: Theory, Tuning and application to frontier areas*.
- [5] Sekara, T.B. and Matausek, M.R., 2009. Optimization of PID controller based on maximization of the proportional gain under constraints on robustness and sensitivity to measurement noise. *IEEE Transactions on Automatic Control*, 54(1), pp.184-189.
- [6] Haugen, F., 2010. Discretization of simulator, filter, and PID controller. *Tech Teach*.
- [7] Stankovic, M., Manojlovic, S., Simic, S., Mitrovic, S. and Naumovic, M., 2016. FPGA system-level based design of multi-axis ADRC controller. *Mechatronics*, 40, pp.146-155.



# INFORMACIONI SISTEM ZA VOĐENJE EVIDENCIJE POKRETNIH STVARI

## INFORMATION SYSTEM FOR KEEPING RECORDS OF INVENTORY

Stefan Đurić<sup>1</sup>, Petar Lukić<sup>1</sup>, Ivan Tot<sup>1</sup>  
*Univerzitet odbrane, Vojna akademija<sup>1</sup>*

**Sadržaj** – U radu je predstavljeno rešenje za pomoć pri vođenju evidencije pokretnih stvari uz upotrebu računarske i Android aplikacije. Glavna zamisao je da ove aplikacije budu namenjene za sva profesionalna vojna lica na službi u Vojsci Srbije koja su zadužena za inventarisanje pokretne imovine. U radu je prikazano rešenje koje omogućava mobilnost i jednostavnost inventarisanja, uz mnogostruku uštedu resursa.

**Abstract** - This paper presents a solution for assistance in keeping records of moving objects, realized through a computer and Android application. The main idea is that these applications are intended for professional military personnel serving in the Serbian Army, who are in charge of stocktaking. The presented solution provides mobility and simplicity of inventory with multiple resource saving.

### 1. UVOD

Inventarisanje je uređeno Zakonom o računovodstvu („Službeni glasnik RS“, broj 62/13), kao i Pravilnikom o načinu i rokovima vršenja popisa i usklađivanja knjigovodstvenog stanja imovine sa stvarnim stanjem („Sl.glasnik RS” br.118/2013, 137/2014) [1].

Inventarisanje je sastavni deo funkcionisanja svake poslovne jedinice jer obezbeđuje kontrolu sopstvene imovine i čuvanje informacija o imovinskoj vrednosti. Zahtevi koje inventarisanje treba da zadovolji su:

- utvrđivanje stvarnog stanja,
- upoređivanje stanja sa knjigovodstvom,
- ustanovljavanje eventualnih manjkova ili viškova,
- usklađivanje sa knjigovodstvenim stanjem,

utvrđivanje kvalitativnog stanja pokretnih stvari.

Detaljnijom analizom navedenih zahteva jasno se uočavaju dva problema koja smanjuju efikasnost ovog procesa. To su: problem resursa i problem lokacije. Problem resursa odnosi se na veliki broj formulara koje treba popuniti prilikom evidentiranja pokretnosti. Svaki pomenuti zahtev iziskuje novi predefinisani formular u koji treba unositi podatke o popisanim stvarima. Znajući činjenicu da je inventarisanje periodičan proces, a da su pokretnosti procentualno najzastupljenija imovina, problem bespotrebnog trošenja resursa hartija, kao i vremena potrebnog za sastavljanje izveštaja, koji se dobija primenom različitih zahteva na popisanoj imovini, jasno je uočljiv. Problem lokacije postaje primetan kada se govori razbijenom tipu skladištnih objekata. Ovaj problem izražen je naročito u vojnom okruženju u kojem se radi sa opasnim materijama koje iziskuju izolovane skladišne prostorije. To znači obavezno nošenje celokupne papirologije od lokacije do lokacije kako bi se ista ažurirala, ili pravljenje

skica koje bi se ponovo morale objedinjavati u jedinstvenu celinu.

Navedeni problemi sa kojima se susreću lica koja su zadužena za sprovođenje inventarskog postupka ne pronalaze rešenja u tradicionalnom načinu inventarisanja, već se posmatraju kao neminovnost. Ovakvim pristupom, pored „traćenja“ resursa, ostavlja se značajno mesto za mogućnost greške izazvanom ljudskim faktorom zbog eventualne konfuzije koja može nastati nagomilavanjem papirologije ili samom činjenicom da se u postupku sastavljanja konačnog evidencionog spiska stanja i upoređivanja sa knjigovodstvenim knjigama mora raditi istovremeno sa više dokumenata (tabela), što čoveku nije svojstveno.

Zahtevi koji se postavljaju pred ovaj rad su:

- maksimalno skraćivanje vremena za postupak popisivanja,
- smanjivanje utroška resursa,
- mobilnost izvođenja postupka inventarisanja bez obzira na udaljenost skladištnih objekata pokretnosti,
- maksimalno umanjivanje verovatnoće greške ljudskog faktora.

### 2. ANALIZA ZAHTEVA

Po razmatranju postavljenih zahteva zaključeno je da rešenje mora biti mobilno, a u isto vreme dovoljno hardverski moćno da skladišti veliku količinu podataka i da njome manipuliše. Rešenje koje je usvojeno jeste kreiranje dve aplikacije. Prva bi bila kreirana za Android uređaje, čime bi se obezbedila mobilnost, a druga za (laptop) računare, što bi obezbedilo hardversku moć.

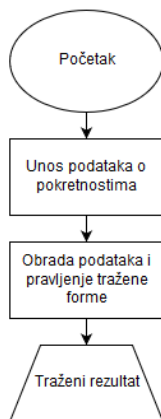
Vodeći se principom jednostavnosti odlučeno je da se Android aplikacija kreira u okruženju Android studio koje omogućava brz razvoj Android aplikacija, dok je za skladištenje podataka odabran Microsoft SQL server, kao standard u Vojsci Srbije. Ovakav izbor sistema za upravljanje bazom podataka proizvodi prirodno rešenje da okruženje za kreiranje baze podataka i programski jezik za kreiranje računarske aplikacije budu iz Microsoft familije. Za programski jezik za kreiranje računarske aplikacije izabran je C# u okruženju Visual Studio 2010, dok je za okruženje za kreiranje baze podataka i programiranje iste izabran Microsoft SQL Server Management Studio.

Kako bi se sačuvala mobilnost koju obezbeđuje Android platforma, kao i paralelno izvršavanje radnji na Android uređaju i računaru odlučeno je da oni budu međusobno povezani Bluetooth konekcijom.

Mobilnost Android uređaja, sa jedne strane, i velike mogućnosti SQL Servera, u polju obrade podataka sa druge, potpuno zadovoljavaju postavljene zahteve i omogućavaju kreiranje aplikativnog sistema koji bi u velikoj meri ubrzao proces inventarisanja i sveo mogućnost greške izazvane ljudskim faktorom na minimum.

### 3. DIZAJN I IMPLEMENTACIJA REŠENJA

Dijagram toka kreiranog rešenja ima sledeće elemente (prikazano na slici 1):



Slika 1. Dijagram toka

Rešenje je realizovano tako da se svakoj pokretnoj stvari određuje jedinstveni BAR ili QR kod po kome bi ona bila prepoznatljiva, a zatim se vrši unos podataka potrebnih za poslove inventarisanja koji se odnose na datu pokretnost. Računarska aplikacija zadužena je za generisanje kodova i njihovo formatiranje u obliku slike. Osim neophodnih podataka za poslove inventarisanja aplikaciji je dodata opciona mogućnost čuvanja fotografija pokretnih stvari zbog lakšeg rada sa istim.

Raznovrsnost i laka implementacija objekata korisničkog interfejsa omogućili su kreiranje jednostavnog korisničkog interfejsa u kome korisnik klikom na dugme ili biranjem ponuđenih stavki iz „combo box“ objekata vrši prikupljanje podataka o pokretnosti, obradu istih, kao i njihov prikaz u traženom obliku (slika 2).

Po unosu svih sredstava u bazu podataka BAR ili QR kodovi dostupni su u Word dokumentu iz kojeg se kasnije mogu štampati ne bi li se izvršilo njihovo postavljanje na odgovarajuća pokretna sredstva. Po završetku pomenutih radnji aplikacija je spremna za rad i korisnik može da krene sa postupkom inventarisanja.

Korisnik sam proces inventarisanja može izvršavati na dva načina u zavisnosti da li je računar na kome se skladište podaci unutar ili van dometa Bluetooth konekcije Android uređaja, te razlikujemo „online“ i „offline“ režim rada što je prikazano na slici 3. U slučaju da je van dometa, korisnik pokretanjem aplikacije na Android uređaju vrši očitavanje postavljenog BAR/QR koda, pomoću kamere na svom uređaju, sa pokretnog sredstva što aplikacija prepoznaje

kao traženu informaciju sa skeniranog koda i skladišti je u tekstualni fajl na uređaju. Skladištene podatke korisnik može kasnije prebaciti na računar kada ponovo bude u neposrednoj blizini računara, čime se postiže apsolutna mobilnost i kompaktnost. Transfer podataka na računar ostvaren je preko Bluetooth tehnologije, jer ne zahteva prisustvo „treće“ hardverske komponente, niti korišćenje usluge bilo kog provajdera.



Slika 2. Stranica sa mogućnostima odabira akcije skeniranog koda

Kada je u pitanju rad u kome Android uređaj i računar mogu ostvariti Bluetooth konekciju, korisnik vrši snimanje BAR/QR koda i direktno slanje informacije koda računaru, koji informaciju prima i skladišti je u tabelu očitanih pokretnosti, prikazano na slici 4. Dalji rad na računarskoj aplikaciji je isti za obe režima rada. Korisnik može vršiti pregled očitanih pokretnosti i njihovo arhiviranje u Word dokumentu radi dalje obrade i formatiranja za popunjavanje formulara inventara.



Slika 3. Prozor za unos novog pokretnog sredstva u bazu podataka

Prilikom rada aplikacija vrši nadzor korisnika i hardvskog dela komunikacije. Ukoliko korisnik unese neodgovarajuć tip podatka ili izostavi unos nekog od polja dobija poruku o greški koja je nastala. Korisnik takođe dobija i informacije u vidu poruke ukoliko je Bluetooth modul prestao sa radom ili ukoliko nije uključen.



Slika 4. Prijem skeniranog predmeta u „online“ režimu

Zaštita od prijema malicioznog sadržaja sa Android uređaja osigurana je time što se uređaji pre slanja sadržaja moraju „upariti“. Ovo obezbeđuje prijem sadržaja sa uređaja od poverenja pri čemu se ne narušava bezbednost samog računara.

Po pitanju Bluetooth komunikacije i Android aplikacije koja se koristi za slanje informacije sa skeniranog BAR/QR koda, omogućeno je korišćenje i jedne od dostupnih aplikacija sa „Play store“ prodavnice za Android uređaje što garantuje modularnost ovog aplikativnog sistema. Modularnost u ovom slučaju označava korišćenje nekog drugog gotovog rešenja za skeniranje BAR/QR kodova koje bi pojedinačnim korisnicima više odgovaralo od ponuđenog.

Skeniranje BAR/QR kodova u Android aplikaciji realizovano je uz pomoć ZXing biblioteke poznate pod imenom „Zebra crossing“ čiji su rezultati na ovom polju najzapaženiji, dok je komuniciranje računarske aplikacije sa Android uređajem putem Bluetooth-a realizovana preko OBEX (Object EXchange) protokola, jer poput HTTP protokola obezbeđuje klijentu pouzdan transport podataka.

#### 4. ZAKLJUČAK

Predloženo rešenje obezbeđuje višestruko skraćivanje vremena potrebnog za popisivanje pokretnih stvari, uštedu resursa i svodenje verovatnoće greške na minimum. Osim navedenog postiže se i trajno čuvanje podataka o pokretnostima što pogoduje skraćivanju neophodnog vremena potrebnog za proces već kod narednog popisivanja.

U predloženom rešenju Android aplikacija vrši skeniranje BAR/QR kodova i njihovo skladištenje, odnosno direktno prosleđivanje računaru, dok računarska aplikacija vrši unos podataka pokretnih stvari u bazu podataka, generisanje jedinstvenog BAR/QR koda i pregled očitanih (popisanih) pokretnosti.

U daljem radu planira se nadogradnja obe aplikacije. Za Android aplikaciju planira se detaljnije dizajniranje korisničkog interfejsa, povećavanje funkcionalnosti u smislu slanja podataka sa očitanih BAR/QR koda na server putem interneta. Dalji rad na računarskoj aplikaciji obuhvatao bi omogućavanje različitih manipulacija informacijama očitanih i neočitanih pokretnosti. Osim nadgradnje baze podataka, rad bi se nastavio i u polju modularnosti rada sa više aplikacija koje ne bi zavisile od platforme na kojoj se pokreću kao i rada sa više vrsta mobilnih uređaja koji mogu vršiti skeniranje BAR/QR kodova i prosleđivanje skeniranih podataka.

#### LITERATURA

- [1] <http://www.skolaknjigovodstva.com/wp-content/uploads/2015/05/ZALIHE-I INVENTARISANJE-.pdf>
- [2] <http://stackoverflow.com/>
- [3] <http://developer.android.com/training>

# UPOTREBA RAZVIJENIH MIDDLEWARE U ARHITEKTURI IOT USE OF DEVELOPED MIDDLEWARE IN IOT ARCHITECTURE

Ivan Tot<sup>1</sup>, Dušan Bogičević<sup>2</sup>, Komlen Lalović<sup>3</sup>

Univerzitet odbrane, Vojna akademija<sup>1</sup>

Vojska Srbije<sup>2</sup>

Fakultet za primenjeni menadžment, ekonomiju i finansije - MEF<sup>3</sup>

**Sadržaj** – U ovom radu prikazani su middleware sistemi koji se koriste kao apstrakcioni sloj sa zadatkom da omoguće upravljanje različitim uređajima na isti način u IoT arhitekturi. Takođe, prikazana je i mogućnost korišćenja pametnih telefona kao gateway sistema.

**Abstract** – In this paper, middleware systems which are used as an abstraction layer with the task of enabling the management of different devices in the same way in the IoT architecture are described. It also shows the ability to use smartphones as a gateway system.

## 1. UVOD

U IoT okruženjima postoji veliki broj raznorodnih uređaja, gde se njihove razlike ogledaju u njihovim funkcionalnostima, kapacitetima, kao i programskim jezicima pomoću kojih je moguće pristupiti njima (slika 1). Zbog toga je potrebno izvršiti apstrakciju, odnosno napraviti apstrakcioni sloj koji će imati zadatak da omogući upravljanje različitim uređajima na isti način. Na ovaj način korisnici i aplikacije mogu razmenjivati i koristiti podatke između sebe, bez potrebe da poznaju arhitekturu svakog uređaja. [1]



Slika 1. IoT okruženje

U IoT okruženjima middleware sistemi (slika 2) služe da bi se programeru koji razvija aplikaciju omogućilo da se maksimalno posveti razvoju aplikacije, bez opterećivanja arhitekturom i načinom na koji hardver radi. To su slojevi softvera koji se nalaze između aplikativnog softvera i sistemskog softvera, kao i unutar komunikacionog dela između ova dva sloja. [2]



Slika 2. Mesto middleware sistema

## 2. ZAHTEVI PREMA MIDDLEWARE SISTEMIMA

Zahtevi koje se postavljaju ispred middleware sistema mogu se podeliti u dve grupe:

1. **zahtevi za middleware servise**: ovi zahtevi se mogu podeliti na dve podgrupe u zavisnosti na koji deo servisa se odnose:

- funkcionalni zahtevi: ovi zahtevi su vezani za funkcionalnosti odnosno mogućnosti koje se očekuju od middleware sistema u IoT okruženjima. Ti zahtevi su:
  - pronalaženje uređaja (senzora, aktuatora...),
  - upravljanje uređajima,
  - upravljanje podacima,
  - upravljanje događajima,
  - upravljanje programskim kodom (modifikacija koda).
- nefunkcionalne zahtevi: imaju za cilj da postavte zahteve koji se očekuju od middleware sistema u IoT okruženjima. Ti zahtevi su:
  - da budu skalabilni,
  - da rade u realnom vremenu,
  - da budu pouzdani,
  - da budu dostupni,
  - da budu bezbedni.

2. **zahtevi u pogledu arhitekture middleware sistema**: ovi zahtevi su namenjeni da olakšaju rad programerima koji razvijaju aplikacije. Zahtevi se odnose na:

- apstrakciju,
- interoperabilnost,
- servisno orjentisanu arhitekturu,
- prilagodljivost,
- svesnost na nivou konteksta,
- samoupravljaljivost (bez čoveka),
- dostupnost.

## 3. PODELA MIDDLEWARE-A

Postoji veći broj realizovanih middleware-a. U zavisnosti od pristupa koji je korišćen pri razvoju middleware sistema, možemo ih podeliti u više grupa [2]:

1. **zasnovani na obradi događaja**: kod ove grupe middleware sistema svi učesnici vrše interakciju preko događaja. Svaki događaj ima svoj tip i vrednosti, na osnovu kojih se opisuje promena stanja. Događaji kreću od aplikacije koja šalje događaj, dok druge aplikacije

oslušuju promenu stanja. Ovakav sistem može da se sastoji od velikog broja učesnika koji objavljuju događaje, kao i velikog broja onih koji oslušuju događaje. Najčešći model koji se koristi za razmenu poruka kod ovog modela je oglašavač/pretplatnik. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- Hermes,
- EMMA,
- GREEN,
- RUNES,
- PRISMA,
- SensorBus,
- Mires,
- MiSense,
- PSWare,
- TinyDDS.

2. **servisno orjentisani:** kod ove grupe middleware-a, sistemi su zasnovani na servisnoj arhitekturi (SOA) i aplikacije se razvijaju u formi servisa. Postoji veliki broj servisno orjentisanih middleware-a i najčešće su dostupni u formi platforme kao servis (PaaS). Pružaju pogodnosti kao što su dostupnost, višestruka upotreba i sl. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- Hydra(LinkSmart),
- SenseWrap,
- MUSIC,
- TinySOA,
- SOCRADES,
- SensorsMW,
- SENSEI,
- Servilla,
- KASOM,
- CHOReOS,
- CarrIoTs,
- Echelon,
- UBIsoap,
- MOSDEN,
- Xivoly.

3. **zasnovani na virtuelizaciji:** ova grupa middleware sistema pruža bezbedno okruženje za izvršavanje aplikacija na taj način što virtuelizuje infrastrukturu. Aplikacije su podeljene u male module, koji su ubačeni i rašireni po celoj mreži. Svaka tačka u mreži ima svoj virtuelni modul koji služi kao interpreter. Ovakav middleware sistem pruža najviši nivo apstrakcije. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- Maté,
- Extended Maté,
- VM,
- Melete ,
- MagnetOS,
- Squawk,
- Sensorware,
- SwissQM,
- DVM,
- TinyReef,
- TinyVM.

4. **zasnovani na agentu:** kod ove grupe middleware sistema, aplikacije su podeljene na modularne delove programa koji korišćenjem mobilnih agenata omogućavaju lakši razmeštaj i ubacivanje u mrežu. Ovakav pristup ima prednosti kao što su upravljanje resursima, dostupnost, pouzdanost, upravljanje programskim kodom i sl. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- Impala,
- Smart messages,
- ActorNet,
- Agilla,
- Ubiware,
- UbiROAD,
- AFME,
- MAPS,
- MASPOT,
- TinyMAPS.

5. **zasnovani na torkama podataka:** kod ove grupe middleware sistema, svaki član infrastrukture zadržava svoj lokani oblik strukture torke. Torka je predstavljena kao podatak kome se može pristupiti konkurentno (paralelno). Sve torke koje se nalaze u sklopu jednog domena, imaju svoje oblike torki na gateway-u. Ovakav pristup omogućava mobilnim uređajima da dele podatke u okviru gateway-ja kome pristupaju. Aplikacije komuniciraju tako što pišu torke, a čitanje podataka se vrši preko obrazaca u zavisnosti za koje podatke su zainteresovane. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- LIME,
- TinyLIME,
- TeenyLIME,
- TS-Mid,
- A3-TAG.

6. **zasnovani na bazama podatka:** ova grupa middleware sistema vidi mrežu kao virtuelni sistem povezanih baza podataka nad kojim dozvoljava pravljenje kompleksnih upita. Istraživanja kod ovih sistema su usmerena na pronalaženje pristupa za distribuirane baze podataka radi interoperabilnosti sistema. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- SINA,
- COUGAR,
- IrisNet,
- Sensation,
- TinyDB,
- GSN,
- Kspot,
- HyCache.

7. **orjentisani ka aplikacijama:** ova grupa middleware sistema vodi brigu o resursima koji su potrebni za svaku aplikaciju pojedinačno, implementirajući arhitekturu koja najviše odgovara potrebama konkretne aplikacije. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [2]:

- AutoSec,
- Adaptive Middleware,



- MiLAN,
- TinyCubus,
- MidFusion.

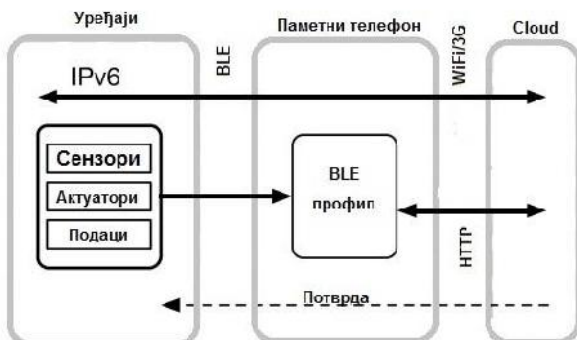
8. **kontekсно orjentisani:** problem velike količine podataka u IoT se može rešiti dodavanjem mogućnosti da middleware-i budu svesni konteksta podataka (informacija). Middleware-i koji pripadaju ovoj grupi mogu se koristiti kao rešenje za obradu velike količine podataka [5]. Neki od realizovanih middleware-a koji pripadaju ovoj grupi su [3]:

- CAMPH,
- ACoMS+,
- Octopus,
- FIWARE,
- CA4IOT,
- CAMPUS,
- CASF,
- SeCoMan,
- CoCaMAAL,
- BDCaM,
- FlexRFID.

#### 4. PAMETNI TELEFON KAO GATEWAY

Gateway sistemi treba da reše i problem na nivou uređaja, tako npr. ako bi se koristile bežične tehnologije kao što je Bluetooth ili Zigbee, potrebno je koristiti poseban uređaj koji bi sa jedne strane učestvovao u komunikaciji sa objektima preko Bluetooth (Zigbee) mreže, dok bi sa druge strane trebalo da obezbedi komunikaciju sa serverima (servisima, IoT platformama) i drugim objektima koji se nalaze u drugoj mreži (slika 3). Neka od rešenja koja se predlažu je korišćenje pametnih telefona kao posrednika koji bi obavljao ulogu Gateway uređaja [2, 3]. Kod ovog rešenja mogu da se koriste dva mehanizma za razmenu podataka:

- prvi mehanizam koristi mobilni telefon kao ruter, dodeljujući IPv6 adrese objektima,
- drugi mehanizam koristi mobilni telefon kao proxy, gde komunikaciju koja bi se odvijala preko Bluetooth, prosleđuje u Cloud-u odnosno serveru.



Slika 3. Pametni telefon kao Gateway

#### 5. PROBLEM VELIKE KOLIČINE PODATAKA

U IoT postoji veliki broj senzora (uređaja) koji postaju sve napredniji, manji i jeftini i oni su najveći izvori podataka u IoT (Big data). Da bi omogućili analiziranje i obradu svih podataka, potrebno je da određeni delovi u IoT budu svesni podataka koje primaju i da odluče na osnovu konteksta da li podatke treba da šalju dalje ili ne.

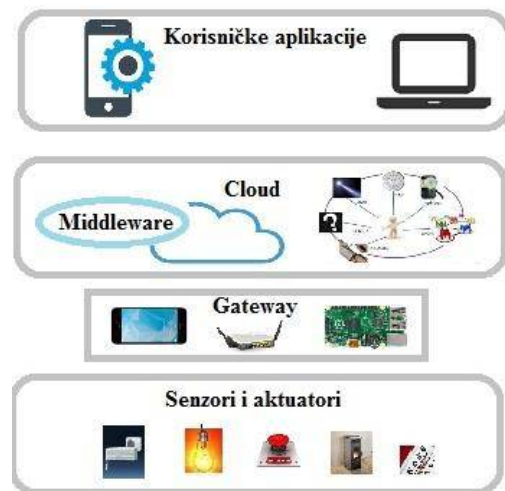
Grupa middleware koja ima mehanizam za obradu velike količine podataka je grupa kontekсно orjentisanih middleware-a. Ova grupa middleware problem velike količine podataka (Big data) rešava uvođenjem konteksta odnosno „pištaljke“ koja se oglašava prilikom promena koje utiču na sam kontekst u kome se IoT uređaj nalazi. Ovo filtriranje je moguće rešiti i na nivou gateway-a. Na ovaj način smanjili bi opterećenje mrežnih resura.

Uvođenje pametnih gateway približava konceptu Fog computing, koji za cilj ima „spuštanje“ servisa bliže korisnicima i omogućavanje boljih performansi mreže.

U Fog computing moguće je razlikovati tri sloja uređaja:

- **ivični:** proizvode podatke pomoću senzora i vrše aktucije uređaja,
- **ulazno/izlazni:** rade kao brokери između ivičnih i serverskih uređaja,
- **serverski:** omogućavaju određene usluge u vidu upravljanja ili prikupljanja podataka.

Pojedini uređaji mogu obalžati funkcije više slojeva, tako npr. gateway može raditi i na ulazno/izlaznom sloju kao i na serverskom sloju (slika 4) [6].



Slika 4. Koncept Fog computing-a

#### 6. ZAKLJUČAK

IoT se zasniva na velikom broju uređaja i njihovoj velikoj raznorednosti. Arhitektura IoT sistema trebalo bi da se sastoji od middleware koji bi vršio apstrakciju uređaja kako bi omogućili njihovo lakše upravljanje. Pored middleware-a potrebno je obezbediti i funkcije gateway, filtriranja saboračaja, kao i bezbednosti sistema. Na ovaj način moguće je smanjiti opterećenje mrežnih resura.

## LITERATURA

- [1] Manuel Díaz, Cristian Martín, Bartolomé Rubio, „State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing”, Elsevier, 2016.
- [2] Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, Siobhán Clarke, “Middleware for Internet of Things: A Survey“, IEEE INTERNET OF THINGS JOURNAL, 2016.
- [3] Xin Li \*, Martina Eckert, José-Fernán Martínez and Gregorio Rubio23, „Context Aware Middleware Architectures: Survey and Challenges“, Sensors, 2015.
- [4] Thomas Zachariah, Noah Klugman, Bradford Campbell, Joshua Adkins, Neal Jackson, Prabal Dutta, „The Internet of Things Has a Gateway Problem“, Santa Fe, New Mexico, USA, February 2015.
- [5] Charith Perera, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos, “Context Aware Computing for The Internet of Things: A Survey”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2013.
- [6] Nam Ky Giang, Michael Blackstock, Rodger Lea, Victor C.M. Leung, „Developing IoT applications in the Fog: A Distributed Dataflow approach”, IEEE, 2015.

# ODREĐIVANJE GPS KOORDINATA, SLANJE NMEA REČENICE PUTEM GPRS I PRIKAZ LOKACIJE NA MAPI

## GETTING GPS COORDINATES, SENDING NMEA SENTENCE OVER GPRS AND DISPLAYING LOCATION ON THE MAP

Lazar Stevanović<sup>1</sup>, Lazar Đorđević<sup>1</sup>, Stefan Đurić<sup>1</sup>  
*Univerzitet odbrane, Vojna akademija*

**Sadržaj** – Određivanje tačne lokacije vojnika od ogromne je važnosti u svim vojskama sveta. U radu je dato rešenje za uređaj za praćenje, i mapu koja prihvata i prikazuje koordinate poslate sa uređaja. U radu je korišćen sistem satelitske GPS lokacije, obzirom na to da je to sistem koji pokriva čitavu Zemlju, lokacija se može odrediti skoro svugde na planeti.

Uređaj za praćenje realizovan je uz pomoć četrdesetopinskog Atmelovog ATmega32 mikroprocesora, SIM808 klik modula i razvojne ploče EasyAVRv7.

Programiranje mikrokontrolera izvršeno je preko programskog paketa MikroC PRO for AVR, dok je mapa programirana u Javi.

**Abstract** - Determining the exact location of soldiers is of great significance for all armies. A tracking device and a map that receives and displays the coordinates sent by the device are presented in this paper. Satellite GPS was used since its global coverage makes it possible to determine location almost anywhere on the planet.

An Atmel's ATmega32 forty pins microprocessor, a sim808 click module, and an EasyAVRv7 development board were used in the construction of the tracking device.

The microcontroller was programmed using MikroC PRO for AVR, and the map was programmed in Java.

### 1. UVOD

Uređaj za praćenje koristi princip satelitske GPS (Global Positioning System) lokacije. GPS se sastoji od 24 satelita raspoređenih u orbiti Zemlje koji šalju radio signal, pomoću ovih radio signala GPS prijemnici mogu da odrede svoju tačnu poziciju - nadmorsku visinu, geografsku širinu i geografsku dužinu na bilo kom mestu na planeti danju i noću, u svim vremenskim uslovima [1]. Ovaj princip lokacije zahteva da antena uređaja bude izložena vidljivosti ka tri ili više satelita. Princip određivanja koordinata funkcioniše po principu TOA (Time of Arrival), to jest merenja vremena prispeća signala od svakog satelita koji je u vidokrugu uređaja. U preseku ovih sfera, dobija se tražena pozicija GPS prijemnika, zapisana u tekstualnom formatu u obliku NMEA rečenice. Tačnost određenih koordinata je na iznenađujuće visokom nivou. Ovaj sistem greši 15-40m za određivanje lokacije.

Bitno je napomenuti da je GPS sistem u vlasništvu vlade SAD, oni mogu zabraniti pristup satelitima ili pak mogu slati pogrešne ili modifikovane informacije običnim korisnicima.

Informacija o geografskoj širini, geografskoj dužini, nadmorskoj visini i broju satelita koji su učestvovali u određivanju lokacije sadržana je u NMEA rečenici.

### 2. NMEA REČENICA

The National Marine Electronics Association (NMEA) je organizacija koja je odredila specifikacije za komunikaciju dva ili više uređaja i prenos podataka prikupljenih nekim senzorom. NMEA rečenica predstavlja tekstualnu rečenicu od okvirno pedeset karaktera, dužina se razlikuje od formata koji se koristi. U toj rečenici sadržana je informacija o lokaciji, vremenu kad je određena lokacija, broju satelita koji se korišćen, kvalitetu podataka itd..

Sve NMEA rečenice počinju karakterom \$, zatim slede 2 karaktera koja označavaju uređaje koji koriste ovu rečenicu. Za GPS prijemnike to je GP. Tako da NMEA rečenica koju koriste GPS uređaji počinje sa \$GP.

Svaka NMEA rečenica je nezavisna od drugih. U ovom radu korišćen je format \$GPGGA (Global Positioning System Fix Data) prikazan na slici 1.

Table 5-1. Global Positioning System Fixed Data

Name	Example	Unit	Description
Message ID	\$GPGGA		GGA protocol header
UTC Time	2153.000		HHmm.ss.ss
Latitude	3342.6618		ddmm.mmmmm
N/S Indicator	N		N=north or S=south
Longitude	11751.3858		dddmm.mmmmm
E/W Indicator	W		E=east or W=west
Position Fix Indicator	1		
Satellites Used	10		Range 0 to 12
HDOP	1.2		Horizontal Dilution of Precision
MSL Altitude	27.0	meters	
Units	M	meters	
Geoid Separation	-34.2	meters	Geoid-to-ellipsoid separation. Ellipsoid altitude = MSL Altitude + Geoid Separation.
Units	M	meters	
Age of Diff. Corr.		sec	Null fields when DGPS is not used
Diff. Ref. Station ID	0000		
Checksum	*5E		
<CR><LF>			End of message termination

Slika 1. Format \$GPGGA

### 3. GPRS

Slanje podataka sa uređaja na mapu realizovano je preko GPRS-a.

GPRS (General Packet Radio Service) je protokol koji omogućava prenos podataka bežičnim putem kroz GSM mrežu. Glavne karakteristike ovog protokola su [2]:

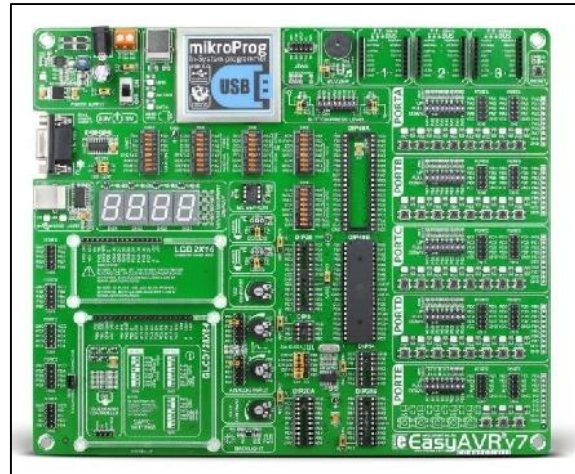
- Brzina prenosa podataka – teorijska maksimalna brzina prenosa putem ovog servisa je 171.2 kbit/s. U praksi, brzina prenosa zavisi od nekoliko faktora: limitiranost brzine prenosa usled samih karakteristika GPS uređaja, jačina signala operatera GSM telefonije, udaljenost uređaja od bazne stanice itd..
- Uvek “Online”  
GPRS protokol ne zahteva klasično povezivanje, ukoliko treba koristiti GPRS usluge, brzina povezivanja sa udaljenim uređajem je gotovo trenutna, zato se kaže da su korisnici GPRS-a uvek “Online”.
- Plaćanje servisa operateru prema količini prenetih podataka  
Primenom savremene tehnologije i konceptom samog protokola operateri mobilne telefonije koji pružaju GPRS usluge naplaćuju uslugu isključivo prema utrošenim podacima, a ne po vremenu korišćenja servisa.
- GPRS servis je relativno jeftin sa stanovišta operatera  
Isplativost ovog servisa leži u tome što on koristi već postojeću infrastrukturu GSM mreža (GSM 900/1800/1900).

GPRS je zasnovan na principu prenosa paketa. Prenos podataka kroz mrežu ide po tipu paketa, koji se ponavljaju dokle god od strane onoga ko prima ne stigne potvrda o ispravnom prijemu.

Sve što je potrebno da bi mogao da se koristi GPRS servis je da korisnik poseduje mobilni telefon koji podržava ovaj protokol i SIM karticu, da operater mobilne telefonije omogućava GPRS servis i da korisnik ima aktiviranu GPRS uslugu kod mobilnog operatera.

### 4. UREĐAJ ZA PRAĆENJE

Osnovu hardverske realizacije predstavlja četrdeseto pinski Atmelov ATmega32 mikropocesor, koji se nalazi na ploči EasyAVRv7 koji je proizveden od strane Mikroelektronike. EasyAVRv7 predstavlja razvojnu multifunkcionalnu ploču, koja u sebi ima ugrađen niz komponenata koji joj daju osnovnu funkcionalnost, koja je dosta ograničena. Ploča je otvorenog koncepta, podržava veliki spektar klik modula koji joj u značajnoj meri proširuju osnovnu funkcionalnost. Izgled EasyAVRv7 ploče sa ATmega32 mikropocesorom prikazan je na slici 2.



Slika 2. Razvojna ploča EasyAVRv7

U radu je korišćen klik modul SIM808 (slika 3) koji omogućava GPS i GPRS funkcionalnost uređaja. Ovaj klik modul ima slot za SIM karticu kojom se pristupa GPRS usluzi mts operatera i dve antene. Jedna je GPS antena za komunikaciju sa satelitima a druga za slanje dobijenih podataka preko GSM(GPRS). [3, 4]

Interfejsi kojim se programira ovaj klik modul su UART i GPIO. U radu je korišćen UART protokol.

Napajanje ovog klik modula je 5 V i to je eksterno napajanje, ploča pruža maksimalno napajanje od 3.3 V, koje nije dovoljno za napajanje ovog klik modula, jer dolazi do automatskog resetovanja usled nedovoljnog napajanja.

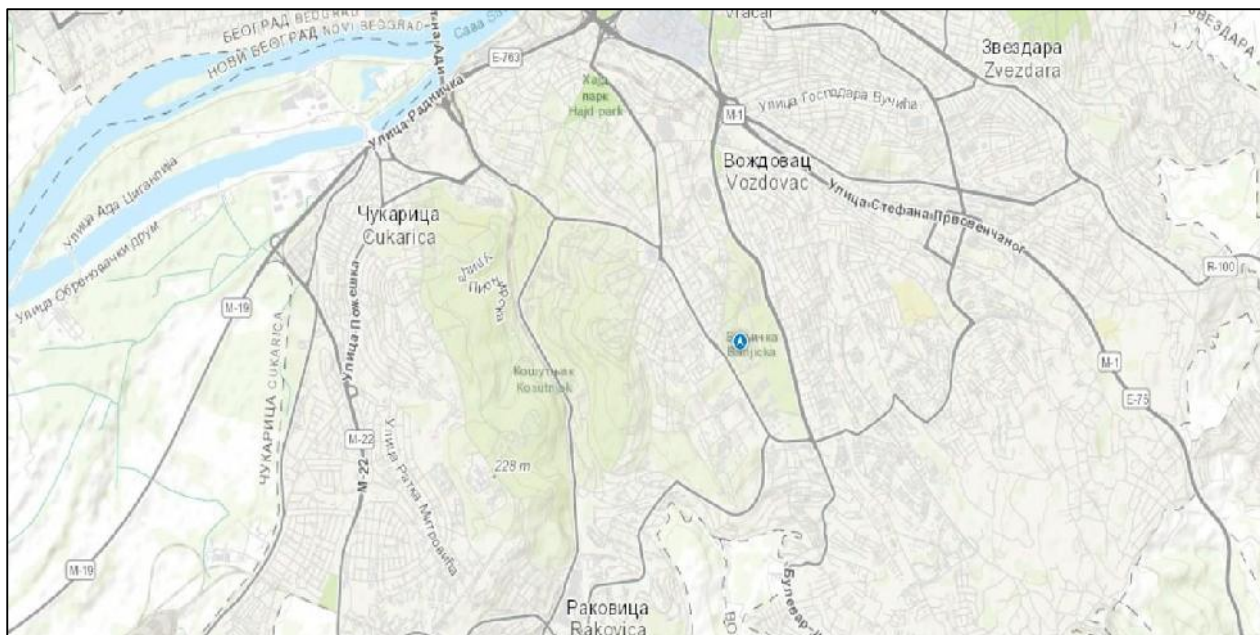
Kompatibilnost ovog klik modula je mikroBUS.



Slika 3. Klik modul SIM808



## 5. PRIKAZ ODREĐENE LOKACIJE NA MAPI



Slika 4. Prikaz određene lokacije na mapi

Za realizaciju mape korišćeno je razvojno okruženje Eclipse, programski jezik Java i softverski alat ArcGIS Runtime. Mapa pruža funkcionalnost zumiranja, praćenja prethodnih lokacija i prikaza vrednosti koordinata. Određena lokacija na mapi (plava tačka) predstavlja lokaciju Vojne Akademije na kojoj je testiran napravljeni uređaj (slika 4). Perioda osvežavanja lokacije je 30 sekundi, koliko je potrebno uređaju da dobije nove podatke od satelita. Prikupljanje NMEA rečenice i paralelni prikaz mape izveden je uz pomoć višenitnog koncepta objektno-orijentisanog programskog jezika Java.

## 6. ZAKLJUČAK

Specifičnost vojnog poziva zahteva od pripadnika Vojske Srbije da često budu na terenu, u prirodi, daleko od civilizovane sredine. Ovaj uređaj predstavlja spoj hardverskog i softverskog koji vojniku Vojske Srbije omogućava na najlakši način da sazna i pošalje drugome informaciju o lokaciji na kojoj se nalazi.

Na izbor ovih komponenata prilikom pravljenja uređaja uticala je njihova cena. Relativno su jeftini za servis koji pružaju, a opet nude potpunu funkcionalnost i tačnost.

Cilj rada bio je i upoznavanje sa osnovnim sistemima lokacije i njihovim karakteristikama, kao i problemom slanja podataka bežičnim putem.

Planirani dalji rad na postojećoj aplikaciji podrazumeva integraciju postojećih komponenti u jedan što kompaktniji i mobilniji uređaj, poboljšanje preciznosti, povećanje periode osvežavanja lokacije radi što vernijeg prikaza u realnom vremenu. Sve ovo zahteva zamenu postojećeg hardvera modernijim komponentama. Softverski razvoj aplikacije podrazumeva uvođenje novih funkcionalnosti kao što su računanje pređenog puta, brzine kretanja i navigacija.

## LITERATURA

- [1] Pratap Misra, Per Enge, "Global Positioning System: Signals, Measurements and Performance", Ganga-Jamuna Press, P.O. Box 633, Lincoln, Massachusetts 01773, 2011.
- [2] Šunjevarić M., Todorović B. "Radio-relejne i satelitske komunikacije", FTN Izdavaštvo, Novi Sad, 2012.
- [3] SIM800 Series\_AT Command Manual\_V1.09, SIM Technology, 2015.
- [4] Srđan T. Mitrović, Mladen Antonić "Mikroprocesorski sistemi", 2017.



# ADD-IN ZA SELEKTIVNO ŠIFROVANJE TEKSTA U OKVIRU MICROSOFT WORD DOKUMENTA

## ADD-IN FOR SELECTIVE ENCRYPTION OF THE TEXT WITHIN MICROSOFT WORD DOCUMENT

Jovana Mihailov<sup>1</sup>, Boriša Jovanović<sup>1</sup>, Boban Mihailov<sup>2</sup>

*Centar za primenjenu matematiku i elektroniku, Vojska Srbije<sup>1</sup>*

*Centar za komandno informacione sisteme i informatičku podršku, Vojska Srbije<sup>2</sup>*

**Sadržaj** – Sigurnost računarskih sistema postaje sve važnija, jer su korisnici sve više privrženiji računarskom svetu. U takvom sistemu postoji i sve veća opasnost od neovlaštene upotrebe informacija. Podaci zahtevaju posebnu pažnju i zaštitu, kako bi se očuvala tajnost posla i projekata kojim se korisnik bavi. Pravovremene i tačne informacije olakšavaju rad, pa njihovo menjanje, krađa i druge zlonamerne radnje utiču na ishod, verodostojnost i tačnost donetih odluka, tako da je vrlo značajno obezbediti adekvatan i visok stepen zaštite podataka. U radu je predstavljeno unapređenje programa za obradu teksta Microsoft Word, u okviru programskog paketa Microsoft Office, realizacijom dodatka (Add-In-a) koji obezbeđuje tajnost podataka prilikom elektronske komunikacije više korisnika.

**Abstract** - Security of computer systems is becoming more important, as users are more and more attached to the computer world. There is an increasing risk of unauthorized use of information in such a system. The data requires special attention and protection in order to preserve the secrecy of the work and projects that the user is dealing with. Timely and accurate information makes it easy to work, so changing, stealing and other malicious actions greatly affect the outcome, credibility and accuracy of these decisions, so it is very important to ensure an adequate and high degree of data protection. This paper presents the improvement of the text processing program Microsoft Word, within the Microsoft Office software package, by implementing Add-In, which secures data confidentiality in the electronic communication of multiple users.

### 1. UVOD

Posmatrajući radna okruženja u vremenu za nama, osiguravanje osetljivih kompanijskih podataka svodilo se jednostavno na zaključavanje vrata, zapošljavanje fizičkog obezbeđenja i izdavanje pristupnih kartica zaposlenima. U modernom radnom okruženju mobilnost je sve prisutniji trend, koji omogućava zaposlenima da rade gde god da se nalaze, umesto u zatvorenom i kontrolisanom kancelarijskom okruženju. Kako bi se zaštitile od gubitka poslovnih podataka, koji može da uzrokuje ne samo finansijsku štetu već i kompromitovanje reputacije, kompanije moraju da implementiraju neki od sistema zaštite podataka. Najefikasniji način da se korisnički podaci na računaru zaštite jeste primena

kriptografskih mera zaštite, koje onemogućavaju čitanje navedenih podataka od strane neovlašćenih korisnika.

Kada se lične, finansijske, vojne ili informacije organa javne uprave prenose sa jednog mesta na drugo, one postaju osetljive na različite načine prisluškivanja. Ovakvi problemi se mogu izbeći upotrebom kriptografskih tehnika zaštite informacija, koje ih čine nedostupnim neželjenoj trećoj strani. Postoje dva glavna tipa šifrovanja podataka u računarskim fajl sistemima: šifrovanje fajlova i foldera (engl. *File/Folder encryption*) i šifrovanje celog diska (engl. *Full-Disk encryption – FDE*).

**Kriptografija** je nauka koja se bavi metodima očuvanja tajnosti informacija. Tehnike kriptografske zaštite informacija obezbeđuju:

- **Integritet ili verodostojnost informacija**, koje se šifruju, (engl. *Data integrity*) se brine o tome da ne dođe do neovlašćene promene informacija, kao što su menjanje informacije, brisanje informacije i zamena informacije. Da bi se osigurala verodostojnost, mora postojati način provere da li je informacija promenjena od strane neovlašćene osobe.
- **Tajnost** (engl. *Confidentiality*) informacija osigurava da je sadržaj informacije dostupan samo ovlašćenim osobama odnosno samo osobama koje poseduju ključ. Postoje brojni načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama kojima se podaci šifruju.
- **Provera identiteta** (engl. *Authentication*) - korisnici koji počinju komunikaciju treba prvo da se predstave jedan drugome pa tek onda počinju sa razmenom informacija.
- **Nemogućnost izbegavanja odgovornosti** (engl. *Non-repudiation*) je vrlo važna stavka, pogotovo u novije vreme kada se veliki deo novčanih transakcija obavlja putem Interneta[1].

Danas je kriptografija usavršila mnoge sisteme i učinila ih naprednim i bezbednim. U radu je predstavljeno unapređenje programa za obradu teksta Microsoft Word, programskog paketa Microsoft Office, sa ciljem da se primenom kriptografskih tehnika šifrovanja podataka osigura tajnost tekstualnih podataka koji se razmenjuju između različitih korisnika. Ovakvo unapređenje se može koristiti u različitim sistemima razmene dokumenta počevši od tradicionalnih sistema razmene podataka baziranih na deljenim fajlovima pa sve do savremenih sistema

elektronske razmene dokumenata (engl. *Electronic Data Interchange - EDI*).

## 2. ELEKTRONSKA RAZMENA DOKUMENATA

*EDI - Electronic Data Interchange* (slika 1) predstavlja međunarodni standard za razmenu poslovnih dokumenata u digitalnom obliku. To je zajednički jezik kojim kompjuterski sistemi samostalno ili polu-automatizovano razmenjuju dokumente različitih tipova kao što su na primer porudžbenice, otpremnice, fakture, izveštaji i slično. Ovakvom automatizacijom prenosa podataka eliminiše se potreba za angažovanjem ljudskih resursa, jer dokumenti idu iz jednog sistema u drugi elektronski, čime se ubrzava rad, umanjuje mogućnost greške.

Pet osnovnih prednosti upotrebe *EDI* razmene dokumenata:

- Apsolutna tačnost između poslatih i primljenih podataka, što isključuje faktor ljudske greške pri prekućavanju,
- Brzina slanja i prihvata podataka je drastično ubrzana u odnosu na manuelni unos podataka,
- Uštede u poslovanju (vreme, radna snaga, potrošni materijal),
- Povećana produktivnosti
- Unapređeno upravljanje logistikom.



Slika 1. *Electronic Data Interchange*

Samim tim što sistemi komuniciraju bez intervencije ljudi postiže se maksimalna tačnost između poslatih i primljenih podataka. Brzina slanja omogućava veće pogodnosti kod prijema dokumenata. Podaci se primaju na vreme, čime se povećava vreme za pravovremenu reakciju u slučaju potrebe i omogućava lakši rad ljudi na prijemu dokumenata.

Primena Interneta u obavljanju *EDI* transakcija (*InternetEDI* tj. *XML/EDI*) omogućila je mnogim srednjim i malim preduzetnicima da iskoriste prednosti *EDI* transakcija bez značajnijih finansijskih ulaganja. Jezik *XML* (engl. *eXtended Markup Language*) je podignut na nivo standarda, koji je pre nekoliko godina prihvatio *Microsoft* i počeo da implementira u svojim

programskim paketima. S obziromna činjenicu da je neutralan po pitanju formata, *XML* predstavlja standardni jezik za razmenu podataka, koji omogućava konzistentne dokumente i njihovu razmenu između kompanija, bez potrebe za bilo kakvim konvertovanjem.

## 3. ANALIZA PROBLEMA I POSTOJEĆA REŠENJA

Sve veće kompanije imaju svoje partnerske firme ili svoje odseke koje/i za nju obavljaju određene poslove. Postavlja se pitanje kako će direktor kompanije imati uvid u kvalitet rada partnerskih firmi? Kako može proslediti svoje zahteve podređenima? Svaka potčinjena firma ima svog nadređenog koji izveštava, komunicira sa direktorom kompanije putem *EID*-a. Veliki broj dokumenata koji se elektronskim putem razmenjuje, najčešće u formi izveštaja, pisan u *Microsoft Word* aplikaciji (sa *.doc/.docx* formatom), je danas opšte prihvaćen u ljudskoj populaciji.

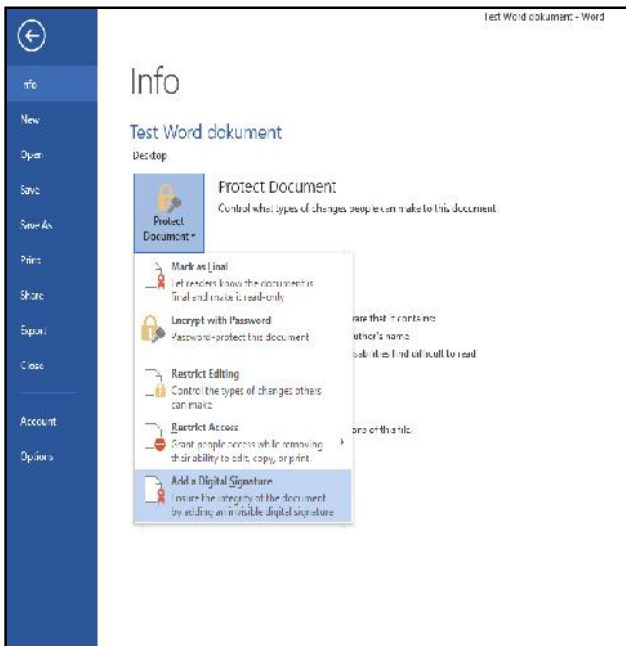
*Microsoft Word* je program za obradu teksta, u okviru programskog paketa *Microsoft Office*. *Microsoft Word* već u toku same obrade teksta prikazuje kako će isti izgledati kada se bude odštampao. Kao i drugi alati *Microsoft Office*-a, *Microsoft Word* može biti oblikovan tako da odgovara konkretnim korisničkim potrebama. Takođe, moguće je dodavati mu i nove mogućnosti, koristeći jednostavan jezik makroa, koji se prvobitno zvao *WordBasic* (danas *Visual Basic for Applications*). Ovaj program je jednostavan za upotrebu.

Prilikom upotrebe *EDI*-a, podaci u dokumentu se prenose u otvorenom tekstu, bez ikakvog nivoa zaštite (zavisi od namene kompanije). Podaci, najčešće u vidu teksta, su u potpunosti dostupni neželjenim korisnicima.

Drugi veliki problem je problem **kolaboracije**- rad većeg broja učesnika u komunikaciji nad istim dokumentom. Potrebno je obezbediti pravila: dozvole/zabrane menjanja (engl. *modify*), čitanja (engl. *read only*) dokumenta. Pored ostalih funkcionalnosti u *Microsoft Word*-u implementirana je mogućnost zaštite dokumenta gde se može:

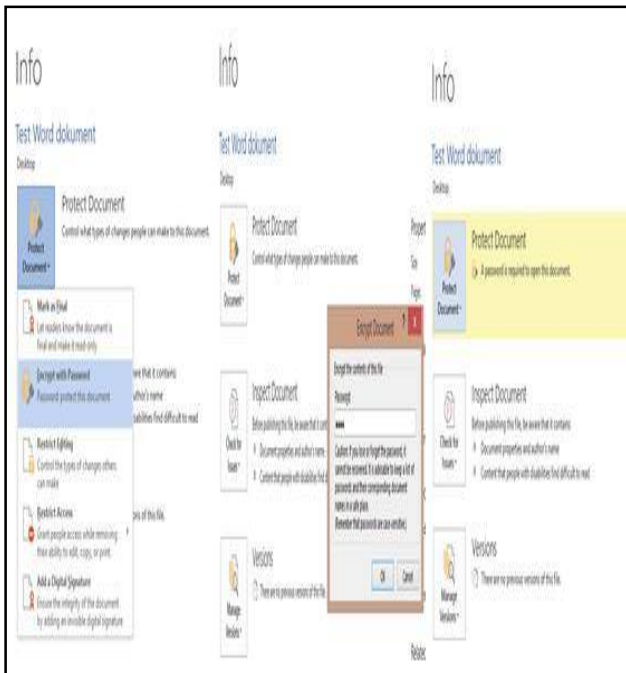
- Zaštiti dokument upotrebom digitalnog potpisa,
- Zaštiti dokument u globalu (opcija *Protect document*) upotrebom *password*-a (zaštita fajla /foldera) i
- Definisati pravilo/a za određene korisnike (koje/a se odnose na dozvole I zabrane).

Nivo zaštite koji se koristi danas u velikim, razvijenim kompanijama je digitalni potpis (engl. *Digital Signature*) dokumenta (slika 2). Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), potvrdi integritet kao i da obezbedi garantovanje identiteta pošiljaoca poruke. Pomoću svog potpisa korisnik ovlašćuje neku radnju i preuzima odgovornost za nju.



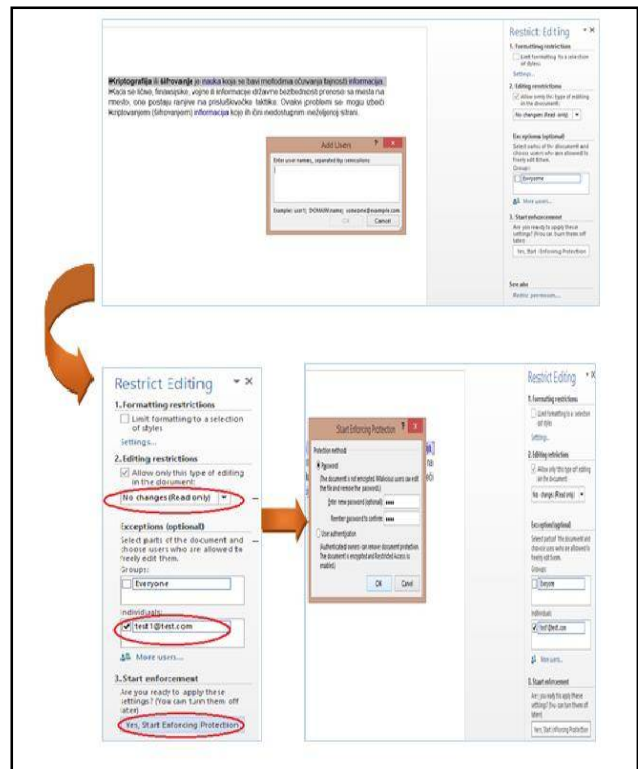
Slika 2. Upotreba digitalnog potpisa u aplikaciji *Microsoft Word*

Drugi navedeni nivo zaštite omogućava autentikaciju korisnika. Ukoliko *password* nije validan korisnik neće moći da pročita/modifikuje dokument (slika 3).



Slika 3. File encryption u *Microsoft Word-u*

U zavisnosti od navedenih pravila, koja su definisana u trećem nivou zaštite, korisnik ima pravo samo da čita dokument ili modifikuje i čita (slika 4). O pravilima odlučuje master (osoba koja sačinjava dokument) [3].



Slika 4. Definisane pravila/ograničenja za korisnike u *Microsoft Word-u*

Međutim, i pored navedenih zaštita, svi korisnici ipak mogu da pročitaju dokument u potpunosti, a samo određenida ga modifikuju, komentarišu. Suština je da svaki korisnik može da pročita u svakom dokumentu samo ono od značaja za obavljanje dužnosti na svom random mestu, a ostalo ne. Rezimirajući ova tri nivoa zaštite ustanovljeno je da implementirane funkcionalnosti, koje dolaze kao deo *Microsoft Word* aplikacije, ne zadovoljavaju jedan od osnovnih kriptografskih mehanizama - **tajnost** podataka. Takva funkcija, za očuvanje tajnosti podataka, u *Microsoft Word-u* ne postoji.

Rešenje je implementacija dodatka (*Add-In*) za *Microsoft Word* realiuovana u razvojnom alatu *Microsoft Visual Studio 2010* u programskom jeziku *C#*. Rešenje nudi šifrovanje selektivno odabranog dela teksta sa ciljem da se obezbedi tajnost tačno odabranog dela teksta. Šifrovani tekst postaje nečitljiv. Na taj način se sprečava mogućnost odliva bitnih informacija kao i zloupotreba istih.

#### 4. DODATAK (ADD-IN) ZA MICROSOFT WORD APPLICATION

Kompanije već dugo vremena oslanjaju se na *Microsoft-ovu* aplikaciju *Office* kako bi pomogla u pokretanju svojih dnevnih rutina. Kao i kod mnogih drugih *Microsoft* proizvoda, *Office* aplikacije su takođe veoma prilagodljive.

##### 4.1 ALATI ZA REALIZACIJU

Razvijanje aplikacija za *Office* proizvode, a naročito za *Office 2007* i *2010*, najbolje se realizuje pomoću *Visual*

*Studio Tools for Office* ili *VSTO*. Sa *VSTO* u *Visual Studio 2010*, i novijim verzijama, mogu se kreirati različite vrste aplikacija koje koriste *Office* proizvode kao platformu. Na primer, možete kreirati dodatke na nivou aplikacije, prilagođavanja na nivou dokumenta, template, i tako dalje. Kao što možete pretpostaviti, možete razviti svoje aplikacije iz *Visual Studio IDE*. Pomoću *VSTO* takođe možete kreirati sopstvene funkcionalnosti na *Ribbon-u* (panelu/toolbox-u), na primer dodavanjem dugmadi ili kreiranjem novih grupa komandi.

*Ribbon Designer* predstavlja sastavni deo *VSTO* počevši od verzije 2007. To je alat za dodavanje kartica, grupa i kontrola u *Toolbox* aplikacije *Microsoft Office*[4]. “ZASTITA DOKUMENTA” je Add- In (prilagodjeni dodatak, tačnije kartica) za *Microsoft Word* implementiran u *Visual Studio 2010* razvojnom okruženju u programskom jeziku C#. Implementacija dodatka (Add-in-a) realizuje se u dva dela:

- Dizajniranje kartice (*Ribbon Designer*)
- Funkcionalnost kartice (Šifrovanje/dešifrovanje selektovanog teksta, konvertovanje dokumenta u PDF).

Izgled kartice uključuje komponente alata za dizajniranje. U projektu su upotrebljena tri dugmeta, labela i editBox. Dok je korisnički interfejs (vizuelni deo) jednostavnog koncepta, u pozadini komponenti je implementirana složena logika: šifrovanje/dešifrovanje kriptografskim algoritmom.

## 4.2 IMPLEMENTACIJA I FUNKCIONALNOST KORISNIČKOG INTERFEJSA

Kriptografski algoritmi se koriste za šifrovanje poruka, odnosno za njenu transformaciju iz otvorenog u šifrovani oblik. Dva osnovna načina šifrovanja su simetrično šifrovanje i asimetrično šifrovanje. Simetrični zahtevaju postojanje istog ključa i procesnog algoritma na obe strane veze. Oni koriste tajni ključ koji se mora dobro zaštititi. Tajnost ključa je esencijalna za bezbednost podataka u sistemu. Svaka osoba koja koristi ovaj sistem mora da poseduje ključ. Šifrovanje se obavlja u blokovima (blok po blok) ili protočno (bit po bit ili bajt po bajt).

Implementacija predloženog dodatka (*Add-In-a*) ogleda se u realizaciji šifrovanja/dešifrovanja selektovanog dela teksta upotrebom simetričnog kriptografskog algoritma *AES* (engl. *Advanced Encryption Standard*) u modu ulančavanja blokova – *CBC mod* (engl. *Cipher Block Chaining*). *AES* algoritam koristi 128-mo bitni ključ i radi nad 128-mo bitnim blokom podataka (slika 5). Moguće ga je proširiti na upotrebu ključa od 192 i 256 bita. Kod *AES* algoritma, blok podataka organizovan je u tabeli od četiri puta po četiri znaka. Karakteriše ga mala brzina izvršavanja, relativno velika dužina ključa a kao posledica toga i zadovoljavajuća kriptografska sigurnost. Predstavlja javno dostupan algoritam i najčešće je upotrebljavani kriptografski algoritam[5]. Za heširanje se koristi *hash* funkcija *SHA256* (engl. *Secure Hash Algorithm 256*).

```
using (RijndaelManaged AES = new RijndaelManaged())
{
    AES.KeySize = 256;
    AES.BlockSize = 128;

    var key = new Rfc2898DeriveBytes(passwordBytes, saltBytes, 1000);
    AES.Key = key.GetBytes(AES.KeySize / 8);
    AES.IV = key.GetBytes(AES.BlockSize / 8);

    AES.Mode = CipherMode.CBC;

    using (var cs = new CryptoStream(ms, AES.CreateEncryptor(), CryptoStreamMode.Write))
    {
        cs.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
        cs.Close();
    }
    encryptedBytes = ms.ToArray();
}
```

Slika 5. Upotreba *AES-a* u *CBC* modu rada

Prilikom kreiranja projekta postoje standardne datoteke koje su njegov sastavni deo kao npr. “ThisAddIn.cs”. One su globalne i ne treba ih menjati. Ne utiču na funkcionalnost projekta.

Logika šifrovanja i dešifrovanja pripisana je kontrolama *Ribbon Designer-a*. Pri prvom pokretanju projekta (engl. *Build*) implementiran dodatak (*Add-In*) se automatski vezujeza *Microsoft Word* aplikaciju kao posebna komponenta sa implementiranim kontrolama. Nakon ugrađivanja *Add-In-a* uticaj korisnika ima najznačajniju ulogu. Od korisnika zavisi upravljanje zaštitom informacija. Korisnik je taj koji bira koji deo teksta će biti kriptografski obrađen.

## 4.3 KORISNIČKI INTERFEJS

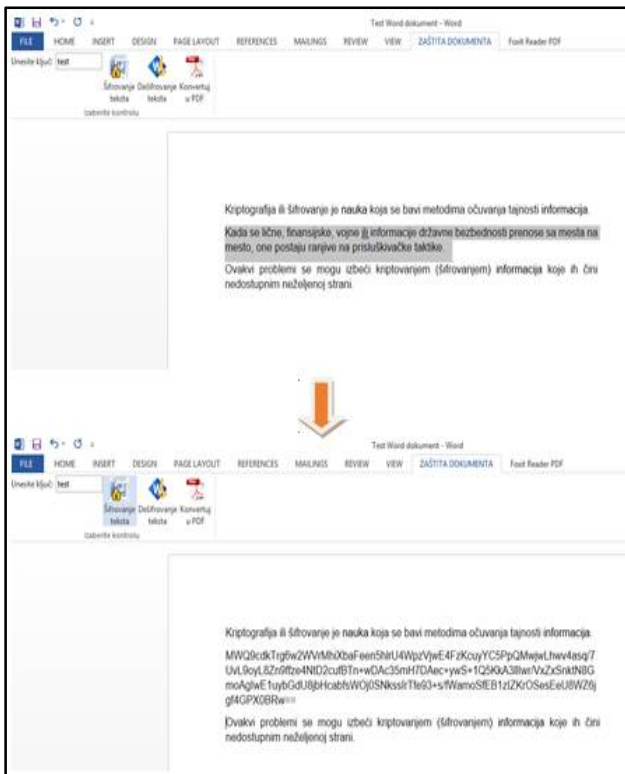
Prilikom pokretanja *Microsoft Word* aplikacije prikazuje se korisnički interfejs. Korisnički interfejs se sastoji od par kartica kao što su Home, Insert, Design, ... Svaka kartica ima komponente sa funkcionalnim kontrolama pa tako I novoimplementirana kartica “ZASTITA DOKUMENTA” (slika 6).



Slika 6. Korisnički interfejs

Prilikom selektovanja teksta treba uneti ključ za šifrovanje u labelu “Unesite ključ”. Zatim, klikom na dugme “Šifrovanje eteksta” postojeći selektovani tekst postaje šifrovan tj. nerazumljiv za korisnike (slika 7).





Slika 7. Šifrovanje selektovanog teksta klikom na dugme “Šifrovanje teksta”

Novodobijeni dokument master prosleđuje korisnicima gde samo osoba koja zna ključ može dešifrovati tekst. Dešifrovanje je inverzna operacija operaciji šifrovanja. Dešifrovanje se izvodi (pod uslovom da je dozvoljena modifikacija dokumnta od strane master-a):

- Selektovanjem šifrovanog teksta,
- Unosom validnog ključa za dešifrovanje i
- Klikom na dugme “Dešifrovanje teksta”.

Ukoliko nije dozvoljena modifikacija dokumenta korisnik ima mogućnost samo da čita dokument. Pored uvođenja tajnosti podataka mogu se primeniti i već postojeći nivoi zaštite koji mogu dodatno omogućiti bezbedan transfer informacija. Primenom AES kriptografskog algoritma kriptografska snaga celokupnog rešenja je podignuta na nivo koji definiše standard AES kriptografskog algoritma.

Add-In je relativno nova stvar koju treba usavršiti, unaprediti i uvesti u upotrebu jer prilikom ostvarivanja komunikacije dva ili više korisnika postojeće rešenje ne obzbeđuje, u potpunosti bezbedan protok podataka.

## 5. ZAKLJUČAK

Nagli razvoj tehnologije računarskih sistema i mreža, doveo je do masovne razmene informacija i podataka. U toj razmeni pojavila se potreba za zaštitom poverljivih podataka od raznih krađa i zloupotreba, što je uslovalo pojavu novog pravca u oblasti bezbednosti podataka. Dalji razvoj tehnologije doprineo je poboljšanju karakteristika metoda koje doprinose bezbednosti podataka. Međutim, isti taj napredak doveo je do bržeg otkrivanja nedostataka i dodatno omogućio eventualne

zloupotrebe. Tako su, tokom vremena, metode za zaštitu podataka postale sve složenije i naprednije.

U osnovi priče o bezbednosti podataka nalazi se Kriptografija. Kriptografija je veoma široka oblast, a u praksi se bazira na upotrebi kriptosistema koji se sastoje od algoritama za kriptovanje, jednog ili više ključeva, sistema za upravljanje ključevima, podataka u vidu standardnog i kriptovanog teksta. Na složenost dodatno ukazuju i činjenice da se kriptosistemi mogu realizovati hardverski, softverski ili hardversko-softverski, kao i to da se prilikom realizacije moraju zadovoljiti osnovni sigurnosni servisi[4]. Uprkos tome, napredak u postojećim kriptografskim algoritmima nastavlja se rastućim tempom, da bi zadovoljio potrebe širenja IT društva u kome živimo.

Imajući u vidu činjenice da je Kriptografija veoma dinamična oblast, da je aktuelna i da je veoma rasprostranjena, ovim radom je obuhvaćen samo jedan deo njenog osnovnog koncepta. Razmatrane su kriptografske metode i algoritmi, kao i mogućnost unapređenja bezbednosti podataka realizacijom sopstvenog rešenja. Ukazano je na osnovne sigurnosne servise koji se u cilju sigurnosti moraju zadovoljiti primenom kriptografskih metoda. Cilj ovog rada je da ukaže na nužnost zaštite podataka i prikaže napredne mehanizme za njihovu zaštitu.

Sigurno je da će se kriptografija razvijati sve bržim i bržim koracima. Upotreba kvantnih računara, računarskih gridova kao i sve masovnije upotrebe računarskih mreža samo su jedan od nagoveštaja budućnosti. U skladu sa tim će se postavljati sve veći sigurnosni zahtevi u smislu ranog otkrivanja i sprečavanja zloupotreba. Odgovor na ove zahteve je upravo upotreba savremenijih i sigurnijih kriptografskih algoritama, koji će prevazilaziti granice jednostavne bezbednosti.

## LITERATURA

[1] William Stallings “Cryptography and Network Security: Principles and Practice“, Fourth Edition, Prentice Hall, London, 2005.

[2] <http://www.8bit.rs/edi>

[3] <https://onedrive.live.com/view.aspx?resid=F96ED643B0D75754!977&app=Word>

[4] <https://msdn.microsoft.com/en-us/library/bb386089.aspx>

[5] Jovana Đurović, Boban Mihailov, Ivan Tot, “CryptoSMS ANDROID APPLICATION“, Konferencija o bezbednosti informacija BISEC 2016, Univerzitet Metropolitan, Beograd



# ANALYSIS AND IMPLEMENTATION OF AES CRYPTOGRAPHIC ALGORITHM ON CUDA GRAPHIC PROCESSING UNITS

Boriša Jovanović<sup>1</sup>, Ivan Tot<sup>2</sup>, Slavko Gajin<sup>3</sup>

*Center of Applied Mathematics and Electronics, General Staff of Serbian Armed Force<sup>1</sup>  
Military Academy, University of Defence, Belgrade, Serbia<sup>2</sup>  
School of Electrical Engineering, University of Belgrade, Serbia<sup>3</sup>*

**Abstract** - *The need to encrypt data is becoming more and more necessary. As the amount of data continues to grow, the speed of encryption must increase to keep up or it will become a bottleneck processing and data exchange. In the past few years, graphics processors are increasingly used for the general purpose calculation. Their intense development has led to their application in a wide range of scientific and commercial applications. In order to improve the performance of the implementation of AES cryptographic algorithm, this paper proposed a CUDA implementation of Counter mode AES encryption on GPU.*

## 1. INTRODUCTION

Graphics processors have been the subject of extensive research in recent years and have been successfully applied to general purpose applications beyond the realm of graphic processing. They are designed to perform hundreds of billions of floating-point operations per second using their embedded memory with a large bandwidth. Since its introduction graphic processors are used for specialized, computationally-intensive calculations in the field of computer graphics. Due to the specific requirements regarding processing graphics, development of graphics processing units (GPUs) went into the other direction in comparison to central processing units (CPUs). Within the central processor unit, a large number of transistors are dedicated to caching data and control flow mechanisms. With graphics processors flow control is simplified, and the delays that occur as a result of access to slow, global memory are compensated by the intensive use of threads. For modern, multicore CPUs it is enough to run several threads for efficient program execution. Graphics processors have a large number of less processing power cores and it is necessary to run several thousand of threads to achieve maximum efficiency. Today's GPUs have great processing power and memory bandwidth, and therefore are suitable for solving computationally complex problems. Now, the graphics processors are used extensively in a variety of scientific and commercial spheres, such as computational physics and chemistry, the analysis of financial data, research of mineral resources etc.

Programming graphics processors is done through dedicated application program interfaces (APIs). Applications are typically executed in the coprocessing regime, where the sequential parts of the application are run on the CPU, and the computation intensive parts are run on the GPU[1]. To obtain maximum performance, it

is necessary to know the architecture and organization of the graphics processor, and accordingly make certain adjustments to the programming code. Since modes for accessing and storing data in memory significantly affect the performance of program execution, it is necessary to know the memory hierarchy of these processors. Access to the global memory is slow, therefore graphics processors have smaller capacity memory, which can fix performance of a program. This paper presents the possibility of using graphics processors in the area of cryptography data processing and improvement of the cryptographic algorithms performance in case of AES cryptographic algorithm.

The paper is divided into several parts. The second section provides a brief overview of CUDA technology which allows the use of GPUs as general purpose processors. The third part briefly describes AES as standard symmetric block cryptographic algorithm and possible modes of operation. The fourth part describes the implementation of the CTR mode of the AES cryptographic algorithm on CUDA GPU. In the fifth section the results achieved by implementing the AES cryptographic algorithm on CUDA GPU are presented and analyzed. Finally, the conclusion is presented with regard to the suitability of using CUDA GPUs as cryptographic coprocessors.

## 2. CUDA GRAPHIC PROCESSOR AS GENERAL PURPOSE PROCESSOR

For a long time GPUs have been developed as a dedicated processors, primarily for rendering 3D graphics. The whole processing was performed within a fixed, graphic pipeline. Because of the need to create complex visual effects, GPUs have evolved and provide some kind of programmability through the graphics application program interfaces such as OpenGL and DirectX[2]. At that point, some researchers have recognized the potential of graphics processors in general purposes calculations. Since the only possible way was the use of graphical programming application programming interface, the first step was to describe desired problem by using graphics primitives, then to write the appropriate shader program, and finally to convert back the results obtained in the form of pixels into data that make sense to developers and which can be interpreted in determined, desired fashion. The coding process was associated with many problems, such as poor support for working with integers and floating point double precision numbers, and limitations regarding memory access. Also, the lack of adequate software support, tools and libraries made the

development of the programs more difficult. Despite these obstacles, there was significant acceleration for specific application domains, as described in[3].

The earlier mentioned researches had impact on some graphics processors manufacturers, who noticed their potential for general purpose calculation and, accordingly, made changes and adjustments in their architecture. CUDA is a parallel computing architecture developed by NVIDIA, which first provided the possibility for resolving the general computational problems by using graphics processors. CUDA provides generic, parallel programming model for programming GPUs in multithreaded environment with significantly better support for synchronization, atomic operations and memory access. Application programming is available through the appropriate application programming interfaces and extensions of the C programming language.

CUDA programming model-paradigm organizes the application in the form of a sequential host program running on the CPU and which, if necessary, calls specialized kernel functions that are executed in parallel on GPU. In essence, the kernel is executed in SPMD programming model by a large number of lightweight threads. One kernel can be executed on multiple processing units (streaming multiprocessors). Each multiprocessor within the graphics processor is a SIMD architecture processor and consists of a large number of scalar processors which execute single threads.

In order to achieve scalability in program execution on hardware with different amounts of resources and available multiprocessors, programmer organizes threads into blocks of threads and kernel execution is organized in the form of the grid (Figure 1). Blocks of threads are distributed on multiprocessors for execution, while all the threads that are executed within one multiprocessors share the available resources, such as registers and shared memory within the multiprocessor. The number of threads within a block and the number of blocks within the grid is set by executable kernel configuration, which is typical work done by the central processor. In order to support different types of memory accesses and data addressing threads can be logically organized into a multidimensional block and grid (one-dimensional, two-dimensional and three-dimensional). In doing so, each thread within a block has a unique identifier, and each block has a unique identifier within the grid by all three possible dimensions. Threads can access these identifiers using the built-in variables visible at kernel level. Typically, threads use these identifiers to make decisions about branching or to determine the address of data in memory[4]. Within the same block, threads can perform the synchronization using the implemented synchronization of the barrier. Since the blocks of threads can run on a variety of multiprocessors, there is no way for the global synchronization during the kernel execution. Global synchronization is achieved through multiple kernel calls which is one of the many core processor architecture limitations.

CUDA architecture offers specific memory hierarchy in order to support the execution of a large number of threads in parallel. That memory hierarchy is the consequence of the basic graphics processors purpose - graphics processing. When rendering a 3D scene, the input data is usually processed only once in a single step while access to them is done on a strictly coherent manner, in accordance to the principles of spatial and temporal locality. Rendering algorithms usually access continuous memory locations simultaneously which allows efficient use of bandwidth. To support these access ways, global graphics processors memory is organized in the form of memory banks in order to provide simultaneous access to adjacent memory locations. The graphics processor memory architecture is oriented towards increasing the bandwidth, and not by reducing latency as is the case with the central processor. Therefore, instead of using cache memories, graphics processors effectively hide memory access latencies by using massive parallel execution[5].

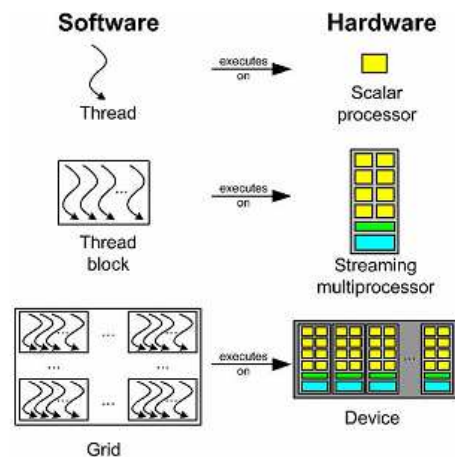


Figure 1. Execution program model on CUDA graphic processor

During program execution, CUDA threads can access different parts of memory. Each thread has its own private local memory, each block of threads has a shared memory which can be accessed by any thread within the block and whose life expectancy is identical to lifetime of the block. All threads can access a shared global memory. There are two additional memory spaces which are available to all threads but only for reading the content: constant memory and texture memory. Newer generation of graphics processors allow writing in textures memory using special primitives.

### 3. AES CRYPTOGRAPHIC ALGORITHM

AES cryptographic algorithm first appeared in 1997 as Rijandel algorithm. In 2001., after a five-year process of standardization, it was elected as the most suitable replacement for the previous standard cryptographic algorithm DES by the NIST[6]. Since then it has become one of the most popular and probably the most widely represented and applied block cryptographic algorithm.

AES algorithm implements operations of encryption and decryption of 128 bits blocks of data in a variable number of cycles. The number of cycles depends on the key size and is 10/12/14 cycle-rounds for 128/192/256 bit key size, respectively. Before the encryption or decryption process, key expansion is done according to pre-described algorithm. The process of encryption of the data can be briefly summarized as follows: firstly an initial cycle (AddRoundKey function) is implemented, and then  $r$  standard cycles whose number depends upon the length of the applied key. First  $r-1$  cycles are identical and include four transformations:

- Nonlinear bytes replacement using substitution tables (function ByteSub),
- Change of bytes order within the same row (function ShiftRow),
- Transformation of bytes within the same column (function MixColumn),
- Addition by moduo two with the appropriate part of the key (function AddRoundKey).

In the last cycle of encryption, no transformation of bytes within the same column is done (function MixColumn).

Despite its complexity, the AES algorithm, or any block cryptographic algorithm, basically represents substitution of a letter with a letter, using 128-bit characters when it comes to AES. Whenever it encounters the same block of plaintext, using the same cryptographic key, the algorithm produces the same ciphertext block. The potential attacker can you take advantage of this feature to make electronic codebook (the set of all pairs of a block of plaintext - ciphertext block), in order to better exploit the shortcomings of cryptographic techniques. Therefore, the block cryptographic algorithms are used in one of the modes. Cryptographic mode is a way to use the basic cryptographic algorithm and is usually a combination of some types of feedback loops and some simple operations. Operations that are applied in the algorithm are usually simple because the safety is set by basic cipher algorithm and not by cryptographic mode. In 2001, NIST has released five recommended modes of AES cryptographic algorithm[7]: ECB, CBC, CFB, OFB and CTR. These modes have different characteristics and parallelization capabilities caused by the very differences within the modes. A brief description, comparison and parallelization capabilities of these modes is given in Table 1.

One of the most important things in the AES algorithm is the key expansion algorithm. This algorithm is used to generate a set of subkeys  $K_r$  and to load then in a linear array  $W$ . The length of the linear array  $W$  depends on the size of a block of plaintext to be treated. It includes subkeys  $K_r$  for each cycle  $r$ . Details of the AES algorithm can be found in [8][9].

Table 1. Block cryptographic algorithm modes

Mode	Description	The possibility of parallelization
ECB	For the given key, block cryptographic algorithm is directly and independently applied to the each block of plaintext	Suitable for parallelization
CBC	In this mode, firstly "exclusive or" (XOR) operation is executed between a block of plaintext and the immediately preceding block of ciphertext, and then the obtained block of data is encrypted using applied cryptographic algorithm.	The decryption process is suitable for parallelization
CFB	In this mode, the successive segments of ciphertext are used as part of the input block of block cryptographic algorithm and with obtained output data block "exclusive or" (XOR) operation is executed with a block of plaintext.	Not suitable for parallelization
OFB	Encryption of the initial vector values is done in several iterations using the applied block cryptographic algorithm in order to produce an output block. This output block becomes the new value of the initial vector for the next iteration. On such obtained output data block "exclusive or" (XOR) operation is executed with a block of plaintext.	Not suitable for parallelization
CTR	Block cryptographic algorithm is applied to the set of input blocks, which are called counters, in order to obtain a set of output blocks. On such obtained set of output blocks "exclusive or" (XOR) operation is executed with a set of plaintext blocks.	Suitable for parallelization

Input data for cryptographic processing for CBC, SFB and OFB modes, in addition to a block of plaintext, is block of data, which is called the initial vector (IV). New and different value of the initial vector must be generated prior to execution of each encryption operation, while the

same value of initial vectors is required on the receiving part of encrypted message to allow the decryption process. It should be noted that in CBC mode chaining mechanism binds ciphertext blocks in a way that a result of the previous encryption blocks are used in the encryption of the current block. In other words, each block is used to modify the encryption of the next block so that each ciphertext block depends not only on the current block of plaintext but also on all previous plaintext blocks. Based on this, it can be concluded that the process of encryption by using CBC mode of operation is not suitable for parallelization. In the process of decryption by using CBC mode, the input blocks of decrypting function, ciphertext blocks are immediately available so that the decryption function using CBC mode can be implemented in parallel.

#### 4. DESIGN AND IMPLEMENTATION OF AES CTR MODE ON CUDA GRAPHIC PROCESSOR

This paper focuses on the CTR mode of AES cryptographic algorithm in which AES cryptographic data processing is applied on the counter value. On the obtained value and the corresponding plaintext block "exclusive or" (XOR) operation is applied in order to get block of encrypted text. This mode has two features which are advantages in the process of implementation on CUDA GPU. First, this mode retains the potential for parallelization on data block level, which is the highest possible level of parallelization available with AES cryptographic algorithm. Second, this mode does not perform the cryptographic processing on the blocks of plaintext but counter value. This fact provides the ability to reduce the amount of data that is transferred between the CPU and the GPU, while the final "exclusive or" (XOR) operation may be performed on the CPU or the GPU.

Many instances of parallelism are inherent in the AES cryptographic algorithm[10]. The highest level of parallelism is ensured by the independence of each 128-bit block of data, allowing each block of data to be cryptographically processed independently of the other blocks of plaintext. This independence is reduced in some modes of operation of block cryptographic algorithms but these modes are not the subject of this paper. Within the cryptographic processing of one data block, every function within the cycle-round can be implemented independently of other instances of the same function: each bytes replacement based on the s-box tables can be performed independently on all the bytes at the same time, each row can be rotated independently and simultaneously with the other rows, the data within one column can be transformed independently of any other column, each key element in round can be coupled with the corresponding element independently of other keys elements of rounds. In order to achieve maximum capacity utilization, it is sufficient to consider only the highest level of parallelism provided by each data block of plaintext. Each CUDA thread executes cryptographic processing operation of one 128-bit block of plaintext,

which as a result offers ability that 128-bit blocks are processed in parallel.

CUDA GPU has two different ways of implementation of the AES algorithm:

- Direct approach - all of previously mentioned algorithm functions are implemented as separate functions and then are called in the correct order as many times as defined by the algorithm itself,
- Application Lookup Table (replace tables) - an approach in which it is possible to increase the speed of execution of one block of data cryptographic processing operations by combining the functions *ByteSub* and *ShiftRows* with function *MixColumns* in which way they are converted into a series of lookup tables. This requires four tables, each with 256 32-bit values and needs a total of 4 KB (4096 bytes) of memory - 1 KB for each of the tables. Each round consists of 16 read operations of 32-bit values from replace table, 12 exclusive or operations on 32-bit words, and finally 4 exclusive or operations on the current state with the key elements of the round. Mathematical representation of this operation is given in (1). The entire round consists of four relations similar to one shown in (1). Symbol  $a_{i,j}$  represents given round input data, where the  $a_{i,j}$  denotes the  $j$ -th byte of 32-bit  $i$  word of the 128-bit input block of data;  $T_i[l]$  represents replace tables;  $\oplus$  denotes exclusive or operation and  $k_j$  represents  $j$ -th subkey of the given round.

$$e_j = T_0[a_{0,j}] \oplus T_1[a_{1,j-C1}] \oplus T_2[a_{2,j-C2}] \oplus T_3[a_{3,j-C3}] \oplus k_j \quad (1)$$

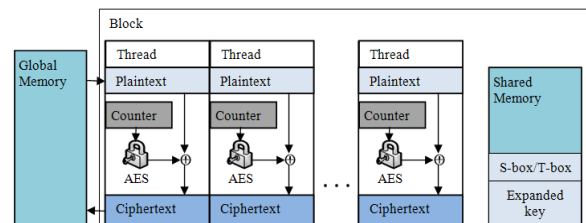


Figure 2. Implementation of AES algorithm CTR mode on CUDA graphic processor.

Regardless of the applied mode, the implementation of the AES algorithm on CUDA GPU can be present in the general scheme shown in Figure 2. The difference between these two modes is the concrete implementation of the AES operations, while all other steps are identical in both ways.

At the very beginning, the keys expansion algorithm is used to ensure the required number of keys for the rounds. Key expansion algorithm is executed on the CPU, because it is not necessary that each CUDA thread repeats this operation because the keys of the rounds obtained by keys expansion algorithm are identical for each block of plaintext of the current input data. The extended keys are then, along with replace tables and blocks of plaintext, copied to GPU memory. At this point the input data is divided into 128-bit blocks and each block is assigned a

single thread. Total number of CUDA blocks is calculated based on the total number of threads (the number of blocks of input plaintext) and selected value of CUDA threads of a CUDA block. Then, a specialized function (CUDA kernel) which executes AES algorithm, starts with a predetermined number of threads and blocks. Each thread first determines the unique identifier (number) which is then used to determine the value of the counter required for the CTR mode and for the access to the corresponding blocks of the input data. Next, the value of the counter is processed through AES cryptographic algorithm using the key obtained by the key expansion algorithm. The final step is exclusive or (XOR) operation between the obtained cryptographically processed value of the counter and the corresponding block of plaintext, which results in the ciphertext block. When all the threads complete their execution, the CPU copies the blocks of ciphertext from GPU memory to CPU memory, finishing the input data cryptographic process.

As a result of experiments, it is found that significant improvement in performance can be achieved when the execution of final exclusive or (XOR) operation is shifted away from the graphic to the central processor. In this way, the need to transmit open text data from the central processor to the graphics processor is eliminated, thus the amount of data that is to be transferred is effectively reduced by 50%.

## 5. RESULT ANALYSIS

This section presents the comparative results and performance of the AES cryptographic algorithm implementation on the CPU and CUDA GPU. Tests were conducted using the Intel (R) Core (TM) i7-2670QM 2.20GHz CPU with 8GB RAM and NVIDIA GeForce GT 540M graphics processor. For testing purposes, firstly custom implementation of the AES cryptographic algorithm for executing on the CPU was conducted and then the implementation intended to run on CUDA GPUs. As for both CPU and GPU, AES cryptographic algorithm is implemented using the approach based on the lookup tables.

Performance testing was conducted for the implementation of the mentioned algorithm with a 128 bits key length and 256 bits key length in CTR mode. Table 2 shows the results for encryption data operation with a 128 bits key length, while Table 3 shows the results of the encryption operation with a 256 bits key length. These tables show the file size of the input data that are cryptographically processed and the achieved results, the time of execution for the encryption input file operation on the graphics processor (GPU execution time) and the time of execution on the central processing unit (CPU execution time).

Time execution consists of reading the data from a file, encrypting the read data on the CPU or the GPU and writing of the results to a file for storing the encrypted data. These tables also show numeric acceleration that is

achieved by implementing AES cryptographic algorithm on CUDA GPU. The acceleration represents how many times the same amount of data is faster cryptographic processed using the AES algorithm in CTR mode on the CUDA GPU compared to processing on the CPU.

Table 2. Performance of AES algorithm implementation in CTR mode with 128 bits key length

Input file size	GPU execution time (ms)	CPU execution time (ms)	Acceleration
32 KB	0,056	<0	-
64 KB	0,108	1,00	9,26
128 KB	0,216	2,00	9,26
256 KB	0,421	4,00	9,50
512 KB	0,832	8,00	9,61
1 MB	1,655	16,00	9,67
2 MB	3,296	34,00	10,32
4 MB	6,528	65,00	9,88
8 MB	13,163	145,00	11,02
16 MB	26,313	262,00	9,96
32 MB	52,585	576,00	10,95
64 MB	105,244	1021,00	9,70

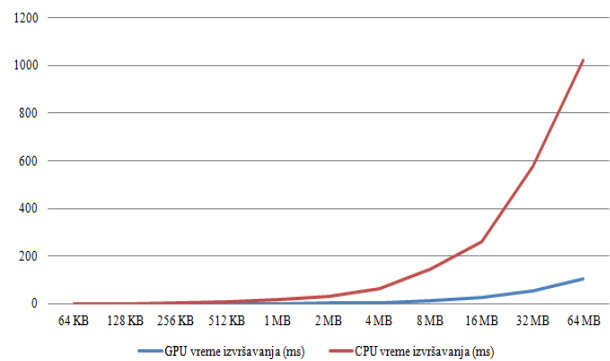


Figure 3. Graphical representation of performance of AES algorithm implementation in CTR mode with 128 bits key length on CUDA GPU and CPU.

Implementation of the AES cryptographic algorithm in CTR mode with a 128 bits key length on CUDA GPU is faster than identical implementation on the CPU for each input file size. To test the implementation with a 128 bits key length, input files larger than 32KB up to 64MB were used. Maximum acceleration for the implementation with a 128 bits key length, is achieved with file size of 8MB and is 11.02 times. Based on these results it can be concluded that the bandwidth of AES encryption algorithm implementation with a 128 bits key length of, in CTR mode on the NVIDIA GeForce GT 540M graphics processor is 4.75 Gb/s.



Table 3. Performance of AES algorithm implementation in CTR mode with 256 bits key length

Input file size	GPU execution time (ms)	CPU execution time (ms)	Acceleration
32 KB	0,074	<0	-
64 KB	0,145	1,00	6,90
128 KB	0,288	2,00	6,94
256 KB	0,568	4,00	7,04
512 KB	1,128	9,00	7,98
1 MB	2,242	19,00	8,47
2 MB	4,485	39,00	8,70
4 MB	8,950	76,00	8,49
8 MB	17,898	152,00	8,49
16 MB	35,786	433,00	12,09
32 MB	71,554	746,00	10,43
64 MB	143,139	1232,00	8,61

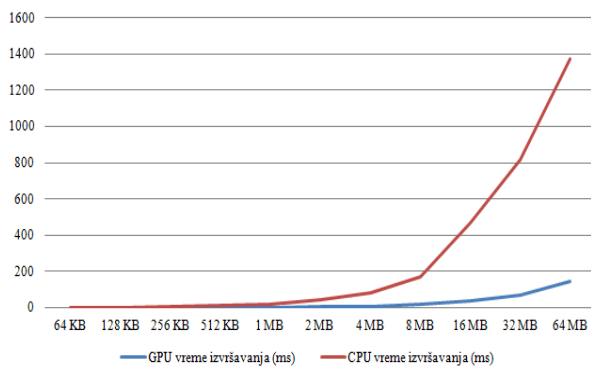


Figure 4. Graphical representation of performance of AES algorithm implementation in CTR mode with 256 bits key length on CUDA GPU and CPU.

Similarly, as can be seen in Table 3, implementation of the AES cryptographic algorithm in CTR mode with a 256 bits key length on CUDA GPU is faster than identical implementation on the CPU for each input file size. To test the implementation with a 256 bits key length, input files larger than 32KB up to 64MB were used. Maximum acceleration for the implementation with a 256 bits key length, is achieved with file size of 16MB and is 12.09 times. Based on these results it can be concluded that the bandwidth of AES encryption algorithm implementation with a 256 bits key length of, in CTR mode on the NVIDIA GeForce GT 540M graphics processor is 3.51 Gb/s.

## 6. CONCLUSION

This paper shows one possible approach for implementation of AES cryptographic algorithm in CTR mode on the general purpose GPU.

Analysis of the obtained results, both for 128 bits key length and 256 bits key length, shows that the acceleration of performance of cryptographic data processing using graphics processors is significant compared to their execution on the CPU. This implementation represents the proof that modern general purpose graphics processors, especially CUDA GPU, can be effectively used as cryptographic coprocessors. In further work, the implementation and analysis of other generally known symmetric cryptographic algorithms will be conducted. Also, on CUDA architecture general purpose graphics processors cryptographic compression functions can be implemented as well as the mechanisms of asymmetric cryptography.

## REFERENCES

- [1] M. Mišić, M. Tomašević, „Analiza performansi memorijske hijerarhije na CUDA grafičkim procesorima“, Proceedings of the 56th ETRAN Conference, Zlatibor, June 11-14, 2012.
- [2] Kirk, D. B., Hwu, W. M., „Programming Massively Parallel Processors: A Hands-on Approach“, Morgan Kaufmann, 2010.
- [3] Owens, J. D., Houston, M., Luebke, D., Green, S., Stone, J.E., Phillips, J.C., “GPU Computing”, Proceedings of the IEEE, vol. 96, No. 5., 2008., pp. 879–899
- [4] „NVIDIA CUDA C Programming Guide“, version 5.0, NVIDIA Corporation, 2012.
- [5] Kirk, D. B., Hwu, W. M., „Programming Massively Parallel Processors: A Hands-on Approach“, Morgan Kaufmann, 2010.
- [6] National Institute of Standards and Technology. (2010, July) Computer Security Resource Center. [Online]. <http://csrc.nist.gov/>
- [7] M. Dworkin, “Recommendation for block cipher modes of operation: methods and techniques,” Gaithersburg: U.S.Doc/NIST,2001.
- [8] J. Daemen, V. Rijmen, “AES Proposal: Rijndael”. Original AES Submission to NIST, 1999.
- [9] National Institute of Standards and Technology (NIST), “FIPS 197: Advanced Encryption Standard (AES)”, 2001.
- [10] Svetlin A Manavski, "CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography," in IEEE International Conference on Signal Processing and Communications (ICSPC 2007), Dubai, 2007.

# ELASTICSEARCH KLASTER I INDEKSIRANJE FAJLOVA

## ELASTICSEARCH CLUSTER AND FILE INDEXING

Zoran Denda<sup>1</sup>, Željana Vučetić<sup>2</sup>  
Ministarstvo odbrane<sup>1,2</sup>

**Sadržaj** – U ovom radu je opisan način kreiranja Elasticsearch klastera na linux operativnom sistemu CentOS i indeksiranje fajlova sa deljenih lokacija upotrebom C# programskog jezika.

**Abstract** - This document presents procedure to create Elasticsearch cluster on linux operating system CentOS and indexing shared files using C# programming language.

### 1. UVOD

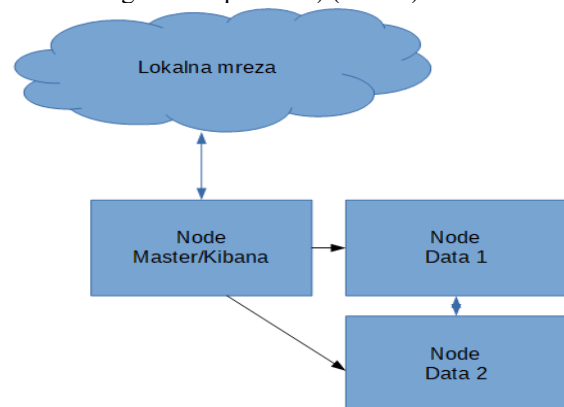
Vrlo često u različitim poslovnim okruženjima postoji potreba za jednostavnom i efikasnom pretragom sadržaja fajlova različitih tipova (word, excel, powerpoint, txt...). Operativni sistemi sami po sebi pružaju ovu mogućnost ali rezultati prilikom pretrage obično imaju nisku primenljivost i elementarnog su nivoa. Problem pretrage dobija na značaju kada kompanija ima ogromne količine fajlova (stotine hiljada), smeštenih na deljenim lokacijama gde pretraga podržana od sistemskog softvera gotovo da ne može da se koristi.

Predloženo rešenje u ovom radu se sastoji od nekoliko modula. Softver za indeksiranje i full-text pretragu je elasticsearch (search engine). Modul koji krajnji korisnici koriste za pretragu i analizu je Veb aplikacija Kibana. Servisni modul koji čita fajlove različitih tipova, transformiše ih u odgovarajući oblik i ubacuje u elasticsearch je implementiran u C# programskom jeziku. Okruženje u kome se ovo kompletno rešenje koristi se sastoji od mreže računara na Windows i Linux operativnim sistemima a fajlovi koji se indeksiraju i pretražuju (full text) su fajlovi iz programskog paketa MS Office (word, powerpoint) i txt fajlovi, dok je za sve ostale tipove fajlova (jpg, png, zip...) podržana samo pretraga po naslovu, autoru i datumima kreiranja i modifikacije (po metapodacima).

### 2. ELASTICSEARCH SERVER

Elasticsearch je *search engine*. On omogućava distriburanu, višekorisničku *full-text* pretragu sa http web interfejsom. Implementiran je korišćenjem Java programskog jezika. Podaci sa kojima elasticsearch radi su u JSON formatu [1]. Podaci se smeštaju u kolekcije podataka (indeksi) koje su pandam tabelama u SQL-u. Jedan elasticsearch server može da ima više kolekcija i prilikom upita (pretrage) moguće je pretraživati jednu ili više kolekcija. Podaci se skladište u kolekciji podataka upotrebom http web interfejsa (Rest API). Za C# programski jezik postoji podrška za ovaj rest API u vidu dve softverske biblioteke Elasticsearch.Net i NEST. U projektu prezentovanom u ovom radu je korišćen NEST. Nest je *high-level* biblioteka, koja mapira request i response objekte, podržava strogo tipiziran jezik za upite. Interno koristi biblioteku *low-level* Elasticsearch.Net. Elasticsearch klaster je konfiguracija više instanci

elasticsearch servera koji međusobno dele podatke, paralelno procesiraju upite i omogućavaju otpornost na otkaze. Elasticsearch se instalira na Linux distribuciji CentOS kao servis pomoću rpm paketa. Konfiguracija za servis se nalazi u yml fajlu. U implementaciji prikazanoj u ovom radu elasticsearch klaster se sastoji od tri instance CentOS servera gde je na svakom instaliran elasticsearch servis (slika 1). Jedan od njih je konfigurisan da radi kao master dok su ostala dva data nodovi (nod – instanca elasticsearch servera na operativnom sistemu). Master nod ima ulogu da upravlja ostalim nodovima, prihvata i deli upite na ostale data nodove, sumira rezultate upita i vraća rezultat pretrage klijentu. Data nodovi sadrže samo podatke. Skup podataka u jednoj kolekciji se deli na određeni broj podskupova (shard). Svaki od data nodova, disjunktivno, od ukupnog broja shard-ova uzima određeni broj koji su primarni (nad njima se izvršava pretraga) i određeni broj koji služe kao redudansa (u slučaju otkaza noda kod koga su oni primarni) (slika 2).



Slika 1. Arhitektura nodova.

id	index	shard	prirep	state	docs	store	ip	node
1								
2	testindex	3	r	STARTED	3	12.5kb	192.168.0.71	elasticdata1
3	testindex	3	p	STARTED	3	17.3kb	192.168.0.73	elasticdata2
4	testindex	4	r	STARTED	2	6.4kb	192.168.0.71	elasticdata1
5	testindex	4	p	STARTED	2	6.4kb	192.168.0.73	elasticdata2
6	testindex	1	r	STARTED	3	12kb	192.168.0.71	elasticdata1
7	testindex	1	p	STARTED	3	12kb	192.168.0.73	elasticdata2
8	testindex	2	r	STARTED	5	17.6kb	192.168.0.71	elasticdata1
9	testindex	2	p	STARTED	5	17.6kb	192.168.0.73	elasticdata2
10	testindex	0	r	STARTED	3	7kb	192.168.0.71	elasticdata1
11	testindex	0	p	STARTED	3	7kb	192.168.0.73	elasticdata2
12	.kibana	0	r	STARTED	2	9.9kb	192.168.0.71	elasticdata1
13	.kibana	0	p	STARTED	2	11.8kb	192.168.0.73	elasticdata2
14								

Slika 2. Raspored shard-ova po nodovima

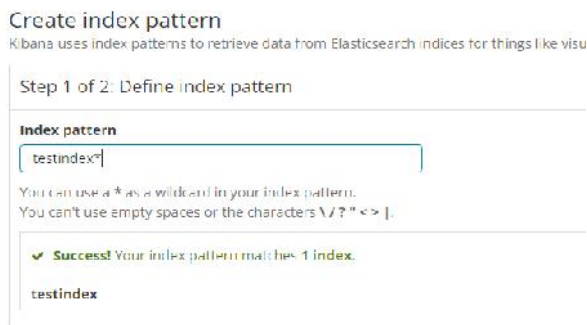
Elasticsearch klaster se uvek može proširiti novim nodovima i sam proces je prilično jednostavan. Dodaje se novi server (nod) u lokalnu mrežu dok se ostalima samo menja konfiguracija kako bi taj novi bio deo klastera. Za CentOS operativni sistem je još potrebno otvoriti portove 9200,9300 i 5601 na firewall-u. Ovi portovi su potrebni za sam pristup elasticsearch servisu (klijentski upiti - 9200), 9300 koristi sam elasticsearch za razmenu

podataka (replikacije i redudansa) dok se 5601 koristi za pristup Kibani. Ovo su osnovna podešavanja koja u konfiguraciji mogu da se promene.

Instalacije CentOS su minimalne, bez grafičkog okruženja tako da se za potrebe samog operativnog sistema koristi svega 250MB RAM memorije dok je sve ostalo za potrebe servisa [2].

### 3. KIBANA

Kibana je Veb aplikacija koji krajnji korisnici koriste za pretragu, analizu i vizuelizaciju [3]. Na CentOS distribuciji se instalira kao servis a pristupa joj se pomoću browser-a. U konfiguracionom fajlu se definiše koji se elasticsearch koristi prilikom upita. U konfiguraciji prikazanoj u ovom radu, Kibana je instalirana na istom CentOS-u koji je i master nod i konfigurisana je tako da upite šalje upravo tom master nodu. Da bi se Kibana koristila, potrebno je definisati koje indekse na elasticsearch serveru će da pretražuje. Indeksi se dodaju svojim punim imenom ili korišćenjem specijalnih karaktera. Na primer, ako postoje indeksi *analiza* i *analiza-godišnja*, mogu se dodati posebno a moguće je i dodati indeks *analiza-\** gde će se prilikom odabira poslednjeg i pretrage, automatski pretraživati obe kolekcije (indeksi) (slika 3).



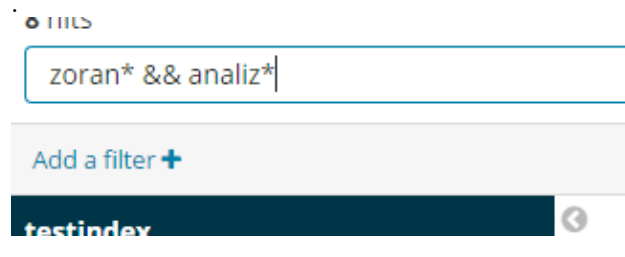
Slika 3. Kibana, odabir indeksa za pretragu

Zavisno od strukture indeksa koji se pretražuje ili više indeksa koji se pretražuju u jednom upitu rezultati će sadržati odgovarajuće kolone u rezultatu pretrage. Struktura indeksa, koja se definiše na elasticsearch serveru, preslikava se na kolone koje se prikazuju u rezultatima pretrage. Svaki zapis koji se dobije kao rezultat pretrage sadrži, pored polja (kolona) definisanih za strukturu kolekcije (indeksa) i neka ugrađena polja: index, score, \_id ,type.(slika 4).



Slika 4. Polja za pretragu i prikaz

Upiti se mogu postavljati na različite načine. Moguće je tražiti identično pojavljivanje stavljajući navodnike oko kriterijuma za pretragu ili koristiti specijalne i logičke operatore. Primer za upit bi bio: sve zapise sa odabranog indeksa (ili više njih) koji sadrže reči koje počinju rečju „analiz“ i bilo koju reč koja počinje sa „zoran“ (slika 5).



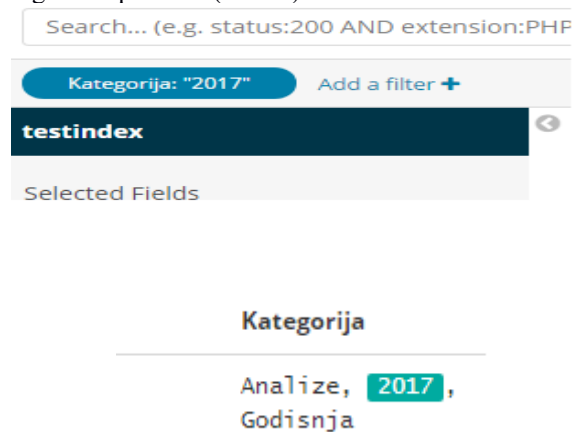
Slika 5. Upit, logički operatori i specijalni karakteri.

Kao rezultat ovakve pretrage dobija se sledeće (slika 6):

egorija	Naslov	Sadržaj
lize, 2017, isnja	[ I ] 2017 godisnja prezentacija	[ I ] 2017 godisnja <b>analiza</b> Zoran Denda Teme za <b>analizu</b> <b>Analiza</b> planova Realizacija planova Naucene lekcije Iskustva

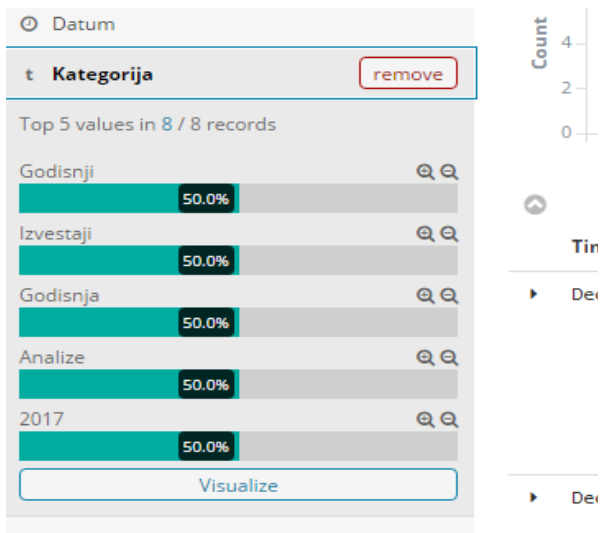
Slika 6. Rezultat pretrage.

U poslednjoj verziji Kibane na naslovnoj strani postoji opcija odabira filtera (jednog ili više njih). Filter se primenjuje na osnovu odabira elementa strukture indeksa (kolone) a na osnovu tipa je moguće primeniti neki od logičkih operatora (slika 7).



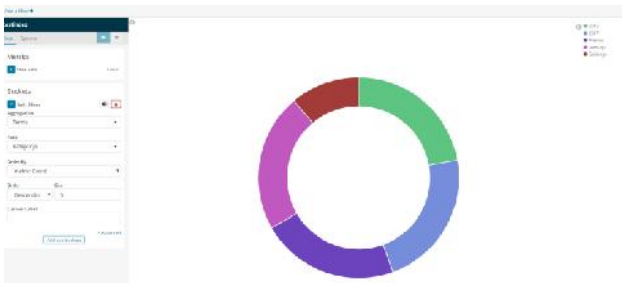
Slika 7. Kibana, dodavanje filtera i rezultat

Prikaz rezultata pretrage je moguće podešavati dodavanjem i uklanjanjem kolona , a u okviru svake kolone moguće je izvršiti i statističku analizu učestalosti vrednosti u celom skupu rezultata pretrage (slika 8).



Slika 8. Raspodela učestalosti vrednosti kolone

Kibana, pored toga što se koristi kao Veb aplikacija za pretragu sadrži i modul za analizu i vizuelizaciju podataka pomoću različitih vrsta dijagrama (slika 9).



Slika 9. Vizuelizacija

Postoje različiti načini prikazivanja podataka. Svaka vizuelizacija može da se sačuva i kasnije koristi. Takođe, moguće je vršiti i filtriranje podataka unutar vizuelizacije.

Vizuelizacije je moguće grupisati u dashboard-ove. Dashboard grupiše više različitih vizuelizacija i takođe je moguće vršiti filtriranje na samom dashboard-u (slika 10,11).



Slika 10. Dashboard



Slika 11. Pretraga unutar dashboard-a

#### 4. SERVIS ZA INDEKSIRANJE

Servis za indeksiranje ima više funkcija i modula. Prvo, on sa zadatih deljenih lokacija pristupa svim fajlovima i čita metapodatke o istim. Metapodaci su: tip fajla, datumi kreiranja i poslednje modifikacije, autor, veličina i naslov. Zatim, ako je fajl odgovarajućeg tipa, otvara fajl i čita sadržaj fajla. Podržani tipovi su: .doc, .docx, .xls, .ppt, .txt, .pdf. Konfiguracijom servisa se definiše kako je to što je pročitano (sadržaj dokumenta) mapirano u odgovarajuću strukturu. Postoje dva osnovna modela mapiranja: ceo sadržaj se mapira u kolonu koji je tipa string i drugi gde se ceo sadržaj dokumenta pretvara u listu stringova ili u neku kompleksniju strukturu (primer: posebno se čitaju boldirani pasusi koji imaju manje od 150 karaktera i stavljaju se kao ključni delovi teksta). Ceo proces se završava tako što se metapodaci zajedno sa sadržajem sastavljaju u strukturu koja se skladišti na elasticsearch server i dostupna je za pretragu pomoću Kibane.

Servis definiše strukturu i okvir za pristup bazama podataka. Implementacijom ove strukture, za svaku bazu posebno, definiše se koji se podaci čitaju i kako se mapiraju u strukturu koja se skladišti na elasticsearch server i koja može da se pretražuje pomoću Kibane.

Implementacija servisa je modularna pa se za svaki poseban deljeni folder definišu mapperi, tipovi fajlova čiji će sadržaj da se čita i način na koji će da se skladište na elasticsearch server.

Servis se direktno koristi u dva osnovna moda rada. Prvi mod rad je inicijalno indeksiranje, gde se sa unapred definisanih lokacija a na osnovu pravila svi fajlovi indeksiraju. Drugi mod rada je inkrementalni, koji periodično ili kada se neki novi fajl pojavi na deljenoj lokaciji, vrši indeksiranje tog fajla.

Aplikacija koje u pozadini rade sa bazama podataka a čiji podaci su potrebni za pretragu zajedno sa podacima sa deljenih lokacija mogu se lako proširiti tako da se prilikom skadištenja novog podataka u bazu podataka, odgovarajućom transformacijom isti takav podatak prebacuje i na elasticsearch pa je dostupan za pretragu pomoću Kibane. Za ove potrebe, implementiran je REST servis kako aplikacije ne bi imale čvrstu vezu sa celim sistemom za indeksiranje i pretragu [4] [5].

#### 5. ZAKLJUČAK

Predloženo rešenje i implementacija su u značajnoj meri povećali dostupnost informacija, analizu i brzinu rada korisnika. Rešenje se posebno dobro pokazalo kada je potrebno ukrstiti rezultate pretrage iz različitih izvora (deljenih lokacija prema tipu ili kategoriji dokumenata). Takođe, mogućnost da se pomoću Kibane, vrši periodično i automatsko osvežavanje rezultata pretrage (na svega nekoliko sekundi) ima posebnu vrednost i primenu kada se koriste aplikacije koje često insertuju nove podatke u bazu podataka ili kada se pojavljuju novi fajlovi na deljenim lokacijama.

## LITERATURA

[1] Elastic stack and product documentation,  
<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

[2] CentOS 7 Linux Server Cookbook – Second Edition,  
Oliver Pelz, Honathan Hobson

[3] Elastic stack and product documentation  
<https://www.elastic.co/guide/en/kibana/6.1/index.html>

[4] ASP.NET Web API 2: Building a REST Service from  
start to finish, Jamie Kurtz, Brian Wortman

[5] Adaptive Code via C#: Agile coding with design  
patterns and SOLID principles, Gary McLean Hall



# PROCENA SLIČNOSTI DOKUMENATA KOMBINACIJOM RAZLIČITIH METODA EKSTRAKCIJE TEMA IZ TEKSTA

## Assessment of Document Similarity using different techniques to extract meaning of the text

Željana Vučetić<sup>1</sup>, Zoran Denda<sup>2</sup>  
MINISTARSTVO ODBRANE<sup>1</sup>

**Sadržaj** – Predmet izučavanja ovog rada je procena sličnosti dokumenata zasnovana na kombinovanoj primeni različitih metoda ekstrakcije tema iz teksta. Konkretno, biće razmotrene i primenjene sledeće metode: 1) metoda ekstrakcije ključnih reči i izraza iz teksta zasnovana na analizi grafa susedstva reči; 2) metoda statističkog modelovanja tema teksta (topic modeling); i 3) metoda prepoznavanja i ekstrakcije entiteta iz teksta. Sličnost dokumenata procenjena primenom svake od tri opisane metode biće agregirana u finalnu ocenu sličnosti dokumenata. U okviru primera razvijena je i prikazana Java aplikacija za preporuku dokumenata, u okviru koje se preporuka zasniva na proceni sličnosti dokumenata opisanim pristupom.

**Abstract** – This document present assessment of document similarity using different techniques to extract meaning of the text. Tree main methods are discussed and applied: 1) keyword and keyphrase extraction using centrality measures on collocation networks; 2) probabilistic topic modeling; and 3) method of extraction and recognition entities from the text. Similarity of documents will be assess by applying all of thee methods and aggregate in final assessment. This document also presents Java application for documents similarity that use this method for assesment.

### 1. UVOD

Kao posledica brzog razvoja Interneta i Veb tehnologija, korisnicima je postao dostupan veliki broj različitih izvora informacija. Osim dobrih strana, ova pojava ima i svoje negativne efekte. Sve češće korisnici Veb aplikacija imaju problema da pronađu odgovarajuću informaciju, a sama pretraga može biti naporan i vremenski zahtevan posao. Ukoliko korisnici znaju šta traže, odnosno potrebna im je samo pomoć da 'lociraju' tražene sadržaje, Veb pretraživači (kao što su Google Search, Yahoo Search, Bing...) mogu u značajnoj meri da olakšaju pronalaženje željenog sadržaja. Međutim, efikasno korišćenje Veb pretraživača podrazumeva da korisnik na pravilan način formuliše upit za pretragu.

Iz ovih razloga, kao i zbog činjenice da korisnici često ne znaju tačno šta traže, prisutnost sistema preporuke na Vebu se stalno povećava. Glavni cilj sistema preporuke je da selektuje skup informacija koje su od potencijalnog značaja za korisnika, odnosno da ponudi interesantne/relevantne sadržaje koji mu nisu poznati.

S obzirom na to da je tekst najčešće sredstvo za razmenu informacija, predmet ovog rada je proučavanje oblasti koje se odnose na analizu teksta i algoritama koji se koriste u procesu procene sličnosti između tekstualnih

dokumenata i koji se mogu primeniti za realizaciju sistema preporuke zasnovanim na analizi sadržaja (eng. content-based recommender systems) [1].

Imajući u vidu da tekst predstavlja nestrukturirani tip podatka - tip koji je najsloženiji za automatsku obradu i interpretaciju - potrebno je omogućiti makar delimičnu interpretaciju značenja tekstualnih sadržaja i na taj način olakšati pronalaženje informacija.

### 2. ANALIZA TEKSTA

U postupku analize teksta, na samom početku, potrebno je izvršiti pretprocesiranje teksta koje će dati izlaz pogodan za dalju automatsku obradu i iterpretaciju.

Pretprocesiranje teksta uključuje [3]:

- Uklanjanje neželjenog teksta (npr., HTML tagova, kodiranog teksta, itd.).
- Uklanjanje reči koje nisu relevantne za postavljene cilj analize teksta, kao što su Ph.D., isn't, e-mail, C|net ili \$19.99.
- Stemovanje ili lematizacija, čime se postiže dobijanje osnovnog oblika neke reči.
- Uklanjanje čestih reči u jeziku koje ne nose u sebi neko značenje (eng. stopwords). Primeri takvih reči su: the, a, of, for, in, itd.

Nakon toga, jedan od tipičnih pristupa je da se sve reči u kolekciji dokumenata indeksiraju i da se odredi frekvencija njihovog pojavljivanja na nivou kako pojedinačnih dokumenata, tako i cele kolekcije dokumenata. Cilj je da se napravi matrica reči i dokumenata čije će ćelije da sadrže numeričke vrednosti (težine) koje odražavaju značajnost svake reči za svaki od dokumenata iz razmatranog korpusa [2]. U ovom radu, na taj način dobijena matrica služi za analizu teksta primenom sledećih metoda:

- 1) Ekstrakcija ključnih izraza analizom grafa susedstva izraza,
- 2) Semantičko indeksiranje i
- 3) Modelovanje tema teksta.

Ekstrakcija ključnih izraza podrazumeva identifikovanje značajnih termina u tekstualnim dokumentima koji bi trebalo da daju veran opis tematike, odnosno sadržaja nekog dokumenta. Primenom ključnih izraza u procesu pretrage dokumenata omogućuje se relativno brzo i tačno identifikovanje relevantnih dokumenta u okviru velike kolekcije dokumenata i ostvaruje se doprinos u domenu pronalaženja informacija (IR), kao i u okviru sumarizacije i kategorizacije teksta.

Prva navedena metoda je realizovana imlementacijom servisa za ekstakciju ključnih izraza iz teksta. Cilj implementacije servisa za ekstrakciju je mogućnost direktnog programskog korišćenja prethodno razvijene funkcionalnosti za ekstrakciju ključnih izraza iz teksta. Da bi servis generisao optimalne rezultate, bilo je potrebno ispitati mogućnosti koje se tiču pretprocesiranja teksta i istražiti na osnovu kojih mera centralnosti se postiže prepoznavanje ključnih izraza u tekstu sa minimalnom greškom. Sama implementacija u velikoj meri se zasniva na istraživanju vezanom za ekstrakciju ključnih reči i izraza primenom mera centralnosti nad kolokacionim mrežama [4].

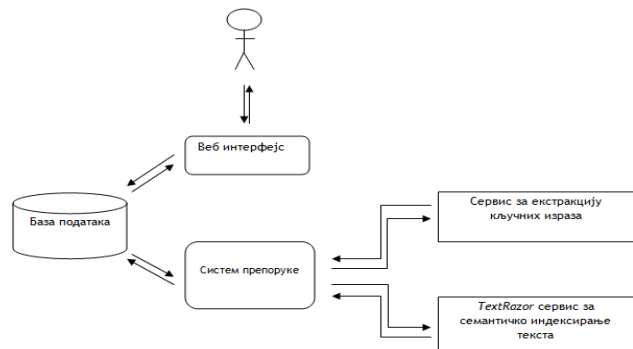
Semantičko ideksiranje (eng. Semantic Indexing, Entity linking) predstavlja kombinovan proces prepoznavanja entiteta u tekstu (eng. Named-entity recognition - NER) i jedinstvenog identifikovanja prepoznatih entiteta (eng. Disambiguation) pomoću baze znanja. Najčešće korišćene baze znanja su: Wikipedia<sup>1</sup>, DBpedia<sup>2</sup>, WikiData<sup>3</sup>. Na primer, u rečenici "Paris is the capital of France.", entitet "Paris" bi mogao da se protumači na različite načine. Ideja je da se utvrdi da se entitet "Paris" odnosi na grad Pariz, a ne na ime neke osobe ili bilo koji drugi entitet koji bi mogao tako da se naziva. [5] Ekstrakcija entiteta iz teksta realizuje se primenom TextRazor servisa za semantičko indeksiranje teksta (prepoznavanje entiteta i njihovo linkovanje sa bazom znanja).

Modelovanje tema (eng. Topic modeling) tekstualnog korpusa je proces čiji je cilj identifikovanje tema, odnosno sadržaja korpusa koji je zatim moguće predstaviti u odgovarajućem mašinski struktuiranom obliku. Modeli tema (eng. Topic models) su statistički modeli čiji je cilj otkrivanje "tema" koje se pojavljuju u skupu dokumenata. Cilj modelovanja tema je matematički opisati tu apstraktnu strukturu "teme", koju možemo shvatiti kao distribuciju reči. [6] Za potrebe ekstrakcije tema primenom statističkog modelovanja tema, koristi se MALLET (MACHINE Learning for Language Toolkit) softverska biblioteka otvorenog koda implementirana u Java programskom jeziku.

### 3. SISTEM ZA PREPORUKU DOKUMENATA

Na slici 1. je prikazan blok dijagram strukture sistema za preporuku koji obuhvata:

- 1) Veb aplikaciju za interakciju sa korisnikom,
- 2) bazu podataka za skladištenje dokumenata i izračunatih metrika potrebnih za kreiranje preporuka,
- 3) alate za analizu sadržaja dokumenata: servisi za ekstrakciju ključnih izraza i semantičko indeksiranje
- 4) sam sistem preporuke za računanje sličnosti među dokumentima.



Slika 1. Blok dijagram sistema preporuke

Kao što je prikazano u blok dijagramu, sistem preporuke preuzima podatke o dokumentima iz baze i šalje upit ka servisima koji mu vraćaju odgovarajući rezultat analize sadržaja – identifikovane ključne izraze, odnosno entitete u tekstu. Dobijene rezultate, sistem preporuke zajedno sa rezultatom primene metode statističkog modelovanja tema (statističko modelovanje tema se realizuje interno, u okviru sistema preporuke), koristi kao ulaz za dalju analizu i određivanje sličnosti između dokumenata. Ovaj proces funkcioniše u "offline" režimu tj. nezavisno od interakcije korisnika sa sistemom za preporuku. Izračunate sličnosti analiziranih dokumenata se upisuju u bazu podataka. Veb aplikacija koristi ove podatke iz baze pri interakciji sa korisnikom.

#### 3.1 SISTEM PREPORUKE

Uopšteno rečeno, sistem preporuke razvijen i opisan u ovom radu spaja rezultate primene tri različite metode procene sličnosti tekstualnih dokumenata i na osnovu toga generiše preporuku. U skladu sa tim, postupak generisanja preporuke čini niz sledećih koraka:

- 1) Preuzimanje dokumenata iz baze podataka.
- 2) Ekstrakcija jedinstvenih identifikovanih entiteta iz sadržaja svakog dokumenta pomoću javno dostupnog Veb servisa.
- 3) Upisivanje ekstrahovanih entiteta u bazu, u okviru podataka za odgovarajući dokument.
- 4) Ekstrakcija ključnih izraza iz sadržaja svakog dokumenta pomoću razvijenog Veb servisa.
- 5) Upisivanje ekstrahovanih ključnih izraza u bazu, u okviru podataka za odgovarajući dokument.
- 6) Kreiranje rečnika koji se sastoji od liste jedinstvenih entiteta svih dokumenata u bazi.
- 7) Kreiranje rečnika koji se sastoji od liste jedinstvenih ključnih izraza svih dokumenata u bazi.
- 8) Kreiranje težinske matrice, gde je svaki entitet iz rečnika jedinstvenih entiteta jedan red matrice, a svaki dokument jedna kolona matrice.
- 9) Normalizacija težinske matrice entiteta i dokumenata tf-idf metrikom.
- 10) Kreiranje težinske matrice, gde je svaki izraz iz rečnika jedinstvenih ključnih izraza jedan red matrice, a svaki dokument jedna kolona matrice.

<sup>1</sup> <https://www.wikipedia.org/>

<sup>2</sup> <http://wiki.dbpedia.org/>

<sup>3</sup> [https://www.wikidata.org/wiki/Wikidata:Main\\_Page](https://www.wikidata.org/wiki/Wikidata:Main_Page)

- 11) Normalizacija težinske matrice ključnih izraza i dokumenata tf-idf metrikom.
- 12) Statističko modelovanje tema sadržaja svakog dokumenta u bazi pomoću softverske biblioteke otvorenog koda.
- 13) Kreiranje težinske matrice, gde svaki red matrice predstavlja redni broj teme (broj tema je fiksna), a svaki dokument jedna kolona matrice.
- 14) Normalizacija težinske matrice tema (distribucije reči) i dokumenata na osnovu statističkog modelovanja tema.
- 15) Izračunavanje kosinusne sličnosti između dokumenata na osnovu a) identifikovanih entiteta u tekstu b) identifikovanih ključnih izraza u tekstu c) identifikovanih tema u tekstu.
- 16) Izračunavanje finalne sličnosti između dokumenata kao linearne kombinacije sličnosti izračunatih na osnovu tema, ključnih izraza i entiteta.
- 17) Upisivanje 10 najbližijih dokumenata za svaki dokument u bazu podataka.

Za svaki od koraka koji su navedeni napravljena je posebna metoda da bi se ceo postupak podelio na „module“, i da bi bilo lakše vršiti kontrolu izlaznih rezultata iz svakog modula, kao i radi utvrđivanja koliko je vremena potrebno svakom modulu da na svom izlazu da rezultat.

### 3.1.1 KREIRANJE VEKTORSKOG MODELA

Osnovni cilj kreiranja vektorskog modela je poređenje sadržaja dokumenata, odnosno utvrđivanje sličnosti između njih. U kontekstu razmatranog problema, vektorski model (eng. vector space model) posmatra sadržaj dokumenta kao skup entiteta, ključnih izraza ili tema, u zavisnosti od primenjene metode analize teksta na osnovu koje se kreira. Sadržaj dokumenta je predstavljen kao vektor, odnosno jednodimenzioni niz indikatora tema dokumenta. Predstavljanjem dokumenata u formi jednodimenzionih nizova otvara se mogućnost računanja sličnosti između dokumenata primenom neke od metrika za računanje sličnosti vektora, kao što je Kosinusna sličnost.

U ovom radu sličnost dokumenata se procenjuje kombinacijom tri metode ekstrakcije značenja iz teksta. U skladu sa tim, kreiraju se tri vektorska modela tako što se svaki dokument predstavlja u vektorskoj formi, pri čemu će elementi i vrednosti vektora zavisiti od primenjene metode.

Za kreiranje svakog pojedinačnog vektorskog modela najpre je potrebno kreirati rečnike čiji su elementi svi entiteti, ključni izrazi ili teme sadržane u razmatranom korpusu. Elementi rečnika su jedinstveni. Ovi rečnici predstavljaju osnovu za formiranje vektorske reprezentacije dokumenata. Svaki element rečnika predstavlja jedan element vektora kojim je svaki dokument iz korpusa predstavljen. U slučaju kada je element rečnika entitet ili ključni izraz, vrednost odgovarajućeg elementa vektora predstavlja broj

pojavljivanja elementa iz rečnika u razmatranom dokumentu. U slučaju kada je element rečnika tema, vrednost odgovarajućeg elementa vektora predstavlja verovatnoća zastupljenosti određene teme iz rečnika u razmatranom dokumentu. Vektori kreirani na opisani način se „povezuju“ u tzv. težinsku matricu u kojoj redovi odgovaraju elementima rečnika, dok kolone odgovaraju dokumentima.

S obzirom na to da je proces kreiranja vektorskog modela, kao i težinske matrice, suštinski isti za sve tri primenjene metode ekstrakcije značenja iz teksta, u nastavku će biti opisan ceo postupak samo u slučaju kada se vektorska reprezentacija dokumenata formira na osnovu entiteta identifikovanih u sadržaju.

### 3.1.2 VEKTORSKA REPREZENTACIJA NA OSNOVU ENTITETA

Pretpostavimo da je dato 5 dokumenata koji se odnose na naučna istraživanja. Primenom metode za semantičko indeksiranje teksta pomoću TextRazor servisa, identifikovani su entiteti u sadržaju svakog pojedinačnog dokumenta.

Na osnovu dobijenih rezultata analize teksta, u ovom slučaju primenom metode prepoznavanja i identifikovanja entiteta u tekstu, formira se rečnik jedinstvenih entiteta u datom korpusu. Zadatak je da se otkrije koliko puta se svaki od entiteta u rečniku nalazi u sadržaju pojedinačnog dokumenta.

Označimo sa  $A$  matricu sa entitetima i dokumentima dimenzije  $m \times n$ . Svaki red odgovara jednom entitetu, a svaka kolona odgovara dokumentu. Ukoliko se entitet  $i$  pojavljuje  $a$  puta u dokumentu  $j$  onda sledi da je  $A[i, j] = a$ . Dimenzije matrice  $A$ ,  $m$  i  $n$ , odgovaraju broju entiteta i dokumenata, redom. Za ovaj primer, deo matrice matrice  $A$ , koji se odnosi na prvih 10 entiteta iz rečnika, prikazan je na slici 2.

ENTITET	Документ				
	d1	d2	d3	d4	d5
<i>Space Telescope Science Institute</i>	1	0	0	0	1
<i>Barclays</i>	1	0	0	0	0
<i>International Petroleum</i>	1	0	0	0	0
<i>Investment Company</i>	1	0	0	0	0
<i>NASA</i>	2	1	0	0	2
<i>Outer space</i>	1	0	0	0	0
<i>Astronomy</i>	1	1	0	1	2
<i>Space telescope,</i>	1	0	0	0	0
<i>Telescope</i>	1	1	0	1	0
<i>Atom</i>	0	0	1	0	0

Slika 2. Frekvencija entiteta u sadržaju dokumenata iz primera

Na slici 2 se vidi, na primer, da se entitet NASA pojavljuje u sadržaju dokumenta d1 i d5 dva puta, a u d2 jednom, da entitet Astronomy pojavljuje u svim dokumentima osim u d3, dok je Atom prisutan samo u dokumentu d3.

### 3.1.3 TF-IDF METRIKA

Za pridruživanje težine ekstrahovanim terminima iz teksta, npr. entitetima, koristi se Term Frequency – Inverse Document Frequency (TF-IDF) metrika, kojom se procenjuje koliko je neki entitet, ključni izraz ili tema važna u dokumentu.

Term Frequency (TF) je broj pojavljivanja određenog termina, odnosno, u ovom slučaju entiteta, u dokumentu. Ovaj broj bi mogao biti mera važnosti entiteta za dati dokument, međutim neki entiteti se suviše često pojavljuju u dokumentima. Da bi se važnost entiteta koji se isuviše često pojavljuju mogla kontrolisati TF metrika se kombinuje sa Inverse Document Frequency (IDF) metrikom. IDF predstavlja meru specifičnosti termina (odnosno entiteta u razmatranom kontekstu) za razmatrani skup dokumenata. Na primer, entitet koji se pojavljuje u 10% dokumenata bi verovatno trebao biti označen sa većom težinom od entiteta koja se pojavljuje u više od 96% dokumenata.

Konkretno, TF-IDF vrednosti termina se računaju formulom:

$$w_{tf-idf} = tf_{t,d} \times idf_t.$$

$tf_{t,d}$  predstavlja broj pojavljivanja termina  $t$  u dokumentu  $d$ , odnosno u kontekstu kreiranja težinske matrice, ovo je vrednost ćelije inicijalne matrice (slika 2) koja se nalazi u preseku termina  $t$  i dokumenta  $d$ .  $idf_t$  se definiše kao:

$$idf_t = \log_{10} \frac{N}{df_t},$$

gde je  $N$  ukupan broj dokumenata u bazi podataka, a  $df_t$  je broj dokumenata u kojima se pojavljuje termin  $t$ .

Prilikom korišćenja skupa termina za predstavljanje sadržaja dokumenta, jasno je da će vektori dužih dokumenata biti popunjeniji i time imati veću šansu da upoređivanjem sa vektorima drugih dokumenata budu označeni kao relevantni. Međutim svi dokumenti bi trebalo da budu tretirani isto bez obzira na njihovu dužinu. U skladu sa tim, dobijena težinska matrica se normalizuje, odnosno vrednosti matrice se svode na vrednosti između 0 i 1. Zadatak normalizacije je da neutrališe uticaj dužine dokumenta [7].

### 3.1.4 RAČUNANJE SLIČNOSTI PRIMENOM KOSINUSNE SLIČNOSTI

Nakon generisanja težinske matrice pomoću tf-idf metrike moguće je upoređivati dokumente koristeći vektorske metrike kao što je Kosinusna sličnost, jer su dokumenti predstavljeni vektorskom reprezentacijom. Skup dokumenata u kolekciji se posmatra kao skup vektora u

vektorskom prostoru, u kojem postoji jedna osa za svaki termin.

Kosinusna sličnost je mera sličnosti dva vektora koja je određena kosinusom ugla koji ti vektori formiraju [8]. Neka su data dva vektora  $v_i$  i  $v_j$  koji predstavljaju dva različita dokumenta. Kosinus ugla između dva navedena vektora se računa po formuli [8]:

$$\cosin(v_i, v_j) = \frac{\sum_k v_i[k] \times v_j[k]}{\sqrt{\sum_k v_i[k]^2} \times \sqrt{\sum_k v_j[k]^2}}$$

Vrednosti kosinusne sličnosti se kreću između -1 i 1. Ukoliko je vrednost kosinusne sličnosti -1 onda su dva vektora potpuno različita, odnosno u koliko je vrednost 1 vektori su u potpunosti identični.

## 4. IMPLEMENTACIJA

Na osnovu koraka opisanih u sekciji 3.1 izvršena je implementacija sistema za preporuku u Java programskom jeziku, konkretno, Veb servisa za ekstrakciju ključnih izraza, samog postupka preporuke (zasnovanog na računanju sličnosti između dokumenata kombinacijom tri različite metode analize teksta), i Veb aplikacije za interakciju sa korisnikom.

Za implementaciju je korišćeno razvojno okruženje NetBeans IDE 8.2<sup>4</sup>.

Dokumenti koji su predmet preporuke se skladište u MongoDB bazu podataka pomoću Java MongoDB Driver<sup>5</sup> koji sadrži potrebne metode za pristup bazi, odnosno za CRUD (Create, Read, Update, Delete) operacije.

### 4.1. VEB APLIKACIJA ZA PREPORUKU DOKUMENTA

Primena predloženog pristupa za ocenu sličnosti dokumenata za realizaciju sistema preporuke koji se zasniva na analizi sadržaja prikazana je kroz Veb aplikaciju za preporuku dokumenata. Veb aplikacija, razvijena u Java programskom jeziku, koristi unapred izračunate sličnosti između dokumenata kako bi selektovala dokumente koji su najbliži dokumentu odabranom od strane korisnika. Veb aplikacija je implementirana korišćenjem Spring tehnologije. Korisnički interfejs je razvijen korišćenjem Bootstrap framework-a, stoga je prilagođen različitim uređajima, odnosno veličinama ekrana (npr., mobilni telefon, računar). Aplikacija je razvijena primenom MVC paterna i sastoji se iz dve stranice.

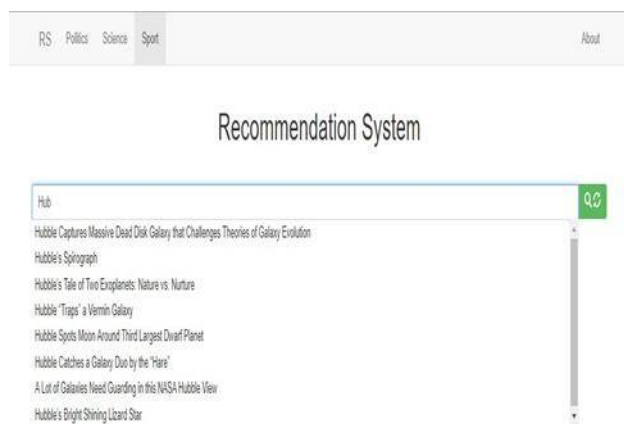
Na prvoj stranici korisnik ima mogućnost da pretražuje postojeće dokumente iz baze podataka prema nazivu dokumenta u okviru tematske oblasti od interesa (trgovina, sport, nauka). Prilikom pretrage dokumenata korisniku je, u vidu pomoći, raspoloživa opcija autocomplete. Ova opcija je sastavni deo jQueryUI plugin-a. Kada korisnik unese početna slova naziva

<sup>4</sup> <https://netbeans.org/>

<sup>5</sup> <https://docs.mongodb.org/ecosystem/drivers/java/>

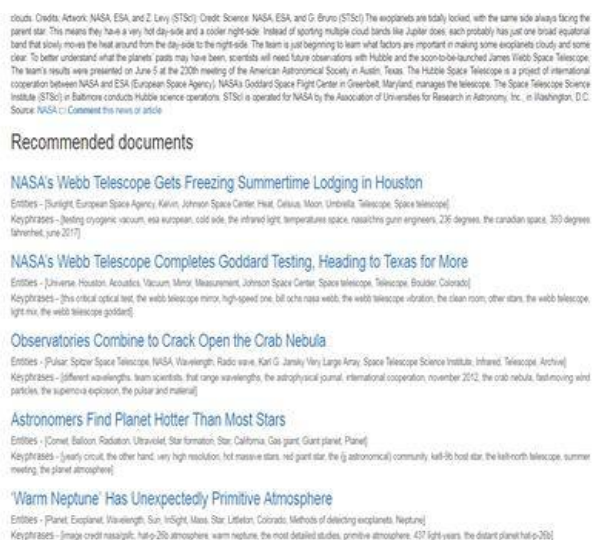


dokumenta koji traži, aplikacija pronalazi sve dokumente koji sadrže u svom nazivu izraz koji je korisnik uneo i prikazuje korisniku listu dokumenata. Izgled prve stranice dat je na slici 3.



Slika 3. Stranica za pretraživanje dokumenata

Nakon odabira dokumenta od interesa, na drugoj stranici korisniku se prikazuje naziv i sadržaj odabranog dokumenta. Ispod teksta „Recommended documents“ (slika 4), prikazuje se lista od 10 najslučajnijih dokumenata dokumentu u čiji sadržaj korisnik trenutno ima uvid. U listi su prikazani nazivi dokumenata i u zagradama - [] 10 najrelevantnijih entiteta i ključnih izraza prepoznatih u sadržaju odgovarajućih dokumenata.



Slika 4. Detalji odabranog dokumenta i preporuka

Naziv dokumenta sadrži URL adresu odakle je preuzet sadržaj dokumenta, tako da korisnik može da pristupi izvornom dokumentu.

## 5. EVALUACIJA APLIKACIJE ZA PREPORUKU

Evaluacija se zasniva na subjektivnoj proceni kvaliteta generisanih preporuka, odnosno rezultata primene predloženog pristupa za ocenu sličnosti dokumenata i generisanja preporuka na osnovu procenjenih sličnosti.

Za potrebe evaluacije korišćeno je po 150 dokumenata iz tri tematske oblasti. Korišćeni dokumenti su novinski članci preuzeti sa sledećih Veb sajtova: 1) actmedia.eu - tematska oblast “trgovina”, 2) www.technology.org - tematska oblast “nauka i tehnologija”, 3) www.skysports.com i www.breakingnews.ie - tematska oblast “sport”.

Da bi se utvrdila svrsishodnost implementacije sistema preporuke na osnovu predloženog pristupa za ocenu sličnosti, potrebno je ispitati u čemu se sastoji prednost 1) kombinovane primene tri različite metode analize teksta u odnosu na 2) primenu jedne od korišćenih metoda za procenu sličnosti između dokumenata.

Analiza rezultata procene sličnosti između dokumenata, odnosno preporuke dokumenata, izvršena je ocenom koliko su preporučeni dokumenti: 1) novi tj. nepoznati korisniku, 2) relevantni za korisnika, 3) interesantni korisniku, i 4) očekivani.

U skladu sa navedenim kriterijuma za procenu kvaliteta preporuka, izvršena je analiza preporuka koje su dobijene na sledeće načine: 1) primenom metode ekstrakcije ključnih izraza iz teksta, 2) primenom metode ekstrakcije identifikovanih entiteta u tekstu, 3) primenom metode ekstrakcije tema iz teksta, i 4) kombinovanom primenom tri prethodno navedene metode za analizu teksta.

U tabeli 5 je ocenjeno na skali od 1 do 5 koliko je svaki od korišćenih kriterijuma zadovoljen za preporuku dobijenu primenom svakog od prethodno razmatranih pristupa, ukoliko je ispunjen uslov da u raspoloživom korusu postoje dokumenti koji su procenjeni kao izuzetno slični odabranom dokumentu (vrednost izračunate sličnosti teži 1) na osnovu i ključnih izraza i entiteta i tema istovremeno. Oцена 1 označava da preporuka, generisana primenom određenog pristupa za procenu sličnosti dokumenata, nije od značaja za korisnika iz aspekta određenog kriterijuma. Suprotno, ocena 5 označava da je dobijena preporuka visokog kvaliteta u skladu sa primenjenim pristupom, odnosno iz aspekta određenog kriterijuma.

Pristup	Kriterijumi za ocenu preporuke			
	Novi	Relevantni	Očekivani	Interesantni
Izrazi	1	4	3	1
Entiteti	3	4	5	3
Teme	5	2	2	5
Kombinacija	3	3	3	3

Tabela 1. Vrednost parametara za ocenu preporuke u zavisnosti od korišćenog pristupa

## 6. ZAKLJUČAK

Fokus ovog rada je procena sličnosti dokumenata na osnovu analize njihovog sadržaja. Konkretno, procena sličnosti između dokumenata se zasniva na kombinovanoj primeni različitih metoda ekstrakcije indikatora tema



(ključni izrazi, entiteti, teme) iz teksta. U cilju prikaza mogućnosti predloženog pristupa za ocenu sličnosti dokumenata, implementiran je sistem preporuke koji se zasniva na analizi sadržaja dokumenata koji su predmet preporuke.

Kroz rad su opisane tri metode za analizu teksta. Kombinovanom primenom izvršena je procena sličnosti dokumenata na osnovu njihovog sadržaja. Korišćene metode zasnovane su na predstavljanju dokumenata u vektorskom prostoru. U radu je pokazan postupak kreiranja vektorskog modela. Za računanje sličnosti između sadržaja dokumenata koji su predstavljeni vektorima u razmatranom vektorskom modelu korišćena je kosinusna sličnost. Podaci o dokumentima, kao i podaci o izračunatoj sličnosti između njih skladište se u bazi podataka.

Primena svake od korišćenih metoda za analizu teksta u svrhu procene sličnosti između dokumenata podrazumevala je istraživanje u oblasti analize teksta. U cilju izbora odgovarajućih rešenja za implementaciju sistema preporuke na osnovu predloženog pristupa za ocenu sličnosti, testirane su različite javno dostupne softverske tehnologije u skladu sa postavljenim korsiničkim zahtevima.

Kroz implementaciju Veb servisa za ekstrakciju ključnih izraza testirane su biblioteke za procesiranje teksta i rad sa grafovima. Rezultat je Veb servis koji je relativno lak za korišćenje. Evaluacija Veb servisa pokazala je da servis daje relevantne rezultate za kratko vreme koji mogu pomoći korisniku da razume tematiku sadržaja na osnovu ključnih izraza.

Izvršena je evaluacija Veb aplikacije za preporuku i pokazana je prednost sistema preporuke zasnovanog na kombinovanoj primeni različitih metoda za ekstrakciju indikatora tema iz teksta u odnosu na sistem preporuke koji se bazira na rezultatima primene isključivo jedne metode ekstrakcije. S obzirom na to da se pojedinačnom primenom svake od korišćenih metoda dobija preporuka različitog značaja za korisnika, može se reći da kvalitet dobijene preporuke umnogome zavisi od uticaja različitih spoljašnjih faktora. Neki od faktora koji mogu imati uticaj na kvalitet rezultata u zavisnosti od metode koja se razmatra su: količina dokumenata u razmatranom korpusu, dužina dokumenata, korišćena terminologija u sadržaju dokumenata, konkretna tematika dokumenta, itd. Osnovna prednost predloženog pristupa ogleda se u tome što preporuka može biti na različite načine od značaja za korisnika (npr. jednako relevantna i interesantna) ukoliko je procenjena visoka sličnost između dokumenata na osnovu bar jedne od primenjenih metoda za ekstrakciju indikatora tema teksta.

U zavisnosti od interesovanja korisnika, jedna ista preporuka može biti od izuzetnog značaja za jednog korisnika, dok za drugog potpuno beskorisna. U skladu sa tim, predstavljeno rešenje ima prostora za unapređenje u smislu prilagođavanja preporuke interesovanjima korisnika. Jedan od načina bi bio omogućiti korisniku

izbor u skladu sa korišćenim kriterijumima za ocenu kvaliteta preporuka - da li bi preporučeni dokumenti treba da budu pretežno nepoznati, relevantni, interesantni, i/ili neočekivani. S obzirom da se finalna sličnost, a time i preporuka, računa kao linearna kombinacija rezultata dobijenih na osnovu primene pojedinačnih pristupa procene sličnosti, i da različiti pristupi različito utiču na razmatrane kriterijume (tabela 1), potrebno je istražiti mogućnost ponderisanja tih rezultata u skladu sa interesovanjem korisnika.

## LITERATURA

[1] P. Lops, M. d. Gemmis, G. Semeraro, „Content-based Recommender Systems: State of the Art and Trends,“ *Recommender Systems Handbook*, Springer US, 2011, pp. 73-105.

[2] I. Witten, „Text mining,“ *The Practical Handbook of Internet Computing*, Boca Raton, Florida, Chapman & Hall/CRC Press, 2005, pp. 14-22.

[3] X.Zhu, „Basic Text Process“, CS769 Spring 2010 Advanced Natural Language Processing, Computer Science University of Madison-Wisconsin, Wisconsin, nastavni materijal. URL: [http://pages.cs.wisc.edu/~jerryzhu/cs769/text\\_preprocessi ng.pdf](http://pages.cs.wisc.edu/~jerryzhu/cs769/text_preprocessi ng.pdf).

[4] S. Lahiri, S. R. Choudhury, C. Caragea, „Keyword and Keyphrase Extraction Using Centrality Measures on Collocation Networks,“ arXiv preprint arXiv:1401.6571, 2014.

[5] J. Jovanović, „Prepoznavanje entiteta u tekstu i Semantičko indeksiranje“, Fakultet organizacionih nauka, nastavni material. URL: <http://ai.fon.bg.ac.rs/wp-content/uploads/2016/10/NER-Entity-Linking.pdf>

[6] D. M. Blei, „Probabilistic topic models“, *Communications of the ACM*, 2012, pp. 77-84.

[7] D. A. Grossman, O. Frieder. *Information Retrieval: Algorithms and Heuristics*, 2004.

[8] Z. Marković, „SKALOMERIZACIJA ELEMENATA MATRICE PODATAKA VIŠEKRITERIJUMSKOG ZADATKA“, XXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju, Beograd, 2008.

# VIRTUELNE SIMULACIJE U VOJNOM OBRAZOVANJU VIRTUAL SIMULATIONS IN MILITARY EDUCATION

Goran Šimić<sup>1</sup>, Tamara Gajić<sup>2</sup>, Stefan Vukadinović<sup>2</sup>  
*Univerzitet odbrane<sup>1</sup> i Vojska Srbije<sup>2</sup>*

**Sadržaj** – U ovom radu predstavljena je analiza savremenih sistema za kreiranje virtuelnih simulacija, problemi sa kojima se kreatori scenarija susreću i primena simulacija u obrazovanju.

**Abstract** – This document presents an analysis of modern systems for creating virtual simulations, problems encountered by script creators and the use of simulations in military education.

## 1. UVOD

U svetu obrazovanja poslednjih decenija jednu od najvećih promena donosi sve veća upotreba računarskih igara i virtuelnih simulacija. Kako bi se shvatilo edukativni potencijal virtuelnih simulacija neophodno je da sagledamo kako se ona slaže sa teorijom učenja i kakve koristi ima učenje od igranja igara.

Virtuelne simulacije menjaju tradicionalni oblik učenja, tako što obogaćuju edukativni sadržaj i čini ga lakšim za razumevanje. Osim toga, u virtuelnom okruženju je mnogo lakše i jeftinije implementirati situacije koje se u praksi mnogo teško ostvaruju.

U radu će biti predstavljen konkretan sistem za kreiranje virtuelnih simulacija VBS3, njegova komparacija sa komercijalnim igrama, prednosti i mane koje ovi sistemi poseduju. Posebno će biti istaknuta njegova modularna struktura kao i kreiranje i upotreba korisnički definisanih modula (skript fajlova). Razmatraće se koncept i realizacija čitavog scenarija uz rešavanje konkretnih problema. Kraj rada donosi kratak opis načina korišćenja sistema, kao i evaluaciju sistema koja je neophodna u daljoj implementaciji ovoga sistema u obuci vojske.

## 2. OPIS PROBLEMA I ANALIZA SAVREMENIH SISTEMA VIRTUELNIH SIMULACIJA

Vreme u kome živimo sve više se ubrzava razvojem nauke i tehnologije. Današnje tehnološke mogućnosti u vizuelizaciji i simulaciji omogućavaju kreiranje virtuelnih okruženja koja su približna realnom, kao i situacija koje je teško izvesti u praksi.

Za razliku od komercijalnih igara koje su primarno dizajnirane za zabavu, vrednost primenjenih ili ozbiljnih igara (*Serious game*) [1] leži u edukaciji i obuci igrača koji ih koriste. Istraživanja su pokazala negativan uticaj igranja igara na studente koji se odražava slabim rezultatima u školi i povećavanjem agresivnosti kod igrača [2]. Iz nekih studija izveden je zaključak da uticaj igranja igara nije loš ukoliko su igre dizajnirane na bazi simulacija i kada sadrže edukativnu vrednost [2]. U simulacijama se kreira scenario u skladu sa edukativnim ciljem. U tom procesu nastavnici imaju ulogu domenskog

eksperta, a informatičari implementiraju zamisao u konkretno simulaciono okruženje.

Računarske simulacije poboljšavaju osobine zapažanja i vizuelizacije učenika, unapređuju kvalitet obrazovnog procesa i omogućavaju predavačima punu kontrolu nad simulacijom i načinom interpretacije obrazovnog sadržaja.

Opšte prihvaćena klasifikacija računarskih simulacija koja se zasniva na kompleksnosti, metodologiji koja se koristi i nivou objekata je na [3]:

- Žive simulacije (*Live Simulation*) – realno okruženje, vojnici ali manevarska municija.
- Virtuelne simulacije (*Virtual Simulation*) – razvijene i dizajnirane od strane programera ili tima stručnjaka u kompleksnom softverskom okruženju.
- Konstruktivne simulacije (*Constructive Simulation*) – najkompleksnije, dizajnirane za obuku i trening osoblja i komandanata združenih taktičkih sastava.

VBS3 (*Virtual Battlespace 3*) je interaktivan, *commercial-off-the-shelf* (COST – softver koji se nalazi u prodaji), 3D trening sistem koji pruža okruženje za kreiranje ogromnog broja spektra simulacija za obuku vojske, a može služiti i u istraživačke svrhe. Baziran je na modernog 3D gaming tehnologiji. Posle VBS1 i VBS2 pojavljuje se poslednja verzija simulacionog softvera, VBS3, kompanije BISim. Pored poboljšanih performansi uvodi se *multicast system* koji omogućava usklađivanje učesnika u *multiplayer* režimu rada, sprečava kašnjenja koja se javljaju pri učitavanju servera, poboljšava performanse u lokalnoj mreži. *Multicast system* radi tako što šalje istovremeno podatke na više računara preko jednog porta koji je prethodno dodeljen od strane servera. Taj port služi da se izjednače brzine prenosa podataka, što omogućava poboljšanje performanse u radu na mreži. Poboljšanja u dizajniranju mapa dodavanjem detalja visoke rezolucije. Sistem komandovanja i upravljanja nadograđen je ORBAT modom koji omogućava hijerarhiju u komandovanju.

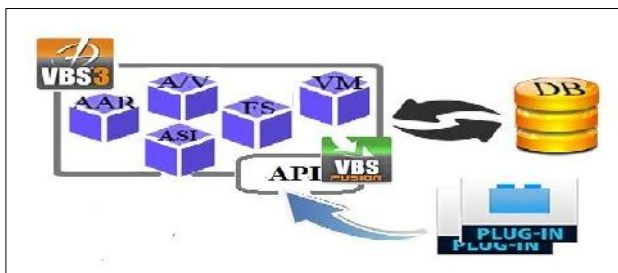
Glavne razlike između komercijalnih igara i virtuelnih simulacija demonstriraćemo na primeru VBS softvera i jednom od klasika u svetu video igara, a to je *Call of Duty (CoD)*. VBS omogućava samostalno kreiranje scenarija, dok *Call of Duty* ima ograničen broj scenarija koji se ne mogu menjati sa aspekta dizajna i logike. Interakcija i donošenje odluka kod VBS scenarija bazirane su na *multiple-choise* (više mogućnosti) i *branching decisions* (više odluka se može doneti), za razliku od *CoD* gde je interakcija zasnovana na ograničenom skupu radnji koje igrač može da uradi, jer su misije unapred određene i mogu se preći na jedinstven način. Jedna od bitnih karakteristika VBS softvera je mogućnost analize i

evaluacije prethodno završene simulacione vežbe, dok toga u svetu komercijalnih igara nema.

### 3. PRIKAZ ARHITEKTURE I DIZAJNA VBS3

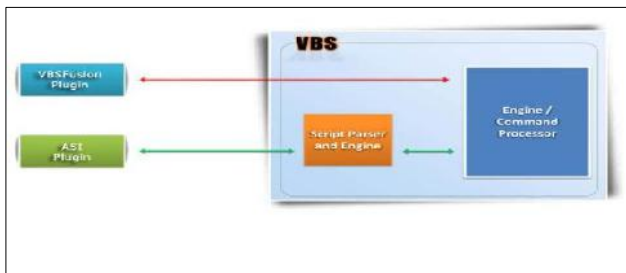
VBS3 je fleksibilan, *open-platform*, simulacioni softver koji pruža programerima širok spektar mogućnosti u kreiranju trening scenarija. Otvorena platforma omogućava komuniciranje eksternih aplikacija sa VBS preko API (Application Programming Interface) modula.

Na slici 1. prikazana je arhitektura sistema VBS gde se konkretno vidi njegova modularna struktura. Sam sistem je u vezi sa bazom podataka sa kojoj vrši razmenu i upis podataka.



Slika 1. Arhitektura VBS-a

VBSFusion je C++ API za VBS. Svaki program koji je pisan kao VBSFusion treba da se kompajlira kao *plug-in* u standardnoj DLL formi i da se postavi u folder /pluginFusion. Na ovaj način kada se poziva VBSFusion on će implementirati *plug-in* u VBS okruženje. Standardan IDE za kreiranje *plug-in* je Microsoft Visual Studio. VBSFusion *plug-in* nemaju *main* funkciju koja se izvršava sekvencijalno kada izvršavanje programa krene, kod za *plug-in* mora da sadrži *callback* funkcije koje kada se desi određeni događaj u VBS okruženju izvršava *plug-in*. Razlika između ASI i VBSFusion *plug-in* ili bilo kog drugog programa koji je u vezi sa njim izvršava se direktno na VBSCore. Ovo znači da nema konverzije podataka kada dođe do izvršavanja programa već se podaci nalaze u razumljivoj formi za VBSCore. Ovo je sasvim suprotno od načina na koji ASI funkcioniše jer svaki program koji je pisan preko ASI modula mora prvo da se konvertuje u string format kako bi bio razumljiv za VBSCore, što praktično znači da pri pozivu programa koji je pisan preko ASI modula mora prvo da se prođe parsiranje u formt razumljiv za VBSCore [4]. Na slici 2. prikazana je razlika između ASI i API modula.

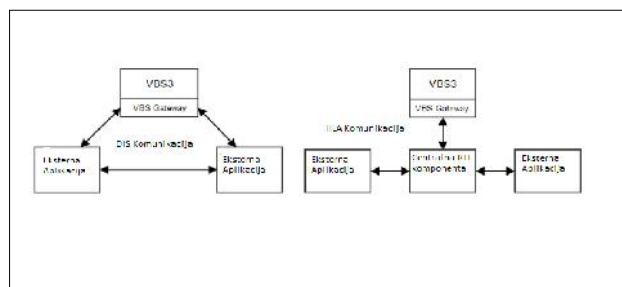


Slika 2. Razlika između API i ASI modula

Pozivanje API programa ne zahteva konverziju podataka, identifikaciju funkcija niti prevođenje u string format za razliku od ASI modula, što znači da se isti program mnogo brže izvršava u API okruženju nego u ASI.

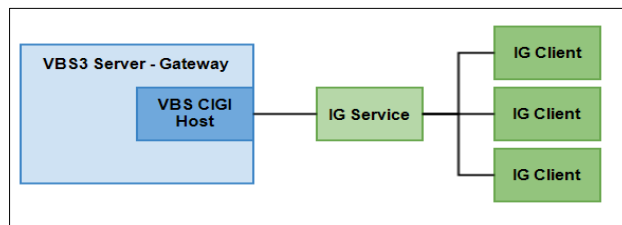
Jedan od najznačajnijih sistemski definisanih modula je AAR (After Action Review). Pomoću AAR reprodukcije (*playback*) omogućena je ocena i evaluacija učesnika simulacije proširujući mogućnosti VBS3 kao softvera za obuku. Startovanje snimanja i zaustavljanje može se vršiti preko Real Time Editor (RTE) interfejsa i preko skripte. Ovaj interfejs je samo dostupan učesnicima sa administratorskim privilegijama.

VBS gateway [5] omogućava komunikaciju (*link*) između VBS i drugih simulacionih sistema. Predstavlja jedan od sistemski definisanih modula. VBS gateway koristi HLA i DIS protokole za bidirekcionu komunikaciju omogućavajući istovremenu prezentaciju objekata između objekata svih kompatibilnih simulacionih komponenti. HLA (High – Level Architecture) omogućava komunikaciju između dve eksterne aplikacije bez obzira na platformu. Interakcija između aplikacija kontroliše se pomoću RTI (Real – Time Infrastructure). DIS (Distributed Interactive Simulation) protokol je IEEE standard za *real-time* upravljanje na nivou platforme na više *host* računara. Na slici 3. predstavljen je dijagram komunikacija HLA i DIS.



Slika 3. Dijagram komunikacije HLA i DIS

VBS gateway sadrži VBS CIGI Host i koristi CIGI protokole za deljenje podataka. CIGI (Common Image Generator Interface) je interfejs dizajniran da predstavlja standardni način za komunikaciju između *host* uređaja i Image Generator (IG). Na slici 4. prikazan je pojednostavljen VBS CIGI komunikacioni dijagram.



Slika 4. CIGI dijagram komunikacija

Pored sistemskih, postoje i korisnički definisani moduli [5] predstavljeni skriptovima (organizovani u tzv. *sqf* fajlove) pisanim u posebnom VBS3 skript jeziku. Pri kreiranju korisničkih modula neophodno je prvo kreirati inicijalni modul (*init.sqf*). Komande i podaci koji su



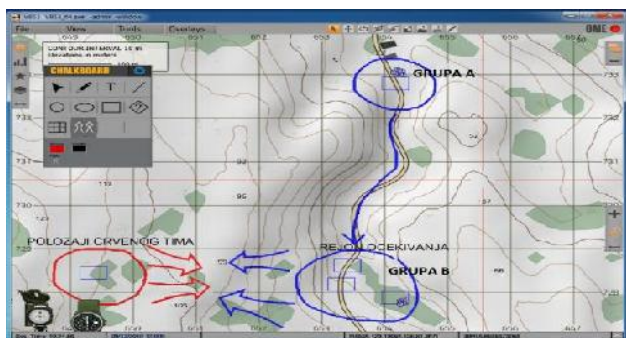
pisani u skriptu konvertuju se u skript datoteku preko modula za prevođenje. Takav skript se potom prevodi u komande i podatke koje su razumljive za *VBSCore*. Zatim prolaze kroz parser (pretprocesiranje) gde se proverava da nema logičkih grešaka i potom se izvršavaju u *VBSCore*. Ukoliko je korisnik skriptom tražio neku povratnu vrednost, proces je obrnut. *VBSCore* daje traženi podatak koji se prevodi u string. Potom se preko modula za prevođenje konvertuje u tip podataka koji je razumljiv korisniku. Kreiranje i kucanje skript fajla može se izvršiti u bilo kojem tekstualnom editoru (*Notepad++*, *TextPad*, *UltraEdit*).

Prilikom pokretanja svakog scenarija skript fajl će biti svaki put kompajliran. Broj korisnički definisanih modula nije ograničen. Preko inicijalizovanog modula vrši se pozivanje ostalih modula korišćenjem posebnog makroa - naredbe *execVM*, *call* ili *preprocessFile*. U primeru koji je izložen u radu, u scenariju su kreirana tri korisnički definisana modula, inicijalizacioni i modul ponašanja sintetičkih jedinica (*AI – Artificial intelligence*) i modul upravljanja pravim igračima.

#### 4. IMPLEMENTACIJA REŠENJA NA KONKRETNOM SISTEMU VIRTUELNIH SIMULACIJA

Predstavljen scenario je istraživanje mogućnosti obuke pešadijskog odeljenja u savlađivanju prepreka, koordinaciji, rukovođenju i komandovanju i primeni osnovne taktičke obuke u okruženju koje simulira realnost. Za implementaciju scenarija izabran je teren čije geografsko-topografske karakteristike su najviše odgovarale realnim karakteristikama sa kojima se učesnici obuke mogu susresti. Vremenski, scenario možemo podeliti na dva dela: uvodni i glavni deo. U uvodnom delu scenarija učesnici nemaju kontrolu nad svojim jedinicama, on služi da se učesnici upoznaju sa situacijom, konkretnim zadacima, da shvate svoje uloge u timu i da se igrači koji se prvi put susreću sa takvom vrstom softvera upoznaju sa komandama koje služe za upravljanje jedinicama. Za kreiranje i kontrolisanje objekata u uvodnom delu napravljen je poseban skript zapamćen u poseban fajl (*blufor.sqf*).

Realizacija uvodnog dela započinje se kreiranjem dve grupe. Grupa koja se nalazi u rejonu očekivanja (Grupa B) i grupe za podršku (Grupa A). Na slici 5. prikazan je izgled mape scenarija.



Slika 5. Izgled mape scenarija

U očekujućem rejonu zadatak grupe B je da čeka dolazak grupe za podršku. Težišni deo uvodnog dela je na grupi A koja treba da se ukrca u borbena vozila i da dođe do grupe B kako bi se formiralo odeljenje koje bi se iz očekujućeg rejonu uputilo na izvršavanje zadataka. Nakon dolaska grupe A i formiranja odeljenja realni učesnici preuzimaju kontrolu nad svojim jedinicama i kreću u izvršavanje zadataka. Praktično ovo je faza tranzicije u kojoj ljudska inteligencija preuzima delimičnu kontrolu od veštačke inteligencije. Tu počinje glavni deo scenarija u kome se izvršavaju dva zadatka. Prvi zadatak je uništavanje minsko-eksplozivnog sredstva (*MES*) koje se nalazi na putu pomoću snajperske puške. Drugi zadatak je zauzimanje određene tačke na mapi gde se nalaze utvrđene neprijateljske snage.

Kao što je već napomenuto, scenario je implementiran u *sqf* skript jeziku koji se prevodi u odgovarajući objektni kod izvršiv u toku same simulacije. Nakon pokretanja modula i postavljanja početnih podešavanja potrebno je kreirati i podesiti objekte koji se koriste u scenariju. U primeru je kreirano i postavljeno minsko-eksplozivno sredstvo na putu što se može videti na slici 6.



Slika 6. Izgled mine

Za kreiranje mine koristi se skript funkcija *createMine* koja prihvata šest ulaznih parametara, instancira minu i vraća je kao rezultat. Na isti način se vrši i kreiranje vozila – skript funkcija *createVehicle* kojoj se prosleđuju dva parametra. Na slici 7. prikazan je izgled vozila, dok se na slici 8. nalazi kod za kreiranje mine i vozila.



Slika 7. Izgled borbenog vozila

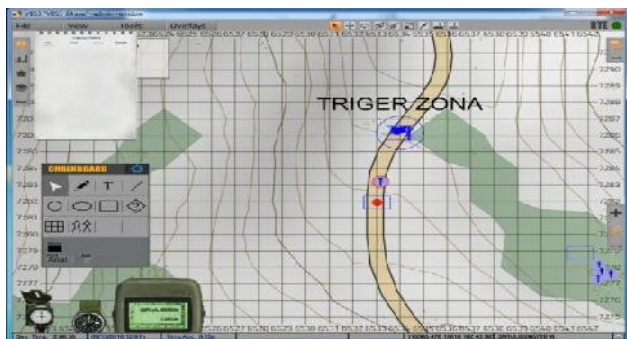
Nakon kreiranja, objekti se dalje kontrolišu posredstvom varijabli koje referenciraju na njih – u konkretnom slučaju za mine je korišćena lokalna varijabla *\_mine*, a za vozilo globalna varijabla *veh1*. Lokalna vidljivost je ograničena

na modul (skript fajl), dok je globalna vidljivost na nivou scenarija.

```
//mina
mine = createMine
["vbs2_mineat_m15",getmarkerpos "marker5", [],
0, false, 5];
//vozilo
veh1 =
"vbs2_us mc m114 iwp w m2 fording kit_x"
createVehicle getmarkerpos "marker2";
```

Slika 8. Kreiranje objekata - mine i vozila

Pokretanje vozila se izvršava pomoću funkcije *doMove*. Prestanak kretanja vozila i izlazak jedinica iz vozila je sled akcija koje su aktivirane događajem (*triggers*). Na sledećoj slici (slika 9) je prikazan izgled triger zone u toku editovanja scenarija – plava kružnica sa zastavicom u centru označava zonu gde triger može biti aktiviran.



Slika 9. Prikaz zone trigera

Programatično kreiranje trigera, kao i niz akcija koje on pokreće predstavljeni su sledećim kodom (slika 10).

```
_trg = createTrigger["EmptyDetector",getmarkerpos "marker4":
_trg setTriggerArea[10,10,0,false];
_trg setTriggerActivation ["west","PRESENI",false];
_trg setTriggerStatements ["this","funit1,unit2,unit3,unit4,unit5]
ordergetin false", "hint 'trigger off'"];
```

Slika 10. Prikaz koda za kreiranje trigera

Praktično kreira se triger određenog tipa (*empty detector*), koji se pozicionira na odgovarajuće koordinate na mapi uz određivanje zone reagovanja. Funkcija koja se izvršava prilikom njegovog aktiviranja nalazi se u poslednjoj liniji koda – u konkretnom primeru vrši se iskrcavanje 5 vojnika iz vozila.

Od tog momenta igrači dobiju kontrolu nad svojim jedinicama, a na ekranu se ispisuje tekst zadatka koje odeljenje treba da izvrši i za to se koristi naredba *titleText*.

Za kreiranje snaga protivnika dizajniran je poseban modul - skript fajl *opfor.sqf*. Za kreiranje jedinica koristi se funkcija *createUnit*. Jedinica može da predstavlja pojedinačnog vojnika ili njihovu grupu. Dalje, jedinica može da bude kontrolisana od strane učesnika, ili od strane VBS-a (*AI Unit Control - Artificial Intelligence*) i u tom slučaju je potpuno samostalna. Na slici 11. nalazi se prikaz koda za kreiranje crvenog tima.

```
createcenter east;
_unitGroupEast = creategroup east;
enemy1= unitGroupEast createmnit
["vbs2_af_taliban_ak74gla",getmarkerpos "emarker",[],0,"NONE"];
enemy2= unitGroupEast createmnit
["vbs2_af_taliban_ak74gla",getmarkerpos "emarker",[],0,"NONE"];
enemy3= unitGroupEast createmnit
["vbs2_af_taliban_ak74gla",getmarkerpos "emarker",[],0,"NONE"];
enemy4= unitGroupEast createmnit
["vbs2_af_taliban_ak74gla",getmarkerpos "emarker",[],0,"NONE"];
enemy5= unitGroupEast createmnit
["vbs2_af_taliban_ak74gla",getmarkerpos "emarker",[],0,"NONE"];
```

Slika 11. Kreiranje crvenog tima

Pored kreiranja jedinica neophodno je podesiti i njihovo ponašanje korišćenjem naredbe *setCombatMode*. Postoje pet nivoa obučenosti stepenovan od najnižeg do najvišeg „blue“, „green“, „white“, „yellow“ i „red“. Praktično u toku istraživanja je zaključeno da je za suprotnu stranu nivo „white“ optimalan za konfortaciju sa nivoom učesnika simulacije. Nivo „white“ znači da AI jedinice neće otvarati vatru izuzev u neposrednoj opasnosti i reagovalaće defanzivno ako budu napadnute. Podešavanje nivoa obučenosti se vrši pojedinačno za svaku jedinicu, kao što je prikazano na sledećem skript fragmentu gde je 7 suparničkih AI vojnika postavljeno na nivo „white“ (slika 12).

```
enemy1 setcombatmode "white";
enemy2 setcombatmode "white";
enemy3 setcombatmode "white";
enemy4 setcombatmode "white";
enemy5 setcombatmode "white";
enemy6 setcombatmode "white";
enemy7 setcombatmode "white";
```

Slika 12. Podešavanje obučenosti crvenog tima

Borbeni mod „red“ označava ofanzivno reagovanje jedinice – neposredno po otkrivanju suparnika. To ne znači da će vatra biti otvorena van dometa naoružanja, ali preduzeti borbeni postupci će biti sa ciljem uništavanja protivnika (prikriveno kretanje, zauzimanje zaklona, osmatranje, nišanje). Mod „green“ označava da jedinice neće napadati protivnike sve dok ne budu napadnuti. Mod „yellow“ omogućava da jedinica napadne protivnika ako je on u zoni dejstva pri čemu jedinice zadržavaju raspored (formaciju). Mod „blue“ označava da jedinice nikada neće napasti protivnika. Iz svega ovoga se može izvesti zaključak o „white“ modu kao najpogodnijem za potrebe obuke jedinica.

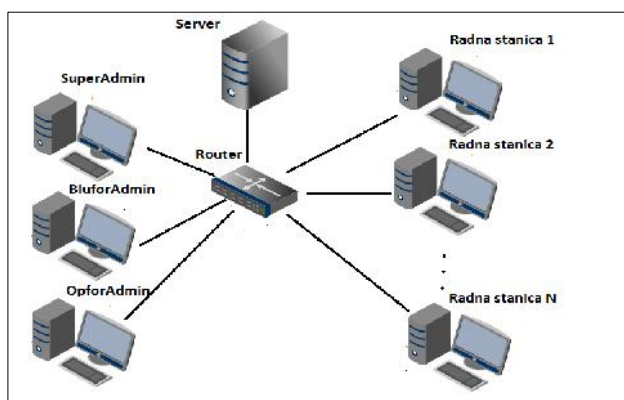
## 5. KONFIGURISANJE SISTEMA I PRIKAZ UPOTREBE

*VBS3 Dedicated server* je instanca VBS3 čija je svrha da hostuje misije i komunikaciju sa učesnicima. Kao što se može videti sa slike 13. gde su u topologiji mreže prikazani svi učesnici. Osnovna podešavanja u mreži:

- Žično ili bežično ruterovanje stanica i servera.
- Zbog intenzivne razmene sadržaja između računara (velika interaktivnost usled intenzivne dinamike dejstva), optimalno je da sistem bude postavljen na izolovanoj lokalnoj mreži uz isključene *firewall* mehanizme i antivirusno skeniranje.
- Ista verzija VBS3 instalacije na svim računarima.
- Softverski *WIBU*, ili hardverski *HASP* rešene licence.



Interesantno je da su instalacije na svim platformama identične, tako da je ovo mreža ravnopravnih učesnika. Ovakvo konfigurisana mreža je dakle fleksibilna, pošto svaka stanica može da bude serverska, administratorska ili učesnička. Mreža treba da poseduje bar jednu ili više administratorskih stanica pomoću kojih se upravlja vežbom. Određivanje režima rada radne stanice je u fazi startovanja softvera. Administratorska stanica ima mogućnost da pokrene sevrer na drugoj platformi. Ovakva fleksibilnost omogućava da simulacija nastavi da se izvršava i u slučaju da usled tehničkih kvarova ili prekida dođe do ispada jedne ili više stanica. Ako ima više administratorskih stanica, u slučaju ispada jedne, druga može da preuzme kontrolu nad vežbom. Ostale radne stanice administrator može da uključi i u toku izvođenja vežbe.



Slika 13. Organizacija korisničke opreme

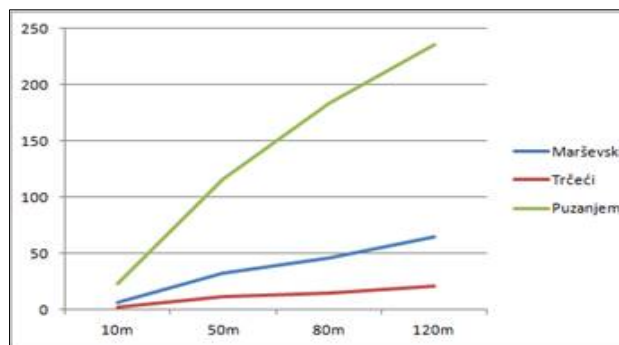
Pokretanje VBS3 može se izvršiti u dva modula: korisničkom i administratorskom. Administratorski mod omogućava kompletan pristup audio, video i ostalim naprednim podešavanjima i ima kompleksan interfejs. U korisničkom modu podešavanja su jako ograničena, interfejs pojednostavljen, a RTE (Real Time Editor) nije dostupan jer je on namenjen za komandovanje i kontrolu simulacija.

## 6. EVALUACIJA PREDLOŽENOG REŠENJA

Sve veća upotreba simulacija i igara u edukaciji i treningu postavlja nam pitanje šta time dobijamo, a šta gubimo? Odgovor dobijamo razvijanjem metoda za evaluaciju softvera na kome se izvodi edukacija kako bismo uvideli njegove mogućnosti, ograničenja, kao i uticaj na učenje [6].

Na taktičkom nivou, kako bi uspešno izvršili vežbu, moramo da poznamo mogućnosti jedinica sa kojima raspolazemo. Izvršavajući određene taktičke zadatke, kao što je zauzimanje položaja, napad na neprijateljske jedinice, odbrana zauzetih položaja jedinice. Vreme koje je potrebno jedinici u simulaciji da pređe određenu distancu zavisi od mnogih faktora, kao što su: konfiguracija terena, oprema koju nosi, osobine terena (blato, šuma, tvrd teren) kao i od izdržljivosti jedinica (Fatigue). Veštačka inteligencija implementira u VBS3 softveru omogućava kontrolu ovih varijabli njihov uticaj na simulaciju kako bi virtuelno ponašanje približila što

više realnom. Slika 14. prikazuje zavisnosti vremena od načina kretanja i distance na ravničarskom terenu. Merenja su izvršena za kretanja: marševski (normalan hod), trčeći i puzanjem. U VBS3 ova zavisnost je izražena varijablom zamor (*fatigue*).



Slika 14. Kretanje jedinica na ravničarskom terenu

Zamor je najmanje pri hodu (marševski), dok je najveći pri trčanju. Indikator zamora ima tri stanja: *white*, *orange* i *red* što je prikazano u tabeli 1.


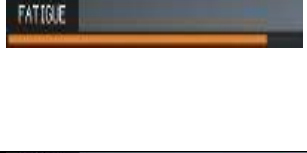
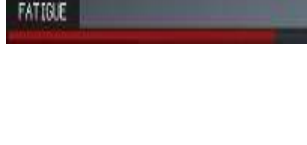
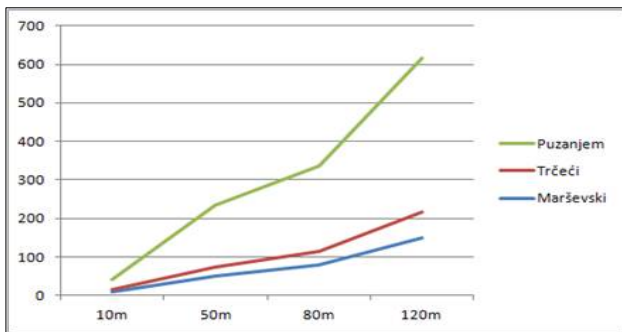
0% - 49.9% indikator umora je <i>white</i> . U ovom stanju jedinica ima mogućnost da se kreće u punoj brzini, ali postoje izuzeci ako je previše opterećena opremom ili se kreće uzbrdo.	
50% - 89.9% indikator umora je <i>orange</i> . Umanjuje performanse jedinice, ne može da se kreće u punoj brzini.	
90% - 100% indikator je <i>red</i> . Ovo stanje govori da je jedinica iscrpljena i automatski staje da se odmori i regeneriše.	

Tabela 1. Indikatori zamora jedinica

Merenje je izvršeno i na brdskom terenu. Rezultati su prikazani na sledecem dijagramu (slika 15.) i na osnovu njih se može videti uticaj indikatora zamora na performanse jedinice. Kako se deonica povećava vidimo eksponencijalni rast vremena koje je potrebno da se deonica pređe. Jedinica koja se kreće trčeći uzbrdo ima drastičnu promenu indikatora zamora, koji u veoma kratkom roku prelazi u *orange* stanje, a ukoliko jedinica nastavi kretanje i u *red*. Ovo je jako značajan podatak i na ovaj način znamo mogućnosti jedinica u kretanju, a samim tim i njene taktičke sposobnosti koje možemo prilagoditi u skladu sa zadatkom i potrebama vežbe.



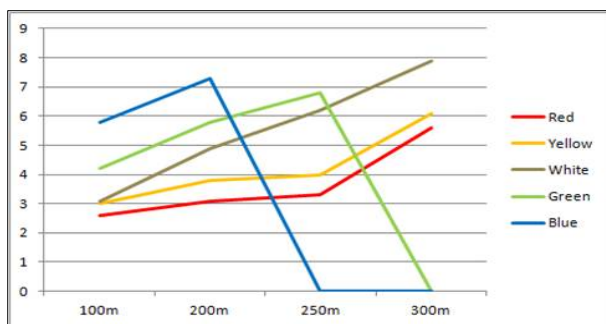
Slika 15. Kretanje jedinica po brdskom terenu

Pored osnovnih, postoje i specifična kretanja koja su modelovanja u sistemu. U tabeli 2. prikazana je zavisnost vremena ukrcavanja posade u vozilo od udaljenosti vojnika od vozila. U merenju je učestvovala kompletna posada borbenog vozila.

	Neposredno ispred vozila	10m	100m
Vreme [sek.]	4,80	7,69	22,90

Tabela 2. Vreme ulaska jedinica u vozilo

U implementaciji scenarija potrebno je i utvrditi i koliko AI jedinicama treba vremena da iz različitih zona dejstva reaguju na učesnički (tzv. plavi) tim (slika 16.). Ovaj podatak je u uskoj vezi sa nivoom obučenosti AI jedinica. U stanjima visoke obučenosti (*red* i *yellow*) vreme koje protekne od uočavanja jedinice do otvaranja vatre je veoma malo i učesnici koji nisu dovoljno obučeni i nemaju iskustva u korišćenju softvera nemaju ikakve šanse protiv njih. Opadajući trendovi za plavi i zeleni nivo govori o tome da na distancama od 250m, odnosno 300m AI jedinice postaju potpuno pasivne u odnosu na protivnika.



Slika 16. Vreme koje protekne od momenta ulaska u zonu dejstva do momenta dejstva AI jedinica

U tabeli 3. prikazano je vreme koje je potrebno od momenta uočavanja, prosečno utreniranom igraču da neutrališe nerijateljskog vojnika na različitim distancama. Upoređujući ove podatke sa podacima za AI jedinice, očigledno je da je reakcija prosečnog igrača približna *white* nivou obučenosti.

	100m	200m	250m	300m
Vreme [sek.]	3,00	5,50	6,60	8,10

Tabela 3. Vreme koje je potrebno igraču da neutrališe neprijatelja

To znači da ili nivo obučenosti učesnika treba da dostigne nivo zahtevan za dati scenario (priprema za vežbu), ili prilikom kreiranja scenarija ostvariti mogućnost promene nivoa obučenosti protivnika (AI jedinica) u skladu sa trenutnom obučenosti učesnika.

## 7. ZAKLJUČAK

Upotreba VBS platforme u istraživanju i obrazovanju omogućava eksperimentaciju uz minimalne utroške resursa, povećanje kvaliteta obrazovanja boljom primenom za terenske sadržaje obuke (tranzicija teorijskog u praktično znanje prenosom iskustva iz virtuelnog u stvarno okruženje). Kao argumentacija, u radu je predstavljen samo deo jednog tipično vojnog scenarija. Virtuelne simulacije međutim nemaju isključivo vojnu namenu, već se mogu primeti i u obuci za sprečavanje i suzbijanje vanrednih događaja i elementarnih nepogoda, protivterorističku borbu, konverziju, pregovaranje u različitim kulturološkim okruženjima i situacijama, zaštitu i kontrolu ulaska i izlaska u/iz bezbedno osetljivih zona i slično. Prednost je i to što se se mogu simulirati uslovi koji se ne dešavaju uopšte, ili retko u realnom svetu.

Postoje mnogobrojne mogućnosti za dalji razvoj i proširenje softvera kao što je VBS3-VBSFusion API interfejs, koji omogućava spregu sa drugim sistemima (npr. komandno – informacionim sistemima, ili drugim simulacionim sistemima), mogućnosti generisanja stereometrijske (3D) slike, koja se može koristiti za kombinovanje stvarnog i virtuelnog korišćenjem Oculus uređaja i senzorske opreme.

## LITERATURA

- [1] Minhua, M. and Oikonomou, A. "Serious games and edutainment application, Volume II", 2016.
- [2] Tobias, S., Fletcher, J.D. and Wind, A. "Computer games and Instructions", Information Age Publishing Inc., 2011.
- [3] Šimić G. "Constructive simulation as collaborative learning tool in education and training if crisis staff", Interdisciplinary journal of information, knowledge, and management, 2012.
- [4] Fusion for VBS3 v3.2 User Guide, SimCentric Technologies, 2014.
- [5] VBS3 Manuals Version 17.1.0, Bohemia Interactive Simulations, 2017.
- [6] Hainey, T., Baxter, G., Boyle, E., Moreno-Ger, P. and Connolly, T. "Psychology, pedagogy, and assessment in serious games", Published by IGI Global, 2013.

# Implementacija i verifikacija AES algoritma na ATmega32 mikrokontroleru

## Implementation and Verification of the AES Algorithm on ATMEGA32 Microcontroller

Stefan Sretenović<sup>1</sup>, Stefan Božanić<sup>2</sup>, Dejan Kršljanin<sup>1</sup>, Radomir Prodanović<sup>1</sup>, Vladimir Kekić<sup>3</sup>

Centar za primenjenu matematiku i elektroniku, Vojska Srbije<sup>1</sup>

Centar za komandno informacione sisteme i informatičku podršku, Vojska Srbije<sup>2</sup>

250. Raketna brigada, Vojska Srbije<sup>3</sup>

**Sadržaj** – U današnje vreme zaštita podataka predstavlja jednu od najvažnijih potreba modernog čoveka. Svako danas želi da informacije koje šalje ili dobija budu nevidljive za treće lice. U radu je predstavljena implementacija AES algoritma za šifrovanje podataka na mikrokontroleru, slanje tih podataka na računar, kao i provera algoritma dešifrovanjem u aplikaciji koja ima zvanične biblioteke za pomenuti algoritam. U prvom delu je predstavljen koncept rada ovog uređaja i njegova funkcionalnost. Drugi deo rada opisuje realizaciju implementacije algoritma i samu aplikaciju za proveru pisanu u programskom jeziku C#.

**Abstract** – Nowadays data security is one of the most important needs for a modern man. Everyone wants their sent and received information secured from a third party. This paper is presenting implementation of AES algorithm for data encryption on microcontroller, sending those data to a computer, and the control of the algorithm by using official library for decrypting mentioned algorithm. The first part of this paper shows system working concept and its functionality. The second part of this paper describes how the implementation was done and shows application for verification written in C#.

### 1. UVOD

Zaštita informacija je oduvek bila jedan od važnijih aspekata čovekovog života. Svako želi da neki deo svojih znanja sakrije od nepoželjnih ljudi. Zbog toga su se sa razvojem civilizacije razvijali i razni načini sakrivanja, pa i šifrovanja podataka. Nekada su se ručno šifrovala pisma i dokumenta, i to je iziskivalo mnogo vremena, kao i veliki broj učenih ljudi. Danas je sve to malo drugačije.

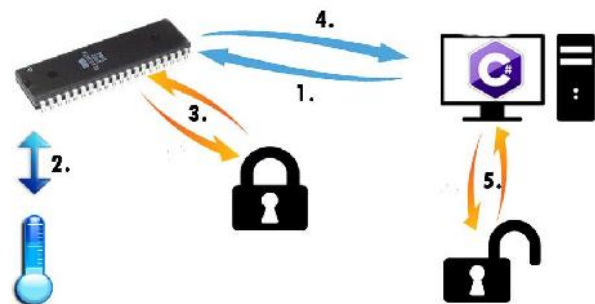
Danas se gotovo svaki podatak šalje elektronskim putem, počevši od običnih poruka, pa sve do poverljivih državnih akata. S obzirom da danas svako komunicira elektronskim putem, povećao se i broj ljudi koji žele da prikupljanjem informacija drugog čoveka profitira. Zbog toga je zaštita tih podataka u moderno vreme od ogromne važnosti. Pojava računara je omogućila da se komplikovane računarske radnje mogu uraditi u trenutku, što je otvorilo vrata implementiranju šifarskih algoritama u skoro svaki softverski i hardverski sistem. Implementiranje u softverske sisteme je rešeno pravljenjem univerzalnih

biblioteka, za skoro sve programske jezike, koje programeri mogu sa lakoćom koristiti uz minimalno poznavanje šifarskih algoritama. Problem se javlja ako takva biblioteka ne postoji. Takav je programski jezik microC koji se koristi za programiranje mikrokontrolera.

Zbog pomenutih razloga, javila se ideja za pravljenje sistema koji ima za cilj da vrši šifrovanje i dešifrovanje trenutno izmerene vrednosti temperature pomoću AES algoritma. Šifrovanje se vrši na samom mikrokontroleru pomoću ručno implementiranog koda (bez korišćenja biblioteke), dok se dešifrovanje vrši u Windows aplikaciji koja ima zvaničnu biblioteku za upotrebu AES algoritma. U nastavku je detaljno opisan pomenuti sistem.

### 2. BLOK ŠEMA SISTEMA

Blok šema sistema predstavljena je na Slici 1.



Slika 1. Blok šema sistema

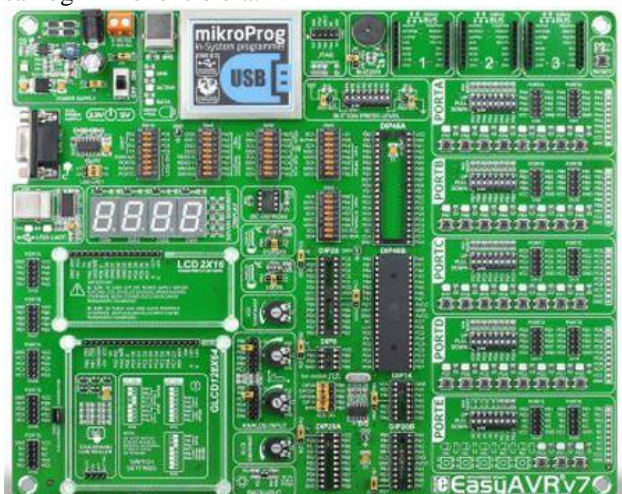
Na zahtev Windows aplikacije, pomoću TCP/IP komunikacije (veza 1.), mikrokontroler uzima trenutnu vrednost temperature i smešta je u string (veza 2.). Zatim mikrokontroler šifrjuje taj string ključem određene dužine (veza 3.) i šalje tako šifrovan string Windows aplikaciji (veza 4.). Potom aplikacija, koristeći isti ključ, vrši dešifrovanje primljenog stringa (veza 5.) i prikazuje na ekranu. U nastavku rada biće detaljno opisana svaka komponenta kao i funkcionalnost sistema kao celine.

#### 2.1 RAZVOJNA PLATFORMA EASYAVR V7

Mikrokontrolerska platforma EasyAVR v7 [1] predstavlja razvojno okruženje za programiranje i testiranje programa za AVR mikrokontrolere (Slika 2.). Eksterni moduli (click



module) pružaju mogućnost proširenja funkcionalnosti samog mikrokontrolera.



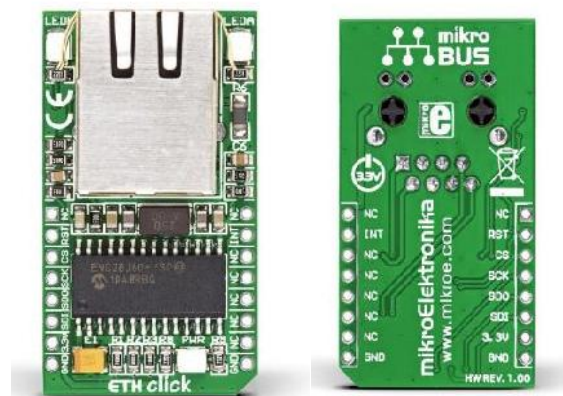
Slika 2. EasyAVR v7

Ova razvojna platforma je korišćena prilikom programiranja i testiranja sistema za proveru stanja kvaliteta vazduha. Na njoj se nalazi mikrokontroler ATmega32 kompanije Atmel [1]. Radi se o osmobicnom kontroleru iz familije AVR (Advanced RISC), sa naprednom arhitekturom procesora i smanjenim brojem instrukcija. AVR jezgro poseduje 32 registra opšte namene. Svi registri su direktno povezani sa ALU (Arithmetic Logic Unit). Svaki od registara može imati ulogu ACC-a (akumulatora) pri obavljanju aritmetičko-logičkih operacija. Podržan je od strane mnoštva paketskih programa, sistema, razvojnih alata kao na primer C kompajler i programa za otklanjanje grešaka odnosno simulatora. Memorijske performanse su znatno poboljšane kombinovanim korišćenjem fleš i EEPROM memorije. AVR mikroprocesore odlikuje velika brzina izvršenja, oko 1 MIPS po MHz, odnosno 16 MIPS-a, ako radi na 16 MHz, što je oko 12 puta više nego kod standardnih osmobicnih mikroprocesora.

U ovom projektu iskorišćena je pin PORT-a A4 za komunikaciju mikrokontrolera sa temperaturnim senzorom DS1820, i tri pina PORT-a B za SPI komunikaciju mikrokontrolera i ETH Click modula.

## 2.2 ETH CLICK MODUL

ETH click modul (Slika 3.) koristi se za povezivanje mikrokontrolera na Ethernet. Ploča sadrži ENC28J60 Ethernet čip koji za razmenu podataka koristi SPI (Serial Peripheral Interface), 8 Kbytes bafer, MAC & PHY (Media Access Control and Physical Layer), kao i 10 pinova preko kojih se click modul povezuje na razvojnu ploču. ENC28J60 je 28-pinski 10Base-T Ethernet kontroler, koji karakteriše brzina od 10 Mbit/s, UTP kategorije 3/5 tip kabla sa maksimalnim mogućim rastojanjem od 100m [2].

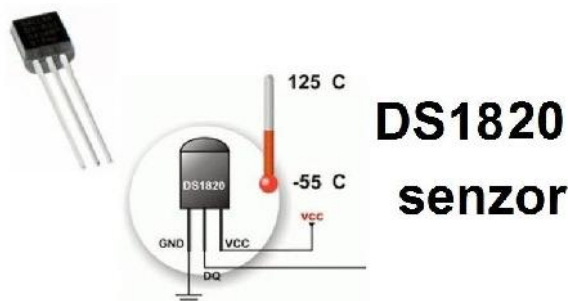


Slika 3. ETH click modul

## 2.3 DS1820 TEMPERATURNI SENZOR

Digitalni temperaturni senzor DS1820 (Slika 4) je namenjen za merenje temperature u rezoluciji od 9 bita. Temperaturni senzor DS1820 komunicira sa mikrokontrolerom pomoću 1-Wire interfejsa.

Senzor ima mogućnost merenja temperatura od  $-55^{\circ}\text{C}$  do  $+125^{\circ}\text{C}$ , a preciznost izmerene temperature je  $\pm 0.5^{\circ}\text{C}$  za temperature od  $-10^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$ . Radi na naponu od 3.0V to 5.5V [4].



Slika 4. Temperaturni senzor DS1820

## 3. TCP PROTOKOL

U računarskom svetu protokol označava skup pravila koja određuju kako dva programa mogu da komuniciraju. Računari komuniciraju tako što razmenjuju određeni set poruka, a protokol određuje formate tih poruka. Protokoli omogućuju i razmenu podataka između različitih vrsta računara. TCP/IP je set protokola razvijen da omogući umreženim računarima da dele resurse putem mreže i jedan je od najrasprostranjenijih. Komunikacija u mreži i između njih se obavlja preko čvorova, TCP/IP hostova, gde je svakom čvoru u mreži dodeljena jedinstvena IP adresa. On je jedan od protokola, koji traži potvrdu da je paket stigao.

TCP će uvek tražiti ponovno slanje paketa ukoliko dođe do gubitka, te je pogodan za sigurniju razmenu podataka gde brzina nije toliko bitna. Osnovna jedinica TCP protokola je segment, koji se pakuje u IP pakete i šalje preko mreže. Dozvoljava dvosmerni prenos podataka. Kako bi TCP funkcionisao, neophodno je obaviti proces uspostavljanja veze. Uspostavljanje veze u TCP protokolu funkcioniše po klijent – server principu, odnosno neophodno je izvršiti proces na jednom računaru radi uspostavljanja veze sa drugim. Prilikom uspostavljanja veze, razmenjuju se tri specijalna segmenta ( three way handshake) kada klijent šalje serveru prvi specijalni TCP segment, na šta server odgovara drugim specijalnim segmentom, nakon čega klijent odgovara trećim specijalnim TCP segmentom.

#### 4. AES ALGORITAM

AES (Advanced Encryption Standard) predstavlja jedan od kriptografskih algoritama koji se koriste za zaštitu elektronskih podataka. AES standard se temelji na simetričnom Rijndael algoritmu, a razvijen je da bi zamenio DES algoritam jer njegova sigurnost u današnje vreme više nije dovoljna. Prihvaćen je od strane NIST-a (National Institute of Standards and Technology) u FIPS 197 dokumentu [3]. AES algoritam predstavlja algoritam simetričnog ključa (isti ključ se koristi i za šifrovanje i za dešifrovanje). Veličina bloka podataka koje šifrjuje je 128 bitova, a dužina ključa 128, 192 ili 256 bitova (da bi se razlikovali nazivaju se AES-128 AES-192 i AES-256 algoritam).

Projektovan je da bude i bezbedan i brz. Ukupan broj mogućih ključeva kod AES-128 je  $2^{128} \approx 3 \times 10^{38}$ , što znači da bi za dekripciju takvog ključa bilo potrebno  $5.4 \times 10^{24}$  godina za jednu dekripciju po  $\mu s$  ili  $5.4 \times 10^{18}$  godina za  $10^6$  dekripcija po  $\mu s$ . Pokazao se i kao otporan na sve do sada poznate napade na blokovske šifarske sisteme.

AES algoritam, kao i ostali blok šifarski algoritmi, ima svoje kriptografske modove. Kriptografski mod je način upotrebe bazičnog blok šifarskog algoritma koji koristi jednostavne operacije (jer je bezbednost već određena bazičnim kriptografskim algoritmom). On je značajan, jer bez njega algoritam kada god naiđe isti blok otvorenog teksta, on daje isti blok šifrovanog teksta. To omogućava trećem licu da kreira tzv. elektronsku kodnu knjigu i da bez poznavanja ključa može da čita poruke koje se razmenjuju. Najpoznatiji kriptografski modovi su: mod elektronske kodne knjige – ECB (Electronic CodeBook) i mod ulančavanja blokova – CBC (Cipher Block Chaining).

U ovom projektu korišćena je implementacija AES-128 algoritma u ECB modu.

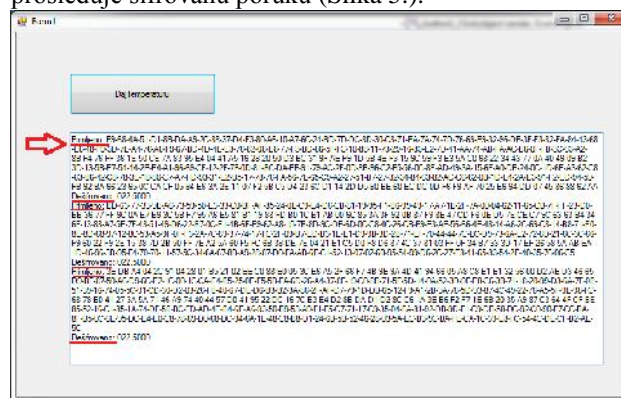
#### 5. SOFTVERSKA IMPLEMENTACIJA

Za potrebe ovog sistema razvijene su dve aplikacije, jedna za rad mikrokontrolera, a druga za Windows platformu. Aplikacija za mikrokontroler je pisana u programskom jeziku C koristeći okruženje mikroC PRO for AVR, dok je

Windows aplikacija pisana u programskom jeziku C# koristeći okruženje Visual Studio Ultimate 2013.

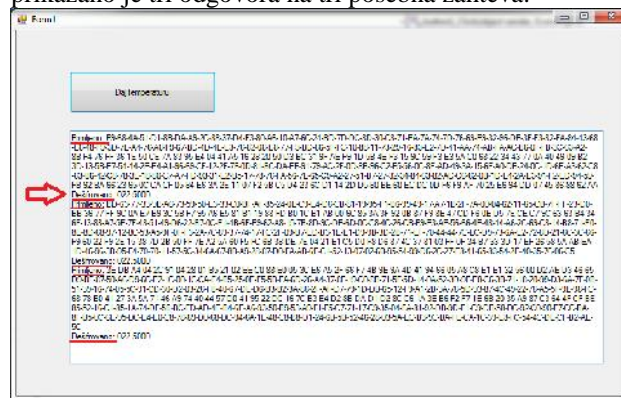
U aplikaciju za mikrokontroler, pored koda za podešavanje hardverskih komponenti, implementiran je i AES algoritam u ECB modu koji je potvrđen u skladu sa podacima u: NIST-ovoj specijalnoj objavi 800-38A iz 2001. godine, dodatak F: Primer vektora za modove operacija AES algoritma [4].

Windows aplikacija je namenjena za komunikaciju sa mikrokontrolerom pomoću TCP/IP konekcije, gde je aplikacija u uspostavljenoj hijerarhiji, klijent. Pritiskom na dugme, aplikacija šalje zahtev mikrokontroleru, i on joj prosleđuje šifrovanu poruku (Slika 5).



Slika 5. Izgled Windows aplikacije

Aplikacija u pozadini izvrši dešifrovanje dobijene poruke, i prikaže je na ekranu (Slika 6.). Dešifrovanje se vrši pomoću Microsoft-ove zvanične biblioteke za AES algoritam: System.Security.Cryptography.Aes. Upotrebom te biblioteke, uzimajući u obzir da je Microsoft pouzdan izvor, potvrđena je uspešna implementacija AES algoritma na mikrokontroler ATmega32. Na slikama 5 i 6 prikazano je tri odgovora na tri posebna zahteva.



Slika 6. Izgled Windows aplikacije

#### 4 ZAKLJUČAK

Ovaj projekat je realizovan i testiran i u tom periodu testiranja nije bilo problema. Uređaj je uspešno šifrovao izmerene vrednosti temperature pomoću AES algoritma, što je potvrđivala Windows aplikacija.

Realizacijom ovog projekta uspešno je potvrđeno korišćenje AES algoritma na mikrokontroleru ATmega32.



Pravci daljeg razvoja sistema je svakako optimizacija koda radi bržeg funkcionisanja sistema, kao i rad sa nekim drugim uređajima i modulima (npr. Wi-Fi Click modulom). Cilj je i pronalazak realne primene samog sistem.

Aplikacija je izrađena tako da je nadogradnja relativno jednostavna. Ideja je da se postojeće funkcije prošire, ili dodaju potpuno nove mogućnosti, kao na primer automatizacija slanje zahteva Windows aplikacije i upisivanje u bazu podataka nakon prijema povratne poruke.

## 5 LITERATURA

- [1] ATmega32 Datasheet, ATMEL.  
<http://www.atmel.com/images/doc2503.pdf>
- [2] ETH Click module Datasheet, MICROCHIP.  
<http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf>
- [3] Federal Information Processing Standards Publication 197, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.  
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>
- [4] <https://github.com/kokke/tiny-AES-c>

# Povezivanje Android aplikacije sa Arduino-om upotrebom MQTT protokola

## Connecting Android Application with Arduino through MQTT Protocol

Božanić Stefan<sup>1</sup>, Antonić Mladen<sup>2</sup>, Sretenović Stefan<sup>1</sup>, Kekić Vladimir<sup>1</sup>  
*Vojska Srbije<sup>1</sup>, Vojna akademija<sup>2</sup>*

**Sadržaj** – Razmena informacija između različitih uređaja i upravljanje istim preko interneta teži da postane neophodna stvar savremenog čoveka. U radu je predstavljena jedna praktična realizacija sistema za daljinsko upravljanje i nadzor uređajima preko interneta korišćenjem MQTT protokola. Upotrebom Arduino platforme sa WiFi modulom i senzora temperature prikazana je kontrola LE diode kao i očitavanje trenutne temperature u prostoriji. U radu je predstavljen koncept rada MQTT protokola kao i njegova praktična realizacija na pomenutom hardveru kojim se upravljanja preko interneta. Za upravljanje LE diode i prikazivanje očitane temperature korišćena je Android korisnička aplikacija pisana u softverskom paketu Android Studio.

**Abstract** – Exchange of information among different devices and controlling them through Internet is becoming necessity to modern humanity. This article is presenting practical realization of system for remote control and supervising devices through Internet using MQTT protocol. Control of the LE diode and showing current temperature in the room is realized by using Arduino platform with WiFi module and temperature sensor. Working concept of the MQTT protocol is shown in this paper, and also practical realization with mentioned hardware that is controlled through Internet. For LE diode controlling and current temperature showing, Android user application, written in Android studio environment, was used.

### 1. UVOD

U današnje vreme sve je više uređaja, koji sadrže hardver, softver i razne senzore koji su povezani na mrežu, koja im omogućava razmenu podataka. Takva mreža povezanih uređaja naziva se Internet Stvari (engl. *Internet of Things*) [1] [5]. Jedna od zanimljivih primena su svakako pametni gradovi, gde se koristi mreža senzora, raspoređenih po celom gradu, koja prikuplja podatke, kao što su temperatura, kvalitet vazduha, jačina buke, kao i mnogi drugi parametri. Prikupljeni podaci se obrađuju i koriste za pružanje informacija korisnicima, kao što je planiranje rute kretanja na temelju prometa ulice ili kvalitete vazduha.

Svaki uređaj u mrežnom sistemu je jedinstveno identifikovan na temelju ugrađenog računarskog sistema, i u mogućnosti je da se služi postojećom mrežnom infrastrukturuom, znanom kao Internet [2]. Međutim, uređaji u mreži mogu biti različiti po performansama (hardveru i softveru). Na primer, uređaji koji pomoću

senzora prikupljaju podatke i šalju ih na dalju obradu, ne zahtevaju hardver velikih performansi. Jedan od primera uređaja pogodnih za takvu svrhu je uređaj Arduino, koji je predstavljen u ovom radu. Važno je posvetiti pažnju i optimizaciji i minimalizaciji kod projektovanja sistema, kako bi se smanjili zahtevi na hardveru, potrošnja električne energije i mrežnog prometa.

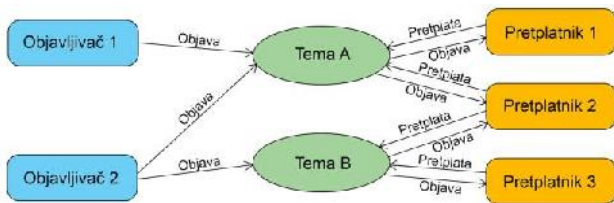
Jedna od najvažnijih stavki kod takvih sistema je komunikacija, odnosno razmena poruka među sistemima [11]. Jedan od najčešće korišćenih protokola u internet stvarima je protokol MQTT, čija je namena razmena podataka. Glavna karakteristika ovog protokola je to što je namenjen za korišćenje kod sistema gde je bitno minimizirati mrežni promet i zahteve hardvera, u uslovima gde je veza nestabilna i gde je mogućnost gubitka poruke velika. Protokol funkcioniše po principu izdavač-pretpatnik, uz slanje poruka putem mrežnog sloja TCP.

U svrhu demonstracije rada protokola MQTT, implementiran je jednostavan sistem na uređajima Arduino Uno i na korisničkoj Android aplikaciji. Putem navedenog protokola i očitane temperatura sa temperaturnog senzora sa jednog Arduino uređaja može se ta temperatura prikazati na Android uređaju, i mogućnost uključivanja i isključivanja diode na drugom Arduino uređaju sa iste Android korisničke aplikacije. U nastavku će biti opisan MQTT protokol, korišćeni hardver i biće prikazana Android aplikacija sa opisom rezultata testa.

### 2. MQTT PROTOKOL

MQTT (engl. *Message Queuing Telemetry Transport*) [3], poznat i po svom starom imenu *MQ Integrator SCADA Device Protocol* je pojednostavljen protokol za komunikaciju između uređaja, baziran na principu izdavač-pretpatnik, koji koristi mrežni protokol TCP/IP [7]. Osmišljen je da bude otvoren, lagan i jednostavan za implementaciju, odnosno da se može koristiti u prostorno ograničenim okruženjima sa ograničenim mogućnostima procesiranja, malim kapacitetom memorije (programske i radne) i sa velikim kašnjenjima. Kao takav, smanjuje zahteve na propusnu moć mreže i predstavlja prihvatljivo rešenje za korišćenje u sistemima sa nestabilnom mrežnom vezom gde prevladavaju male brzine prenosa i gde postoji velika mogućnost za gubitak informacija. Protokol je nastao krajem 1990-ih i početkom 2000-ih godina, a inicijalno je razvijen od strane firme IBM. Danas je to otvoreni protokol.

Princip izdavač-pretpatnik (engl. *publish-subscribe*) [4] je obrazac za razmenu poruka, u kojem pošiljaoci poruka, koji se nazivaju izdavač (engl. *publishers*), ne šalju svoje poruke unapred poznatom primaocu poruke, već ih smeštaju u klase, koristeći teme. Na taj način izdavači ne znaju ko će sve primiti poruku. Pretplatnici (engl. *subscribers*) se pretplaćuju na teme (engl. *topic*) koje ih zanimaju, i tako primaju sve one poruke koje izdavači objavljuju na tu temu. Načelo rada je prikazano na slici 1. Pretečom ovog obrasca se smatra sistem za novosti, pod imenom Isis Toolkit, opisan 1987. godine.



Slika 1. Prikaz načela obrasca izdavač-pretpatnik

Poruke koje izdavači objave, potrebno je filtrirati kako bi se poslane odgovarajućim pretplatnicima. Svaki pretplatnik prima određeni podskup poruka, za koje je zainteresovan. Za to je zadužen treći posrednik, koji se naziva broker. Pretplatnici se registruju na brokera i odlučuju na koje se teme žele pretplatiti, a broker zatim sprema poruke koje primi od izdavači i prosleđuje ih pretplatnicima koji su pretplaćeni na tu temu (engl. *store and forward*). Broker može postaviti prioritete poruka u redu poruka, pre nego što ih prosledi dalje. Postoje dva oblika filtriranja:

- 1) Bazirano na temi (engl. *topic-based*)
- 2) Bazirano na sadržaju (engl. *content-based*)

Moguće su i hibridne konfiguracije navedenih oblika, gde se pretplatnici pretplaćuju na određene teme, te postavljaju ograničenja na sadržaj poruka iz tih tema.

Izdavač-pretpatnik obrazac za prenos poruka ima određene prednosti i nedostatke, naspram ostalih oblika prenosa, kao što je na primer tradicionalno korišćeni klijent server (engl. *client-server*) obrazac, a to su:

1. Slaba veza i velika prilagodljivost
2. Nefleksibilno semantičko razdvajanje
3. Poteškoće kod prenosa poruka
4. Problem sa prilagođavanjem
  - Periodi opterećenja (engl. *load surges*)
  - Zastoji (engl. *slowdowns*)
  - Zasićenje usled emitovanja (engl. *IP broadcast storms*)
5. Problem sigurnosti [6]

Protokol MQTT koristi prethodno opisani obrazac objavi-pretpatni s pojedinim specifičnostima, za razliku od na primer protokola HTTP, koji koristi obrazac zahtev-odgovor. U središtu se nalazi posrednik (broker), na kojeg se spaja mnoštvo klijenata koji se pretplaćuju na određene teme (engl. *topic*), koje ih zanimaju. Takođe, klijenti se mogu povezati na posrednika i kao izdavači i objavljujati poruke na određene teme, pri čemu ih broker prosleđuje svim klijentima-pretpatnicima koji su pretplaćeni na te

teme. Reč je o principu događaja, gde klijent ne mora zahtevati informacije (engl. *pull*) od posrednik, već mu posrednik dostavlja informacije za koje je zainteresovan (engl. *push*), čim se pojavi nešto novo, odnosno čim se desi neki događaj (engl. *event*). Klijent može biti bilo koji uređaj, koji ima implementiran protokol MQTT, od malih ograničenih čvorova u obliku senzorskih sistema s mikrokontrolerom do velikih izdavača. Klijent mora znati za brokera, na kojeg se povezuje putem protokola TCP/IP, pa, ako je reč o pretplatniku, mora znati na koju se temu pretplaćuje.

Posrednik (broker) je središnji čvor kod protokola MQTT. Njegova zadatak je da prima objave od izdavača pa ih, pomoću tema i filtriranja, prosleđuje zainteresovanim klijentima-pretpatnicima. Svaki klijent mora znati za posrednika, tako da zna njegovu IP adresu i port, i tek onda ostvaruje trajnu vezu s posrednikom putem protokola TCP/IP, koja traje sve dok klijent ne zatraži prekid veze, ili dok ne dođe do raskida veze.

Za usmeravanje poruka prema klijentima koriste se teme (engl. *topics*). Svaki klijent-izdavač šalje objave u neku temu, dok se klijenti-pretpatnici pretplate na određenu temu i dobijaju sve objave koje klijenti šalju u istu. Tema nije potrebno konfigurisati, već je dovoljno slati objave na neku temu. Ako ona do tada nije postojala, kreira se nakon slanja objave u nju. Reč je o jednostavnom nizu znakova (engl. *string*), koji može sadržati više hijerarhijskih nivoa odvojenih znakom "/". Primer su senzori koji se nalaze u raznim prostorijama unutar kuće, kao i izvan kuće. Klijent se može pretplatiti na senzore kao što su:

```
/kuca/dnevni-boravak/temperatura
/kuca/soba/vlaznost
```

Moguće je i pretplatiti se istovremeno na više tema, koristeći zamenski znak (engl. *wildcard*). Zamenski znakovi se mogu koristiti isključivo kod pretplata, ne i kod objava. Postoje dva zamenska znaka:

```
+ za hijerarhije sa jednim nivoom
# za hijerarhije sa više nivoa
```

Na primer, ako se klijent želi pretplatiti na sve temperaturne senzore u kući, koristiće temu:

```
/kuca/+/temperatura
```

S druge strane, ako se želi pretplatiti na sve senzore u sobi, može koristiti temu:

```
/kuca/soba/+
```

S obzirom na to da je reč o zamenskom znaku za hijerarhije sa jednim nivoom, pretplata:

```
/kuca/+/temperatura
```

neće uključiti sljedeću pretplatu:

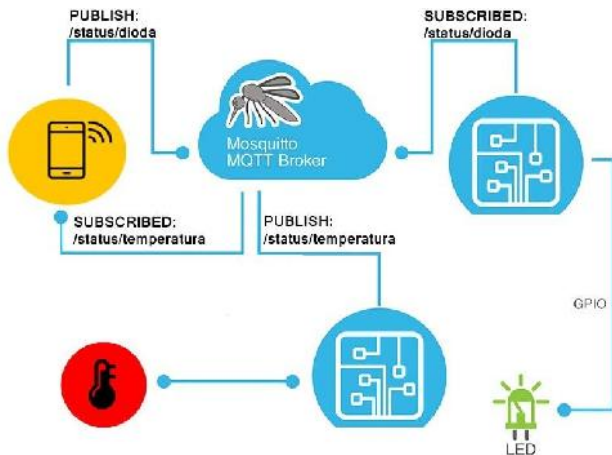
```
/kuca/soba/ormar/temperatura
```

Za to se koristi zamenski znak za hijerarhije sa više nivoa. Ako se klijent želi pretplatiti na sve moguće senzore unutar kuće, koristi temu:

```
/kuca/#
```

### 3. HARDVERSKA REALIZACIJA

Blok šema sistema predstavljena je na Slici 2.



Slika 2. Blok šema sistema

Za implementaciju protokola MQTT je potreban posrednik (broker). Radi jednostavnosti je odabran Mosquitto besplatni posrednik/poslužitelj. Ovaj posrednik nalazi se na adresi [test.mosquitto.org](http://test.mosquitto.org). Besplatan je i prikladan za testiranje protokola.

Sistem čine dve Arduino Uno [8] razvojne ploče, dva Wi-Fi modula za njihovo povezivanje na bežičnu mrežu, jedan temperaturni senzor DS1820 i jedna LE dioda.

Prvi Arduino Uno je povezan sa temperaturnim senzorom. Očitava temperatura sa senzora i tu vrednost objavljuje na temu /status/temperatura. Korisnička Android aplikacija se pretplatila na tu temu i ta se vrednost prikazuje korisniku u aplikaciji. Svaka promena očitane temperature se manifestuje na aplikaciji. Android aplikacija ima mogućnost uključivanja i isključivanja diode na drugom Arduino Uno razvojnoj ploči tako što objavljuje vrednost ON ili OFF na temi /status/dioda. Drugi Arduino je pretplaćen na tu temu i u zavisnosti od pročitane vrednosti menja stanja na pinu gde se nalazi dioda.

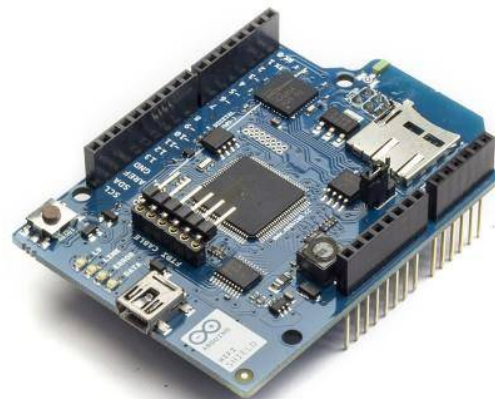
Arduino je platforma otvorenog koda (engl. *open-source*) namenjena za modeliranje i izgradnju elektroničkih uređaja. Platforma obuhvata hardver, u obliku samih razvojnih ploča s mikrokontrolerima i sa dodacima, koji se nazivaju moduli, uključujući programsko razvojno okruženje, pod nazivom Arduino IDE.



Slika 3. Arduino Uno

Arduino Uno (slika 3) se razlikuje od svih prethodnih ploča u tome što ne koristi FTDI USB-to-serial driver chip, već koristi Atmega16U2 programiran kao USB-to-serial pretvarač. Napaja se preko USB-a ili preko spoljnog izvora napajanja i tom slučaju se napaja sa naponom od 7V do 12V.

Za implementaciju MQTT protokola u ovom radu je, kod povezivanja na mrežu, korišćen Wi-Fi modul [9] prikazan na slici 4. Ovaj modul omogućava bežično povezivanje Arduino uređaja na mrežu koristeći 802.11 bežični protokol (Wi-Fi). Baziran je na HDG204 Wireless LAN 802.11b/g sistema (engl. *System in-Package*), AT32UC3 mikrokontroleru koji su podršku za TCP i UDP veze. Takođe podržava i WEP i WPA2 enkripcije, napaja se naponom od 5 V dobijenim iz samog uređaja Arduino. S Arduino uređajem komunicira putem SPI interfejsa, sadrži prostor za SD kartice, koji se može koristiti. Takođe, moguće je nadograditi sam modul pomoću ugrađenog mini USB konektora. Na modul se nalaze 3 svetleće diode koje označavaju uspešnu vezu, grešku kod spajanja, trenutno slanje ili primanje podataka.



Slika 4. Arduino WiFi modul [9]

Digitalni senzor temperature DS1820 [10] pruža 9-bitno merenje temperature. Jednožična je komunikacija između DS1820 temperaturnog senzora i mikrokontrolera.

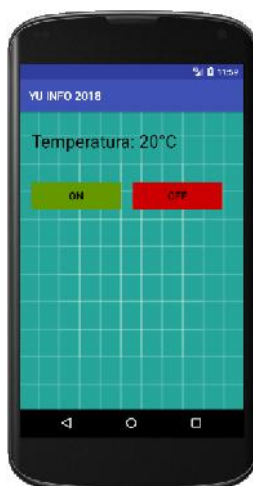
Opseg temperature merenja je od  $-55^{\circ}\text{C}$  do  $+125^{\circ}\text{C}$ . Tačnost merenja je  $\pm 0.5^{\circ}\text{C}$  za temperature od  $-10^{\circ}\text{C}$  do  $+85^{\circ}\text{C}$ . Rezolucija senzora je 9-bitna. Napaja se naponom od 3.0V do 5.5V.

### 4. SOFTVERSKA PODRŠKA SISTEMA

Korisnička aplikacija koja je pisana u okruženju Android Studio 3.0.1 i instalirana na Nexus 4 uređaj (operativni sistem Lollipop 5.1.1) prikazana je na slici 5.

U gornjem levoj uglu je prikazana temperatura koju je očitao prvi Arduino Uno uz pomoć temperaturnog senzora i objavljuje na temi /status/temperatura. Ispod prikazane vrednosti temperature nalaze se dva dugmeta sa nazivima ON i OFF čija se vrednost, na događaj klik, šalje na temu /status/dioda. U zavisnosti od te vrednosti menja se stanje diode na drugom Arduino uređaju.





Slika 5. Korisnička Android aplikacija

Program za Arduino razvojne sisteme je pisan u Arduino IDE 1.8.5 okruženju i korišćene su biblioteke za komunikaciju Arduino uređaja sa internet modulom (SPI.h) i biblioteka za MQTT protokol (Ethernet.h i PubSubClient.h). Zadatak prvog Arduino uređaja (pošiljaoca) je inicijalizacija i čitanje temperature sa temperaturnog senzora, inicijalizacija Wi-Fi modula i konekcija na bežičnu mrežu, slanje objave brokeru o svakoj promeni temperature. Zadatak drugog Arduino uređaja (primaoca) je inicijalizacija digitalnog izlaza na kojem je priključna LE dioda, inicijalizacija Wi-Fi modula i konekcija na bežičnu mrežu, osluškivanje teme o statusu LE diode kao i upravljanje njenim statusom.

## 5. REZULTATI TESTA

Da bi se sistem testirao upotrebljen je besplatni MQTT broker skinut sa zvaničnog sajta koji je instaliran na laptop računaru koji se nalazi u lokalnoj mreži. Preko AP (*access point*) su Arduino moduli konektovani na istu tu lokalnu mrežu. Kako bi i korisnička Android aplikacija bila na toj lokalnoj mreži morala bi da se konektuje na lokalni AP.

Sistem je testiran 24 sata za vreme kojih je praćena temperatura prostorije i menjano stanje LE diode. Rezultati su pokazali da nijednog momenta nije došlo do gubitka informacije o temperaturi ili do neočekivane promene stanja LE diode.

Dalja testiranja bi bila usmerena na zaštitu brokera od neovlašćenih klijenata i brzini odziva sistema.

## 6. ZAKLJUČAK

U ovom radu objašnjen je protokol MQTT prikladan za korišćenje u ograničenim sredinama u mreži Internet stvari. MQTT protokol je prikladan za korišćenje kod međusobne komunikacije više čvorova (engl. *many-to-many*), omogućava prenos poruka među više klijenata putem središnjeg čvora odnosno broker. Iako postoje mehanizmi za trajnost podataka, MQTT najbolje

funkcioniše kao komunikacijska magistrala za podatke. Koristi se protokol TCP za vezu s brokerom. MQTT ne podržava označavanje tipa sadržaja te se poruke mogu koristiti za razne primene, ali klijenti moraju unapred znati tip sadržaja.

Postoje brojni uređaji prikladni za ulogu čvorova u Internet stvarima, a u ovom radu je opisan Arduino uređaj, kao jedan od najpoznatijih i najkorišćenijih uređaja tog tipa. Brojne mogućnosti, jednostavnost korišćenja, brojni dodaci u vidu hardverskih modula i softverskih programskih biblioteka, odlična podrška i niska cena čine Arduino odličnim izborom za korišćenje u Internet stvarima. U skladu s tim, i u sklopu ovog rada, isproban je MQTT protokol sa očitavanjem temperature i prikazivanje vrednosti na korisničkoj Android aplikaciji. Takođe je proverena i mogućnost uključivanja i isključivanja LE diode na Arduino Uno uređaju preko iste te Android aplikacije, i time potvrđena dvostrana komunikacija sa brokerom.

## 7. LITERATURA

- [1] S. Božanić, M. Antonić, "Daljinsko upravljanje i nadzor uređajima preko interneta", Kopaonik, Yu info, March 2017., pp. 242-247
- [2] Dogan Ibrahim: Internet stvari, 2016. godine, Agencija EHO.
- [3] S. Furrer, W. Schott, H. L. Truong, B. Weiss, "The IBM wireless sensor networking testbed", 2nd International Conference on Testbeds & Research Infrastructures for the DEvelopment of NeTworks & COMMunities (TRIDENTCOM'06), Mar. 2006.
- [4] HWANG, Hyun Cheon; PARK, JiSu; SHON, Jin Gon. Design and implementation of a reliable message transmission system based on MQTT protocol in IoT. *Wireless Personal Communications*, 2016, 91.4: 1765-1777.
- [5] S. Božanić, S. Sretenović, "Laboratory Example for Controlling Devices in Smart Homes", Bucharest, CERC, May 2017.
- [6] S. Božanić, D. Mikluc and S. Sretenović, "An example of encrypting communication in smart houses", Obrenovac, ICMNEE, September 2017.
- [7] B. A. Forouzan, S. C. Fegan, "TCP/IP Protocol Suite", Mc Graw Hill book, ISBN 0071115838, 3rd edition, New York, 2006.
- [8] Badamasi, Yusuf Abdullahi. "The working principle of an Arduino." *Electronics, Computer and Computation (ICECCO)*, 2014 11th International Conference on. IEEE, 2014.
- [9] <https://store.arduino.cc/arduino-wifi-shield> posećeno 22. jan.
- [10] <http://cdn.sparkfun.com/datasheets/Sensors/Temp/DS18B20.pdf>
- [11] S. Sretenović, S. Božanić, "Monitoring Air Quality from Location", Bucharest, CERC, May 2017.



# MODELOVANJE PROCESA SAMOVOĐENJA RAKETA U MATLAB-Simulink PROGRAMSKOM OKRUŽENJU MODEL OF HOMING GUIDANCE IN MATLAB-Simulink PROGRAM ENVIRONMENT

Vladimir Kekić<sup>1</sup>, Filip Nikolić<sup>2</sup>, Stefan Božanić<sup>3</sup>, Stefan Sretenović<sup>3</sup>  
250.rbr za PVD, Vojska Srbije<sup>1</sup>  
Vojna akademija, Univerzitet odbrane<sup>2</sup>  
Vojska Srbije<sup>3</sup>

**Sadržaj** – U ovom radu simuliran je proces samovodjenja metodom klasične proporcionalne navigacije (KPN), upoređivanje rezultata linearizovanog modela samovodjenja kod KPN, proširene PN i optimalnog samovodjenja u MATLAB-Simulink® programskom okruženju.

**Abstract** – This paper presents a simulation of homing guidance using method of proportional navigation (PN), comparison of the results of homing guidance liner model for PN, extended PN and optimal homing guidance in MATLAB® software package.

## 1. UVOD

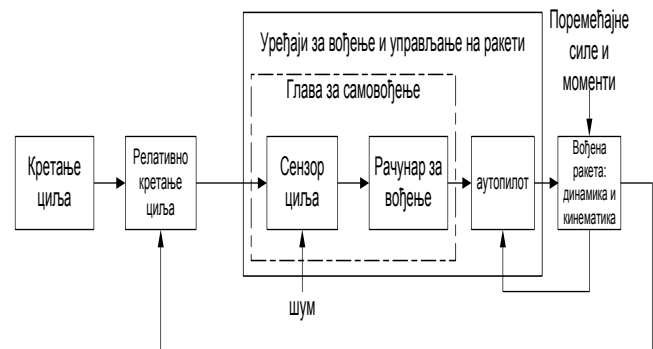
Osnovna podela raketa je na nevođene i vođene. Pojam nevođena raketa podrazumeva da se tokom leta ne vrši prinudna izmena njene trajektorije, tj. raketa nema sistem vođenja i upravljanja (SVU). Vođene rakete poseduju SVU. Postoje dve osnovne grupe metoda vođenja raketa. Jedna je vođenje u tri tačke (komandno ođenje), druga je vođenje u dve tačke (samovodjenje). Vrsta energije koju glava za samovodjenje (GSV) koristi za detekciju i praćenje cilja može biti energija radio talasa, svetlosnih ili infracrvenih zraka, emitovanih ili reflektovanih od cilja. U zavisnosti od prirode energije zračenja samovodjenje, odnosno sistemi samovodjenja mogu biti: radaski, optički, laserski, akustički i dr. Zavisno od mesta *razmeštaja* prirodnog izvora energije zračenja sistemi samovodjenja mogu biti aktivni, pasivni i poluaktivni.

Samovodjenje predstavlja automatsko vođenje rakete na cilj bazirano samo na informaciji o cilju koja se dobija detekcijom energije zračenja koja dolazi od cilja pomoću uređaja na raketi. Opšta blok šema sistema samovodjenja prikazana je na slici 1. Sistem samovodjenja koji realizuje ovaj koncept vođenja kompletno se nalazi na raketi i sastoji se od senzora (koordinatora), uređaja za formiranje signala vođenja (računar za vođenje), autopilota i rakete kao objekta upravljanja. Koordinator i računar za vođenje zajedno čine glavu za samovodjenje (GSV).

Metoda klasične proporcionalne navigacije (KPN) je jedna od najzastupljenijih metoda samovodjenja. Široko je rasprostranjena zbog jednostavnosti implementacije, a do ideje o nastanku KPN došlo se na onovu zakonitosti

kretanja po metodi paralelnog zbliženja, koje dovodi do susreta rakete i cilja.

Osnovni nedostatak KPN su što ona nije optimalna metoda vođenja na manevrišući cilj, jer pri formiranju komande vođenja ne uzima u obzir imformaciju o manevru cilja. Zbog toga se došlo do ideje o proširenju KPN tako što bi se na neki način u komandu vođenja uključio i manevr cilja. To je dovelo do pojave proširene proporcionalne navigacije (PrPN). Međutim, pokazuje se da u prisustvu dinamike sistema upravljanja raketom, ni PrPN ne daje najoptimalnije rezultate. Na osnovu zahteva za minimizacijom manevarskih zahteva rakete tokom leta, došlo se do metode optimalnog samovodjenja (OPN), koje predstavlja najekonomičnije rešenje.



Slika 1 Opšta blok šema sistema samovodjenja

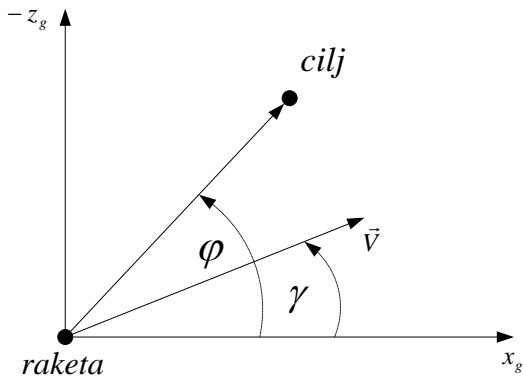
## 2. KLASIČNA PN I REZUTATI SIMULACIJA

U ovom poglavlju bice opisana metoda PN. Radi pojednostavljenja analize kinematike samovodjenja, posmatraće se samo vertikalna ravan. Rešavanje problema u horizontalnoj ravni je analogno problemu u vertikalnoj ravni.

Metoda proporcionalne navigacije (metoda proporcionalnog zbliženja) je metoda vođenja pri kojoj je tokom vođenja rakete ugaona brzina nagiba vektora brzine rakete ( $\dot{\gamma}$ ) proporcionalna ugaonoj brzini LVC ( $\dot{\phi}$ ) (slika 2):

$$\dot{\gamma} = K\dot{\phi}, \quad (1)$$

gde je  $K$  koeficijent proporcionalnosti ili navigaciona konstanta.



Slika 2. Geometrijski odnosi

Ako se izraz (2.6) pomnoži sa  $-V$  dobija se :

$$-V\dot{\gamma} = -VK\dot{\phi} = a_n = a_{zk}, \quad (2)$$

gde je  $V$  brzina rakete. Ubrzanje rakete je normalno na trajektoriju u vertikalnoj ravni pa se  $a_n$  odnosno  $a_{zk}$  naziva normalno komandovano ubrzanje ili opterećenje koje raketa trpi prilikom leta u vertikalnoj ravni [1].

Trenutni promašaj (tekući promašaj) predstavlja najkraće trenutno rastojanje kojim bi raketa proletela pored cilja kada bi se njeno kretanje i kretanje cilja odvijalo bez promena posle odgovarajućeg trenutka posmatranja [1].

Gde je izraz za trenutni promašaj :

$$h = \frac{r^2 \dot{\phi}}{\sqrt{\dot{r}^2 + (r\dot{\phi})^2}}, \quad (3)$$

Model u prostoru stanja kinematike samovodjenja u vertikalnoj ravni dat je vektorom stanja:

$$\mathbf{X} = [r \quad \dot{r} \quad \phi \quad \dot{\phi} \quad \gamma \quad \gamma_c \quad x \quad z \quad x_c \quad z_c]^T \quad [3].$$

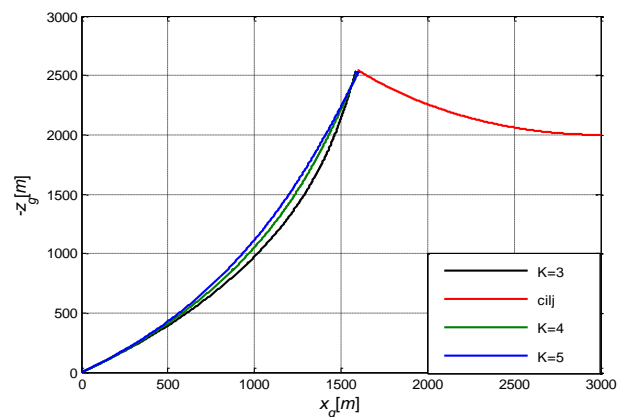
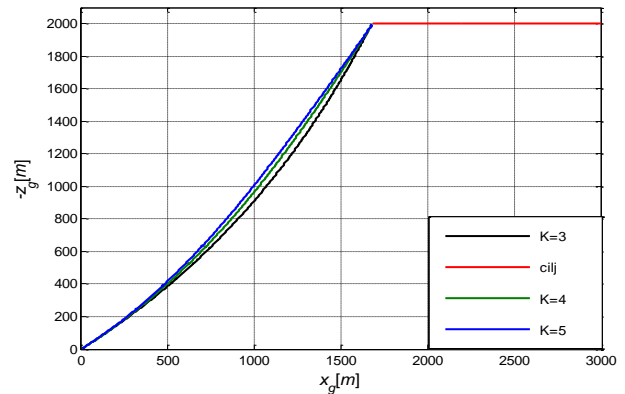
Model u prostoru stanja je veoma bitan jer sa na osnovu njega formira kinematika samovođenja rakete. Vektor stanja je opisan diferencijalnim jednačinama koje su iskorišćene za formiranje simulacije u programu *MATLAB*®.

U daljem tekstu bice opisana analiza tačnosti KPN u zavisnosti od promene navigacione konstante  $K$  za slučajeve kad cilj ne vrši manevar i kad manevariše.

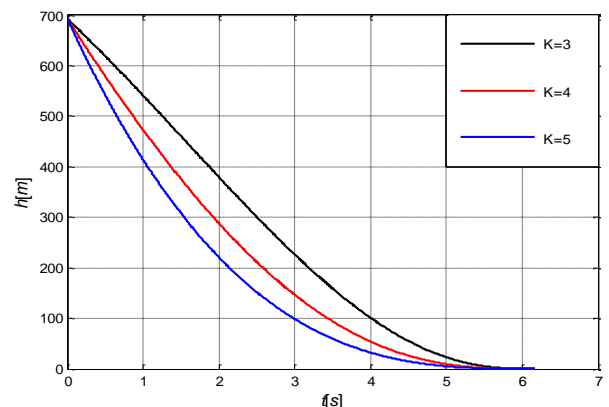
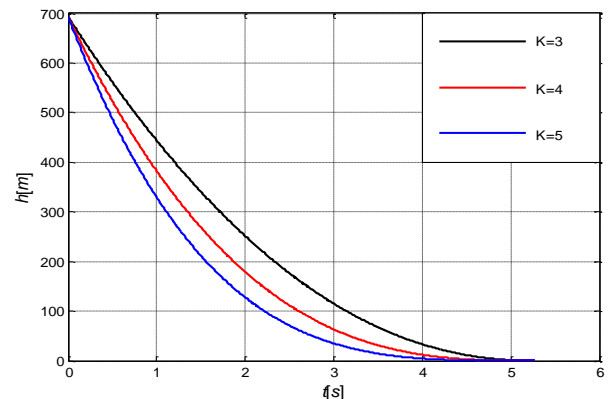
Prvo su analizirane zakrivljenost trajektorije rakete, trenutni promašaj i opterećenje koje raketa trpi tokom leta, u zavisnosti od izbora navigacione konstante  $K$ . Na slici 3 su prikazane trajektorije rakete i cilja, kad cilj ne vrši manevar i kada manevariše, respektivno. Na slici 4 su prikazani trenutni promašaj ,a na slici 5 opterećenje rakete za dati scenario. U oba slučaja se gađa bez preticanja.

Sa slika se vidi da trajektorija rakete postaje zakrivljenija sa porastom navigacione konstante, bez obzira da li cilj manevariše ili ne. Pošto se gađa bez preticanja, trenutni promašaj je u početku maksimalan, i tokom vremena pada na nulu. Uočava se da se sa porastom navigacione konstante, trenutni promašaj brže anulira.

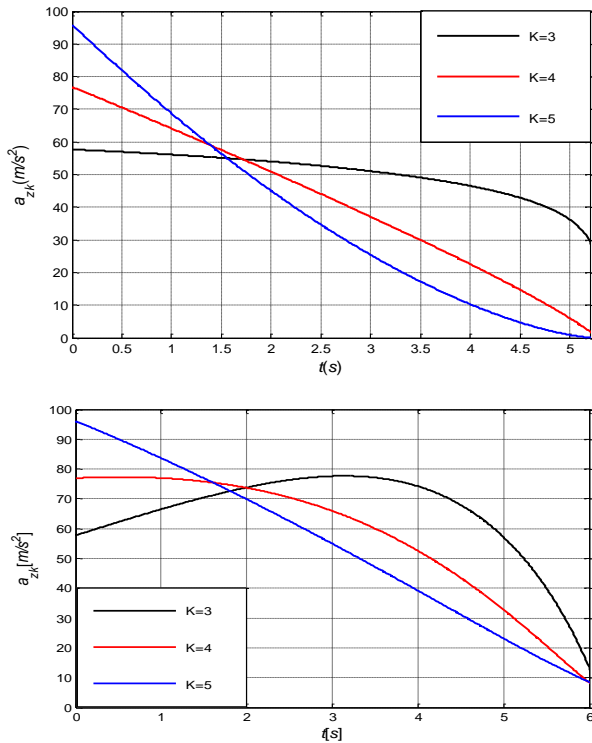
Kao posledica gađanja bez preticanja su i maksimalni manevarski zahtevi za raketu odmah nakon lansiranja, dok se tokom leta oni smanjuju i teže nuli. Izborom veće navigacione konstante, bez obzira da li se gađa nemanevrišući ili manevarišući cilj, povećava se maksimalno zahtevano opterećenje na početku, ali se nakon izvesnog vremena oni značajno smanjuju.



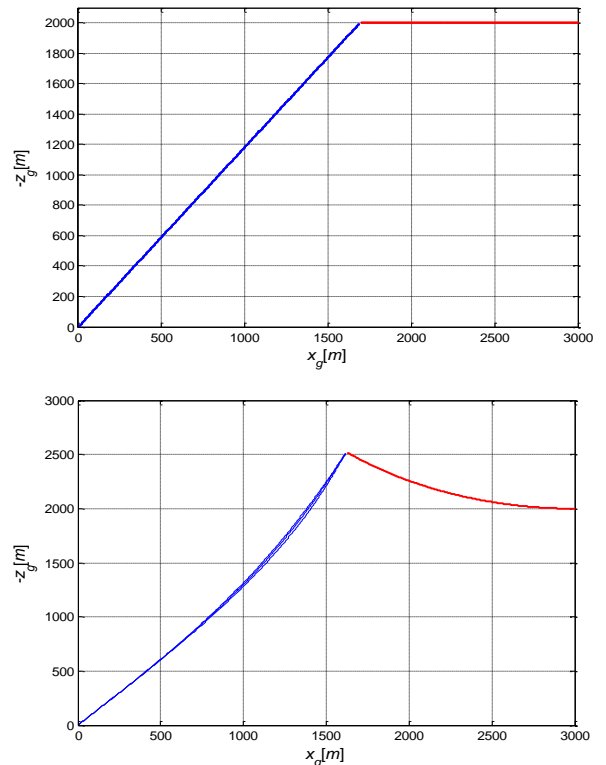
Slika 3. Trajektorije rakete i cilja u zavisnosti od navigacione konstante  $K$  : a) (gore) cilj ne manevariše, b) (dole) cilj manevariše



Slika 4. Trenutni promašaj u zavisnosti od navigacione konstante  $K$  : a) (gore) cilj ne manevariše, b) (dole) cilj manevariše

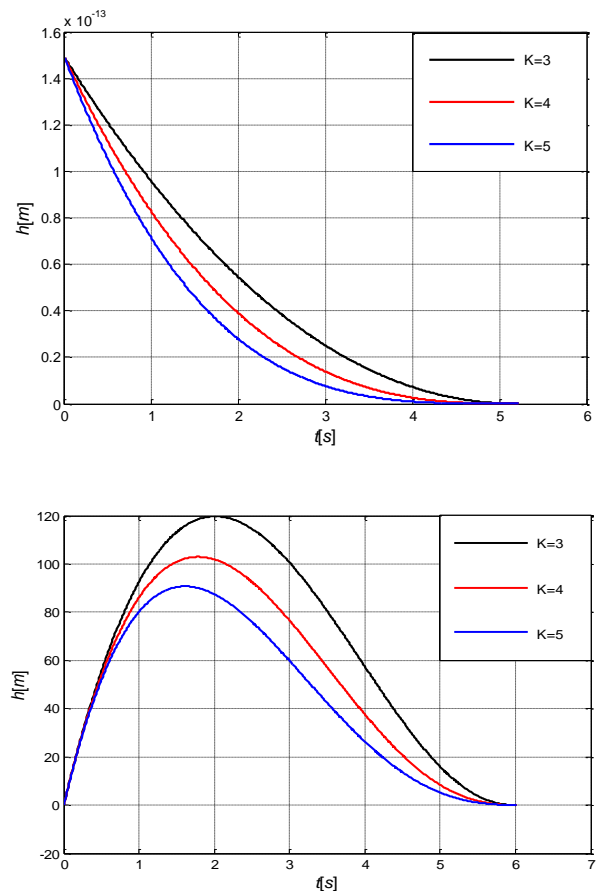


**Slika 5.** Opterećenje rakete u zavisnosti od navigacione konstante  $K$  : a) (gore) cilj ne manevriše, b) (dole) cilj manevriše

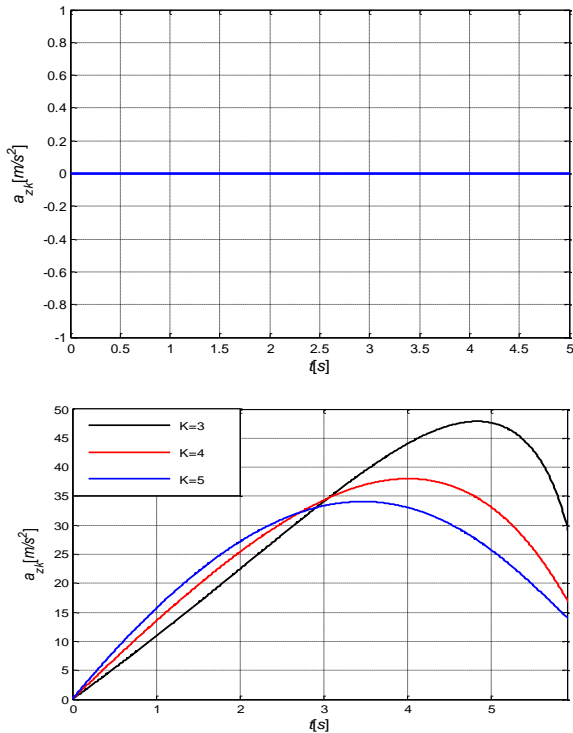


**Slika 6.** Trajektorije rakete i cilja u zavisnosti od navigacione konstante  $K$  : a) (gore) cilj ne manevriše, b) (dole) cilj manevriše

Zatim su analizirane zakrivljenost trajektorije rakete, trenutni promašaj i opterećenje koje raketa trpi tokom leta, u zavisnosti od izbora navigacione konstante  $K$ , ali kada se gađa sa preticanjem. Na slici 6 su prikazane trajektorije rakete i cilja, kada cilj ne vrši manevar i kad manevriše, respektivno. Na slici 7 prikazani trenutni promašaj i na slici 8 opterećenje rakete za dati scenario. Sa slika se vidi da, bez obzira da li cilj manevriše ili ne, promenom vrednosti navigacione konstante ne dolazi do značajne promene u izgledu trajektorije. Razlog za to je gađanje sa preticanjem, ali i to što je u početnom trenutku cilj dosta udaljen od lansera. Pošto se gađa sa preticanjem, trenutni promašaj je praktično jednak nuli pri gađanju cilja koji ne manevriše, što se vidi sa slike 7 a). Kada cilj vrši manevar, uočava se uticaj navigacione konstante (slika 7b)), i to da što je ona veća, vrednosti trenutnog promašaja su manje i promašaj se brže elimiše. Ovi efekti su povezani sa opterećenjem rakete. Na osnovu slike 8 može se zaključiti da ako se gađa nemanevrišući cilj (slika 8a) sa preticanjem, raketa neće trpeti nikakvo opterećenje, što je veoma idealizovana pretpostavka. Ako se gađa manevrišući cilj (slika 8b), porast navigacione konstante dovodi do porasta zahtevanih opterećenja na početku, ali se ti zahtevi tokom leta, nakon izvesnog vremena značajno smanjuju. Takođe, treba primetiti da se smanjenjem navigacione konstante maksimum opterećenja postiže u vremenskom trenutku koji se približava vremenu susreta.



**Slika 7.** Trenutni promašaj u zavisnosti od navigacione konstante  $K$  : a) (gore) cilj ne manevriše, b) (dole) cilj manevriše



**Slika 8.** Oprećenje rakete u zavisnosti od navigacione konstante  $K$ : a) (gore) cilj ne manevisiše, b) (dole) cilj manevisiše

Može se zaključiti da se primenom KPN uspešno pogađaju i nemanevrišući i manevisišući cilj. Pogodak nemanevrišućeg cilja pri gađanju sa preticanjem se ostvaruje pod optimalnim uslovima: trenutni promašaj i opterećenje su sve vreme jednaki nuli. Međutim, kada cilj vrši manevar tokom leta i trenutni promašaj i opterećenje rakete dostižu značajne vrednosti. Pokazano je da izborom navigacione konstante, može uticati na efikasniju eliminaciju trenutnog promašaja, ali je to uvek praćeno zahtevom za većim (u određenim periodima leta) opterećenjem rakete. Prethodni zaključci ukazuju na potrebu za uvođenjem informacije o manevaru cilja u zakon vođenja, što predstavlja proširenu proporcionalnu navigaciju (PrPN).

### 3. PROŠIRENA PN I OPTIMALNO SAMOVOĐENJE

Za razliku od klasične (KPN), proširena proporcionalna navigacija (PrPN) je zakon vođenja koji pri formiranju komandovanog opterećenja rakete uzima u obzir i informaciju o manevaru cilja, i za očekivati je da u odnosu na KPN, u izvesnom smislu daje bolje rezultate. Da bi mogla da se izvede PrPN i optimalno samovođenje mora da se izvrši linearizacija modela kinematike samovođenja [2].

Daljim izvođenjem može se formulisati zakon vođenja :

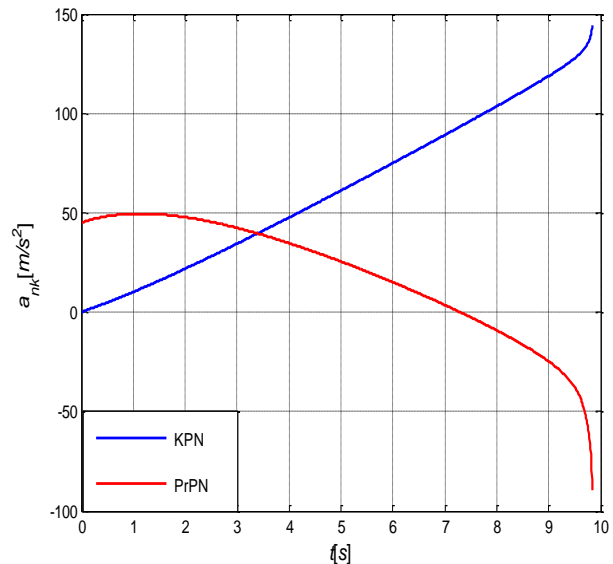
$$a_{nk} = KV_r \dot{\varphi} + \frac{K}{2} a_c, \quad (4)$$

PrPN se zapravo sastoji iz dodatka člana koji je proporcionalan ubrzanju cilja. Efekat ovako formulisano zakon vođenja na zahtevana ubrzanja se uočava iz analitičkog rešenja za slučaj bezinercionog SVU.

Daljim sređivanjem i uvođenjem švarcove nejednakosti [2] dobija se izraz

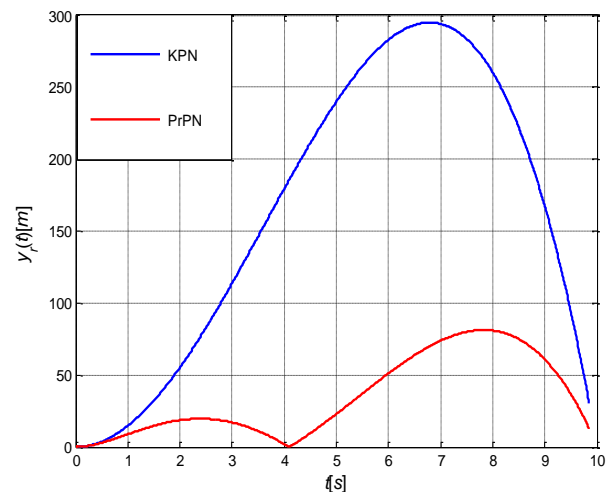
$$a_{nk} = \frac{3(y_r + \dot{y}_r \tau + 0.5a_c \tau^2)}{\tau^2}, \quad (5)$$

U nastavku će se analizirati kakav uticaj na PrPN ima realan SVU koji unosi dinamičko kašnjenje. Dinamika SVU može se aproksimativno predstaviti kao sistem prvog reda sa vremenskom konstantom od 1s. Ubrzanje rakete je 3g, a navigaciona konstanta  $K=3$  (slika 9) .



**Slika 9.** Realizovana ubrzanja u slučajevima KPN i PrPN kada je SVU predstavljen sistemom prvog reda

U slučaju KPN profil zahtevanih ubrzanja ne odstupa od slučaja bezinercionog SVU, osim što u samoj završnici ubrzanje neograničeno raste. Dinamika SVU ima uticaj i na trenutni promašaj. Analizirajući gornji primer primene KPN i PrPN, dobijaju se dijagrami zavisnosti trenutnog promašaja od tekućeg vremena, kao na slici 10. Na osnovu izraza (4) i (5) generisane su slike 9 i 10 pomocu *MATLAB-Simulink* simulacionih dijagrama.



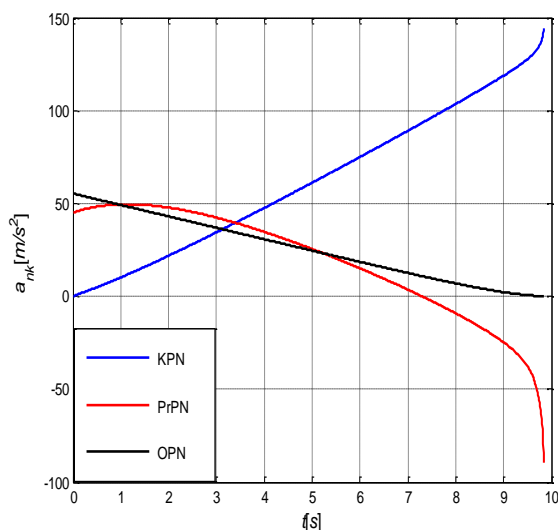
**Slika 11.** Krajnji promašaji u funkciji vremena leta u slučajevima KPN i PrPN kada se SVU predstavi sistemom prvog reda sa vremenskom konstantom od 1s

Minimizacijom manevarskih zahteva uz uslov da krajnji promašaj bude nulti. Daljim izvođenjem dolazi se do optimalnog zakona vođenja u formi [4]:

$$a_{nk} = \frac{K}{\tau^2} [y + \dot{y}\tau + 0.5a_{czr}\tau^2 - T^2a_N(\exp(-x) + x - 1)]. \quad (6)$$

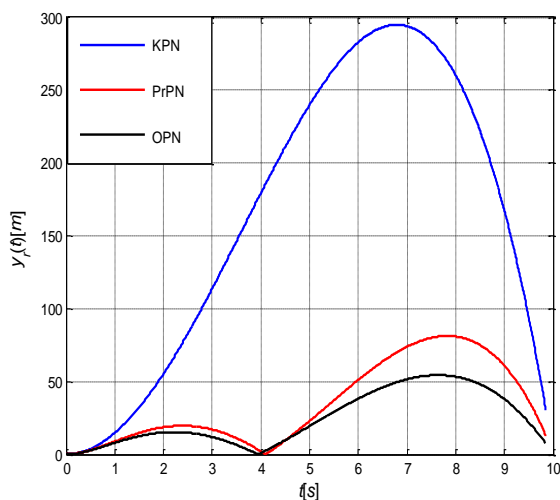
U odnosu na razmatranu modifikaciju PrPN, pojavljuje se dodatni član u (6). On uvodi informaciju o realizovanom ubrzanju vođenog objekta i oslanja se na poznatu dinamiku SVU (vremenska konstanta  $T$ ) i merenje preostalog vremena leta.

Realizovana ubrzanja u slučaju optimalnog samovođenja za prethodni opisani slučaj data su na slici 11, uporedo sa rezultatima dobijenim preko KPN i PrPN.



**Slika 11.** Realizovana ubrzanja u slučajevima KPN i PrPN i optimalnog samovođenja

Poređenja krajnjih promašaja između rezultata dobijenih pomoću KPN, PrPN i optimalnim samovođenjem prikazano je na slici 12 i pokazuje da je najmanji promašaj kod optimalnog samovođenja.



**Slika 12.** Krajnji promašaji u funkciji vremena leta u slučajevima KPN i PrPN i optimalnog samovođenja

Mane optimalnog samovođenja leže u složenosti primene (traži se estimacija cilja, merenje ubrzanja vođenog objekta, rastojanja vođenog objekta i cilja, brzine zblizavanja). Određene pretpostavke mogu da se dovedu u sumnju (dinamika SVU je realno kompleksnija od sistema prvog reda i promenljiva je tokom leta).

#### 4. ZAKLJUČAK

U ovom radu izvršena je analiza tačnosti klasične proporcionalne navigacije u zavisnosti od navigacione konstante  $K$  za slučajeve kada cilj ne manevriše i kada se gađa sa i bez preticanja. Došlo se do zaključka da je klasična proporcionalna navigacija efikasna metoda kada cilj ne manevriše i kad se gađa sa preticanjem. Tada su minimalni manevarski zahtevi. Sa manevrom cilja i kad se gađa bez preticanja zahtevi naglo rastu i tada ova metoda nije dovoljna već joj je potrebno proširenje u vidu informacije o manevru.

Proširena proporcionalna navigacija uzima u obzir manevar cilja. Linearizacijom modela kinematike samovođenja izvršeno je izvođenje proširene proporcionalne navigacije. Dobila su se rešenja u zatvorenoj formi i postizani su manji manevarski zahtevi nego kod klasične proporcionalne navigacije.

Na osnovu rezultata dobijenih simulacijom utvrđeno je da se efikasnost proširene proporcionalne navigacije gubi uvođenjem dinamike sa sistemom prvog reda, pokazalo se da PrPN nije dovoljna i izvršena je optimizacija manevarskih zahteva i na osnovu toga izvedeno je optimalno samovođenje. Upoređujući rezultate linearizovanih modela klasične, proširene i optimalnog samovođenja došlo se do zaključka da optimalna pokazuje najmanji trenutni promašaj i najmanja opterećenja tokom leta.

#### 5. LITERATURA

- [1] S.Deskovski, "Sistemi samovođenja", Visoke vojnotehničke škole KoV JNA, Zagreb, 1991.
- [2] S.Graovac, "Automatsko vođenje objekata u prostoru", Akademska misao, Beograd, 2005.
- [3] S.Deskovski, "Matematički model i simuliranje sistema samonavođenja", Naučno-Tehnički PREGLED, vol.XXXI, br.6, 1981.
- [4] P.Zarchan, "Tactical and Strategic Missile Guidance", Progress in Astronautics and Aeronautics, vol.199, 2002.



# MIKROSEGMENTACIJA U CLOUD-U

## CLOUD MICRO-SEGMENTATION

Vladimir Dobrosavljević<sup>1</sup>, Mladen Veinović<sup>2</sup>, Mladen Trikoš<sup>3</sup>  
*Centar za KISIP, Vojska Srbije - Ministarstvo Odbrane, Beograd<sup>1</sup>*  
*Univerzitet Singidunum, Beograd<sup>2</sup>*  
*Vojna akademija, Univerzitet odbrane, Beograd<sup>3</sup>*

**Sadržaj** – Organizacije imaju za cilj da što efikasnije i što sigurnije koriste IT resurse u cilju povećanja efikasnosti i minimiziranja troškova. Mikrosegmentacija nam predstavlja bezbednosne metode i tehnologiju koja nam nas približava ranije navedenim ciljevima i to u fizičkim, virtuelnim i cloud okruženjima. Metode mikrosegmentacije nam omogućavaju distribuiran bezbednosni model koji omogućava mikrosegmentaciji da bude skalabilna, visoko dostupna, primenljiva i nezavisna. U ovom radu su opisani koncepti i principi mikrosegmentacije, problemi i rizici.

**Abstract** – Organizations tend to use IT resource more efficiently and more secure in order to increase productivity and minimize costs. Micro-segmentation brings us security methods and technology which gets us one step closer to goals and objectives of every successful company has in any kind of environment (physical, virtual and cloud). Micro-segmentation methods allow us to implement security policies on a distributed level, making our security environment into a fully distributed driven one utilizing distributed security model in order to obtain scalability, high availability, ease of application and independence. This paper describes concepts and principles of micro-segmentation, problems and potential risks.

### 1. UVOD

Velike organizacije su veoma lako usvojile tehnologiju virtuelizacije, a sve to u cilju konsolidacije poslovnih procesa i efikasnijeg iskoriscenja resursa. Veliki broj organizacija koriste cloud tehnologije u sklopu konvergirane infrastrukture koje služe za hiper-konsolidaciju poslovnih procesa do nivoa koji im sama virtuelizacija nije mogla obezbediti. Hiper-konsolidacija omogućava organizacijama da veoma lako pristupe transformacijama data centara koje prate velike uštede u resursima i povećavaju samu skalabilnost i agilnost sistema.

### 2. MIKROSEGMENTACIJA

Bezbednost predstavlja veliki izazov za proces hiper-konsolidacije. Kada jedna IT organizacija želi da optimizuje poslovne procese i obim posla dodajući bezbednosnu komponentu, kao u slučaju kada se želi zaštititi produkciono okruženje od uticaja iz testnog okruženja, mora se uzeti u obzir novi pristup bezbednosti u data centru.

Mikrosegmentacija nam daje osnove za implementacije zaštite ovog tipa, omogućavajući nam da primenimo bezbednosne polise na svako individualno okruženje u mreži. Implementirajući bezbednosne mehanizme u okviru samih radnih okruženja, bezbednosne polise postaju specijalizovane za svako okruženje. Na primer, može se kontrolisati komunikacija između radnih okruženja iako se ona nalaze na istom mrežnom opsegu (subnet-u) ili na istom hipervizoru, bez obzira na lokaciju, različite tipove infrastrukture ili različite tipove okruženja. Kao rezultat, dobijamo radna okruženja različitih bezbednosnih nivoa koja dele infrastrukturu, omogućavajući visok nivo konsolidacije i agilnosti.

Mikrosegmentacija omogućava organizacijama da prevaziđu ogroman broj izazova pri formiranju i pri samom radu data centara prateći koncepte:

- 1) transformacije data centara;
- 2) primene bezbednosnih polisa, koje direktno izražavaju poslovne procese;
- 3) kontrole rizika, povezanih sa unutrašnjim širenjem - infiltriranjem;
- 4) bezbednog pristupa za treća lica.

### 3. TRANSFORMACIJA DATA CENTARA

IT organizacije su pod kontinuiranim pritiskom da što efikasnije iskoriste resurse u sopstvenim data centrima. Neefikasno iskorišćenje resursa može biti rezultat preuzimanja neke već postojeće infrastrukture, migracija zastarelih (*legacy*) aplikacija ili nedovoljnih resursa u svakom individualnom radnom okruženju. Krajnji rezultat projekata transformacije data centara bi trebao biti visok nivo konsolidacije infrastrukture koji se ogleda u efikasnijem iskorišćenju resursa, ali samo u slučaju kada su i bezbednosni zahtevi uzeti u obzir. Mikrosegmentacija nam pomaže u rešavanju ovih problema izdvajajući mrežnu topologiju od bezbednosnih polisa, što za posledicu ima mogućnost da više okruženja različitih nivoa bezbednosti koristi istu infrastrukturu. Mogućnost kreiranja bezbednosnih polisa za svako radno okruženje nam omogućava granularnu zaštitu IT servisa, održavajući visoku dostupnost i primenu bezbednosnih polisa čak i kada je data centar u fazi promena.

Zastareli (*legacy*) parametarski bezbednosni pristup nije u mogućnosti da primeni principe mikrosegmentacije jer su prilikom kreiranja bezbednosnih polisa uzeti u obzir drugi zahtevi – konkretno, kreirati bezbednosnu polisu između spoljašnjeg i unutrašnjeg sveta (najčešće Interneta i lokalne mreže). Ovaj pristup se oslanja na lokaciju mreža

kroz kreiranje bezbednosih zona kao osnove svih bezbednosnih polisa. Granice između zona, je veoma teško, a ponekad čak i nemoguće definisati u privatnom ili javnom *cloud*-u, jer tehnologije kao što je migracija virtuelnih mašina, određuju radna okruženja kao dinamička. Lokacija radnog okruženja se nikada ne može tačno odrediti, što direktno predstavlja izazov tradicionalnih bezbednosnih zona. Kreiranjem više mikroparametara u okviru svakog radnog okruženja, mikrosegmentacija rešava problem mobilnosti radnog okruženja. U mikrosegmentiranom okruženju, pri kreiranju bezbednosnih polisa, poželjno je voditi se bezbednosnim rizicima ili modelima radnih okruženja.

#### 4. PRIMENA BEZBEDNOSNIH POLISA

U fleksibilnim privatnim *cloud* arhitekturama, dinamičko radno okruženje i mobilnost zahtevaju konstantno unapređivanje u pogledu tradicionalnih bezbednosnih polisa baziranih na IP adresama i portovima. Međutim, kada polisa može da analizira konekstualne meta-podatke iz spoljašnjih izvora, administratori su u mogućnosti da identifikuju i zaštite radno okruženje mehanizmima efikasnijim od polisa baziranih na filteru aplikacija. Polise mogu biti definisane na osnovu meta-podataka koji se kreiraju iz poslovnih procesa visokog nivoa ili samih potreba radnog okruženja – pri razvoju aplikacija (u svim fazama životnog ciklusa), pri proveru usaglašenosti, kritičnosti...

Integrirana sa *cloud* sistemom za upravljanje, mikrosegmentacija nam omogućava široke mogućnosti da razdvojimo radna okruženja bazirana na atributima koji upravljaju radnim okruženjem, a ne samo mrežnim adresama koje se koriste u radnom okruženju. Koristeći prirodu meta-podataka da se lako integrišu u svaki sistem za upravljanje *cloud*-om, bezbednosne polise mogu imati veoma mala preklapanja što znatno olakšava posao administratora. Na primer, radno okruženje u kojem su sve operacije označene sa „TEST“ neće moći da komunicira sa radnim okruženjem gde su operacije označene sa „PROD“. Ovaj način eliminiše potrebu za ručnim menjanjem polisa svaki put kada se izvrši neka promena na sistemu, što se direktno odražava na jednostavnost i smanjuje kompleksnost operacija u data centru.

#### 4. KONTROLA RIZIKA

Napadi hakera, sajber kriminalaca ili bilo kojih drugih zlonamernih korisnika često otpočinju kompromitovanjem nekog manje važnog radnog okruženja, i onda se vrši napad na kritična radna okruženja. Na primer, portal javnih nabavki je kompromitovan od strane hakera i iskorišćen je za pristup resursima data centra. Ova faza napada se povezuje sa „unutrašnjim širenjem“ - infiltriranjem.

Mikrosegmentacija može pomoći pri kontroli i izolovanju infiltriranih radnih okruženja da bi se usporio ili onemogućio napadač i time sprečio dalje kompromitovanje data centra. Kreiranjem interne

segmentacije u cilju ograničavanja prava pristupa internim sistemima samo na ona lica kojima je odobren pristup, mikrosegmentacija omogućava administratorima da na efektan način ograniče ili smanje izloženost na pretnje.

#### 5. BEZBEDAN PRISTUP ZA TREĆA LICA

Mikrosegmentacija se može efikasno upotrebiti da bi se kontrolisao pristup internim resursima od strane trećih lica, kao što su na primer poslovni partneri. Neki dobavljači usluga često zahtevaju pristup radnim okruženjima ili unutrašnjoj lokalnoj mreži da bi odradili svoj deo posla. Ovo bi često značilo da se dobavljačima daje pristup delovima data centra koristeći VPN ili neku drugu vrstu udaljenog pristupa. Upravljanje bezbednošću koristeći ove tehnologije je veoma zahtevno i sklono je greškama.

Mikrosegmentacija omogućava organizacijama da kreiraju bezbednosne polise koje omogućavaju poslovnim partnerima da izvrše svoje zadatke, dok se sa druge strane verovatnoća kompromitovanja radnog okruženja umanjuje. Na primer, moguće je kreirati bezbednosnu polisu koja omogućava pristup samo onim resursima koji su potrebni poslovnim partnerima i/ili dobavljačima da obave svoj deo posla.

#### 5. PRINCIPI MIKROSEGMENTACIJE

Mikrosegmentacija omogućava IT kompanijama da ostvare visoke nivoe efikasnosti data centara istovremeno smanjujući rizike za pojavom bezbednosnih incidenata. Mikrosegmentacija se oslanja na četiri ključna principa:

- 1) Proširivost. Održavanje visokog nivoa bezbednosti je automatizovano i vođeno kroz *API*-eve koji se lako prilagođavaju arhitekturi data centra;
- 2) Skalabilnost. Bezbednosne polise se mogu primeniti na sva radna okruženja, povećavajući elastičnost pri odgovoru na napade;
- 3) Nezavisnost. Bezbednosne polise štite svako radno okruženje, nezavisno od infrastrukture na kojoj se nalazi i bez potreba za bilo kakvim dodatnim softverima ili resursima;
- 4) Reaktivnost. Tehnologija mikrosegmentacije obezbeđuje sigurnu primenu bezbednosnih polisa, detektovanje napadača i reagovanje na napade.

#### 6. PRIMENA, PROBLEMI, RIZICI

Na slici 1. dat je primer primene tehnologije mikrosegmentacije. IT organizacija poseduje sopstveni data centar u okviru kog postoji više radnih okruženja. Radna okruženja predstavljaju korporativna radna okruženja za IT odeljenje, finansijsko odeljenje i odeljenje za ljudske resurse. Isto tako poslovni partneri i dobavljači usluga koriste resurse sistema. Sva okruženja su fizički spojena na jednu lokalnu mrežu. Svako okruženje ima sopstvenu meta oznaku, IT, FIN, HR, respektivno. Svaka operacija u lokalnoj mreži je označena meta oznakom. Tako svi korisnici mogu da pristupaju zajedničkim korporativnim servisima kao što su na

primer: servis elektronske pošte (*email*) i servis za razmenu kratkih poruka između zaposlenih (*chat*), dok servisima finansijskog sektora mogu pristupati samo korisnici sistema čiji zahtevi sadrže meta informaciju FIN. Isto tako podacima o ljudskim resursima mogu pristupati samo korisnici sistema čiji zahtevi sadrže meta informaciju HR.



Slika 1. Primer mikrosegmentacije

Sve ovo održavaju lica iz IT odeljenja preko centralne konzole (*Central Orchestrator*).

Najčešći problemi se sreću pri samom procesu usvajanja i implementacije tehnologije mikrosegmentacije. Da bi se bezbednosne polise uspešno implementirale potrebno je detaljno poznavanje mrežnog saobraćaja i komunikacionih obrazaca ka data centru i iz data centra. Ovo često zahteva korišćenje analitičkih alata koji mogu da prepoznaju obrasce mrežnog saobraćaja i naprave korelaciju između njih. Analitička analiza saobraćaja mora da identifikuje veze između aplikacija kao i potencijalna ranjiva mesta u mreži, i označi nisko efikasne komponente mreže. Nije svaka aplikacija pogodna za implementiranje mikrosegmentiranih bezbednosnih polisa. Mora se izvršiti procena radnih okruženja bi se omogućila kontrolisana interakcija istih.

Bezbednosna pravila se implementiraju sa nultom tolerancijom. Ovo često dovodi do prekida u funkcionisanju servisa u svim radnim okruženjima jer nije moguće precizno i tačno implementirati sve bezbednosne polise bez dodatne analize nakon implementacije polise sa nultom tolerancijom.

## 5. ZAKLJUČAK

Mikrosegmentacija nam donosi nove bezbednosne izazove sa kojima se moramo suočavati. Virtuelne komponente i virtuelno okruženje ne može biti zaštićeno postojećim bezbednosnim mehanizmima i bezbednosnim procedurama.

Mikrosegmentacija nam omogućava dodatan nivo zaštite ali ne može u potpunosti zameniti tradicionalne bezbednosne metode i polise. Dodatan nivo bezbednosti nam pomaže da smanjimo marginu napada kako iz spoljnog sveta tako i iz lokalne mreže. Pravovremena instalacija zakrpa, bezbedna administracija, izmena fabrički podešenih vrednosti na resursima sistema je samo početak rada na povećanju bezbednosti. Model nulte tolerancije nam ovo prikazuje kao prvi od zahteva pre implementacije nezavisno od lokacije resursa, bilo da se nalaze u lokalnoj mreži ili *cloud-u*.

Mikrosegmentacija ne sme biti ideja koja se javlja nakon implementacije virtuelne infrastrukture i svih njenih komponenti.

Bezbednosni aspekti na polju virtu elizacije će se poboljšavati kako i sama tehnologija virtuelizacije napreduje i kao sledeći korak očekuje se uvođenje standarda koji se moraju ispoštovati da bi se obezbedilo svako novo virtuelno okruženje.

## 6. LITERATURA

- [1] Dave Shackleford, "Is cloud micro-segmentation secure enough for enterprise use?", <http://searchcloudsecurity.techtarget.com/tip/Is-cloud-microsegmentation-secure-enough-for-enterprise-use>
- [2] Alan S. Cohen, „The Truth About Micro-segmentation”, <https://www.illumio.com/resource-center/white-paper-the-truth-about-micro-segmentation>
- [3] Data Center Micro-Segmentation, <https://www.ntpro.nl/blog/archives/2960-Whitepaper-Data-Center-Micro-Segmentation.html>
- [4] The Business Case for Network Segmentation, <https://assets.extrahop.com/whitepapers/ExtraHop-Modern-Network-Segmentation.pdf>
- [5] Leveraging micro-segmentation to build a zero trust network, [https://www.cio.com.au/campaign/370920?content=%2Fwhitepaper%2F372932%2Fleveraging-micro-segmentation-to-build-a-zero-trust-network%2F%3Ftype%3Dother%26arg%3D0%26location%3Dfeatured\\_list](https://www.cio.com.au/campaign/370920?content=%2Fwhitepaper%2F372932%2Fleveraging-micro-segmentation-to-build-a-zero-trust-network%2F%3Ftype%3Dother%26arg%3D0%26location%3Dfeatured_list)

# SISTEM IDENTIFIKACIJE SLEDEĆE GENERACIJE NEXT GENERATION IDENTIFICATION SYSTEM

Mladen Trikoš<sup>1</sup>, Vladimir Dobrosavljević<sup>2</sup>, Dejan Simić<sup>3</sup>, Dejan Savić<sup>4</sup>

*Vojna akademija – Univerzitet odbrane u Beogradu<sup>1</sup>*

*Centar za KISIP, Vojska Srbije - Ministarstvo Odbrane, Beograd<sup>2</sup>*

*Fakultet organizacionih nauka – Univerzitet u Beogradu<sup>3</sup>*

*Ministarstvo odbrane Republike Srbije<sup>4</sup>*

**Sadržaj** – Biometrijski sistemi koji se baziraju samo na jednom biometrijskom podatku-identifikatoru u praksi obično ne daju željene rezultate u smislu performansi takvih sistema. Biometrijska identifikacija bazirana na više biometrijskih podataka-identifikatora postaje sve više prisutnija u istraživačkim oblastima a i u praksi. U ovom radu prikazan je najsavremeniji biometrijski sistem identifikacije razvijen od strane Federalnog zavoda za istrage (FBI) u cilju očuvanja nacionalne bezbednosti.

**Abstract** - Biometric systems that are based on only one biometric data-identifier in practice usually do not give the desired results in terms of the performance of such systems. Biometric identification based on multiple biometric data-identifiers is becoming more and more present in research areas and in practice. This paper presents the most advanced biometric identification system developed by the Federal Bureau of Investigation (FBI) in order to preserve national security.

## 1. UVOD

Povećanjem računarskih zloupotreba kao što je hakovanje računarskih sistema, ilegalni pristup bankomatima i mobilnim uređajima i kršenjem bezbednosti u vladinim institucijama i privatnim subjektima, povećava se i potreba za sigurnosnim sistemima i sigurnosnim mehanizmima. Napadači na informaciono-komunikacione sisteme (IKS) koriste fundamentalne nedostatke konvencionalnih sistema zaštite. Rešenje za prevazilaženje takvih sigurnosnih problema sistema prilikom lične identifikacije korisnika jeste biometrijsko prepoznavanje korisnika.

Biometrijska identifikacija znatno otežava napadačima da neovlašćeno pristupe podacima u sistemu nego što bi to uradili putem lozinki, brojem lične karte, jedinstvenim matičnim brojem građana, pametnim karticama itd. Multimodalni biometrijski sistemi mogu kombinovati bilo koji broj nezavisnih biometrijskih podataka i tako prevazići neka od ograničenja sistema koji koriste samo jedan biometrijski podatak za identifikaciju korisnika.

Spajanje više biometrijskih podataka smanjuje stepen sistemske greške prilikom identifikacije korisnika. Metod fuzije biometrijskih podataka uključuje sekvencijalnu obradu biometrijskih modaliteta dok se ne dobije prihvatljivo podudaranje kod identifikacije korisnika.

Ovaj rad predstavlja pregled multimodalnih biometrijskih sistema, sa posebnim osvrtom na sistem za identifikaciju

sledeće generacije, razvijen od Federalnog zavoda za istrage (FBI).

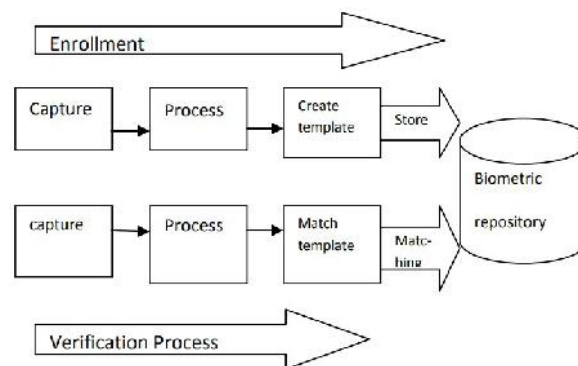
## 2. BIOEMTRIJSKI SISTEMI

Biometrija, koja se odnosi na automatsku identifikaciju osobe na osnovu njenih psiholoških ili bihevioloških karakteristika, oslanja se na “nešto što ona jeste ili što ona radi” (npr. stavljanje prsta na skener) da bi se identifikovala [1]. Biometrija je inherentno pouzdanija i ima veću sposobnost diskriminacije pri identifikaciji korisnika za razliku od pristupa zasnovanog na tokenu ili na osnovu znanja, jer su psihološke ili biheviološke karakteristike jedinstvene za svakog pojedinca [2].

Biometrija je nauka i tehnologija merenja i analiza bioloških podataka ljudskog tela, ekstrakcije skupa karakteristika iz dobijenih podataka i upoređivanja ovog skupa sa snimljenim biometrijskim šablonima u bazi podataka, a ovi sistemi se nazivaju Biometrijski sistemi [3]. Ovi sistemi mogu raditi u sledećim režimima:

**1. Upisni mod** - sistem prepoznaje pojedinca, upisuje njegov biometrijski šablon u bazu podataka korisnika,

**2. Režim verifikacije** - sistem potvrđuje identitet osobe tako što upoređuje uzete biometrijske podatke sa sopstvenim biometrijskim šablonima koji se čuvaju u baza podataka korisnika (slika 1).



Slika 1. Biometrijski sistemi [3]

Biometrijski sistemi se sastoje od četiri modula:

- *Senzor* – snima biometrijske podatke pojedinca,
- *Izdvajanje* – u ovom modulu se biometrijski podaci obrađuju, tj. iz njih se izvlače određene karakteristike,
- *Upoređivanje* – u ovom modulu vrši se upoređivanje uzetih biometrijskih podataka sa snimljenim podacima u bazi,

- *Baza podataka* – ovde se čuvaju biometrijski podaci korisnika.

Kao sredstvo za upravljanje identitetima ovi biometrijski sistemi su implementirani u različite komercijalne, civilne i vojne aplikacije. Međutim, zbog povećanja performansi i pouzdanosti sistema identifikacije, pristupa se razvijanju i korišćenju novih biometrijskih sistema – multimodalnih biometrijskih sistema.

### 3. MULTIMODALNI BIOMETRIJSKI SISTEMI

Unimodalni biometrijski sistemi imaju određene nedostatke, kao što su “noisy sensor data” – osetljivost podataka na šumove senzora, neuniverzalnost biometrijskih osobina, ograničen stepen slobode i neprihvatljive stope greške. Multimodalni biometrijski sistemi pokušavaju da prevaziđu navedene nedostatke pružanjem više dokaza o istom identitetu-korisniku.

Multimodalni sistemi mogu da kombinuju bilo koji broj nezavisnih biometrijskih podataka (slika 2). Multimodalni biometrijski sistemi su znatno otporniji na napade lažnog predstavljanja u sistemima identifikacije. Mnogo je teže lažirati više biometrijskih podataka nego jedan biometrijski podatak. Time se obezbeđuje veća tačnost pri identifikaciji korisnika, a samim tim i jača zaštita od prevara.



Slika 2. Multimodalni biometrijski sistemi [4]

Biometrijski podaci iz dva ili više biometrijskih uzoraka mogu se kombinovati koristeći moguća četiri nivoa spajanja:

- *Spajanje na nivou senzora* - biometrijske osobine koje se uzimaju od različitih senzora se kombinuju u obliku kompozitne biometrijske osobine i dalje obrađuju,
- *Spajanje na nivou izdvajanja* – prvo se unapred obrađuju različite biometrijske karakteristike, zasebno se vektorski ekstrahuju koristeći specifične algoritme i na kraju se kombinuju da

bi se formirao kompozitni vektor biometrijskih karakteristika.

- *Spajanje na nivou upoređivanja* – za razliku od prethodnog nivoa, ovde se pojedinačno obrađuju i upoređuju biometrijske karakteristike različitih biometrijskih podataka, a zatim se u zavisnosti od tačnosti svakog biometrijskog rezultata oni spajaju pa se radi upoređivanje.
- *Spajanje na nivou odluke* – svaki modalitet se prvo preklasifikuje nezavisno.

Radi poboljšanja performansi sistema, multimodalni biometrijski sistemi mogu implementirati bilo koju od navedenih strategija spajanja ili da kombinuju više strategija.

### 4. NGI SISTEMI

Termin “biometrija” danas nije više ograničen samo na otiske prstiju. On takođe podrazumeva i druge biometrijske podatke, otisak šake, zenicu oka, lice, hod.

U naporu da se iskoriste nove tehnologije i da se poboljša primena desetogodišnjeg pretraživanja otisaka prstiju, Odsek za krivično pravosudne informacije FBI-a (CJIS) razvio je i postepeno integrisao novi sistem koji bi zamenio Integrisani automatizovani sistem za identifikaciju otisaka prstiju (IAFIS). Ovaj novi sistem, Identifikacija nove generacije (Next Generation Identification - NGI), pruža zajednici krivične pravde mogućnost korišćenja svetske najveće i najefikasnije elektronske baze biometrijskih podataka i informacija o kriminalnoj istoriji pojedinaca [5].

NGI sistemi zasnivaju se na multimodalnoj biometrijskoj platformi koja se razvija zahvaljujući novim tehnologijama i korisničkim zahtevima. Ovaj sistem je poboljšao efikasnost i tačnost biometrijskih usluga u cilju rešavanja lokalnih, državnih, federalnih, nacionalnih i međunarodnih zahteva krivičnog pravosuđa.

Mogućnosti NGI sistema:

- Implementacijom novog algoritma upoređivanja otisaka pristuju poboljšana je preciznost prepoznavanja otiska sa 92 procenata na 99,6 procenata. Osim toga, ubrzano je vreme odziva, smanjene su odbijene transakcije i povećana je učestalost identifikacije.
- Brža usluga pretrage baze korisnika dostupna je službenicima policije na terenu i agencijama, pomoću mobilnog uređaja za otisak prsta (slika 3).
- Upotreba otiska šake za identifikaciju korisnika, pored već postojećih otisaka prstiju povećava preciznost identifikovanja lica.
- *Rap Back* servis omogućava autorizovanim agencijama da primaju obaveštenja o aktivnostima pojedinaca koji su na položajima od poverenja (npr. nastavnici u školama, radnici u zdravstvu, sudstvu).



- Pristup međudržavnom sistemu fotografija lica sa otiscima svih deset pristiju. Prilikom ulaska u USA svi posetioci su dužni da ostave svoje biometrijske podatke.
- Mogućnost pretrage na osnovu prepoznavanja lica.
- Mogućnosti nadogradnje sistema prepoznavanjem zenice oka (irisa).



Slika 3. NGI sistem - mobilni uređaja za otisak prsta [5]

NGI sistem je modularan sistem (omogućava jednostavnu proširivost). Ovaj sistem identifikacije ima naprednije mogućnosti za pretraživanje, uključujući otisak dlana, irisa i identifikaciju lica. FBI je prvi put koristio ovaj sistem u februaru 2011. godine i dalje se neprestano razvija, a baza biometrijskih podataka raste (300.000 otisaka dnevno).

## 5. ZAKLJUČAK

Tokom poslednje decenije, u industriji a i u akademskim institucijama bilo je puno radova na temu razvoja novih sistema za identifikaciju korisnika, odnosno za kontrolu pristupa zaštićenim resursima. Interes u ovoj oblasti i dalje ostaje visok, zato što predstavlja problematično istraživačko područje i zbog obilja praktičnih aplikacija koje olakšavaju korisnicima pristup neophodnim zaštićenim sadržajima i uslugama (e-banking, e-health, m-health itd.).

Biometrija pruža povećane bezbednosti širokom spektru korisnika, od IT vendora do krajnjih korisnika IT uređaja, od programera samih sigurnosnih sistema do korisnika takvih sistema. Okruženja visokog nivoa bezbednosti pristupa kao što su vojska, policija, bezbednosne agencije, nuklearne elektrane već decenijama koriste biometrijsku

tehnologiju za identifikaciju korisnika. Danas, primarna upotreba biometrije je u fizičkoj kontroli pristupa zaštićenim resursima (sobe, zgrade, elektrane itd.).

Ovaj rad predstavlja pregled multimodalne biometrije, i prikaz praktične primene multimodalnih biometrijskih sistema u svakodnevnom ljudskom okruženju.

Još uvek je potrebno dosta istraživačkog rada i eksperimentalne analize u ovoj oblasti. U bliskoj budućnosti može se primeniti kombinacija više od dva biometrijska podatka kako bi se poboljšala bezbednost postojećih sistema identifikacije, odnosno, zahvaljujući razvoju tehnologije može se preći sa standardnih sistema identifikacije na multimodalne biometrijske sisteme ili na sistem identifikacije sledeće generacije.

## NAPOMENA (ZAHVALNICA)

Rad je nastao kao rezultat rada na istraživačkom projektu Upravljanje pristupom zaštićenim resursima računarskih mreža u Ministarstvu odbrane i Vojsci Srbije na osnovu multimodalne identifikacije korisnika, pod brojem VA-TT/3/18-20, od 2018. do 2020. godine na Vojnoj akademiji Univerziteta odbrane u Beogradu.

## LITERATURA

- [1] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, Boston, 1999.
- [2] A. Jain, L. Hong, Y. Kulkarni, "A Multimodal Biometric System Using Fingerprint, Face, and Speech", *Second International Conference on AVBPA*, Washington D.C., USA, pp 182–187, 1999.
- [3] T. Panchal and A. Singh, "Multimodal Biometric System", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, pp 1360–1363, 2013.
- [4] <http://www.umiacs.umd.edu/~sshekh/projects.html>
- [5] <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>
- [6] <https://www.fbi.gov/file-repository/repository-for-individuals-of-special-concern-brochure.pdf/view>

# FLEKSIBILNOST: KLJUČNI FAKTOR UPOTREBLJIVOSTI WEB APLIKACIJA

## FLEXIBILITY: KEY USABILITY FACTOR OF WEB APPLICATIONS

Nebojša D. Đorđević<sup>1</sup>, Dejan D. Rančić<sup>2</sup>, Olivera R. Pronić-Rančić<sup>2</sup> i Uwe Siart<sup>2</sup>

*Vojska Srbije, Komanda Kopnene Vojske, Niš, Srbija<sup>1</sup>*

*Elektronski fakultet, Univerzitet u Nišu, Srbija<sup>2</sup>*

*Fakultet za elektroniku i računarstvo, Univerzitet u Minhenu, Nemačka<sup>3</sup>*

**Sadržaj** – *Fleksibilnost može da poveća kvalitet softvera i njegovu sposobnost da zadovolji korisnike i njihove potrebe. Fleksibilnost kao karakteristika upotrebljivosti definisana je od strane mnogih autora i nekoliko ISO standarda. Razvijeno je mnogo različitih metoda procene fleksibilnosti. Upotrebljivost proizvoda je pod uticajem ne samo karakteristika samog proizvoda, nego i karakteristika korisnika, zadataka koje oni obavljaju, kao i tehničkog, organizacionog i fizičkog okruženja u kojem se koristi proizvod. Međutim, pre nego što počne bilo koja aktivnost dizajna ili evaluacije upotrebljivosti, potrebno je razumeti kontekst upotrebe proizvoda, odnosno ciljeve korisnika, glavne korisnike, zadatke i karakteristike sredine u kojoj će se koristiti. U radu su date smernice i podrška za rešavanje važnih pitanja na kojima se zasniva procena fleksibilnosti.*

**Abstract** - *Flexibility can increase software usability and its capability to satisfy users and their needs. Flexibility as a usability characteristics is defined by many authors and several ISO standards. Many various methods of flexibility evaluation have been developed. The usability of a product is affected not only by the features of the product itself, but also by the characteristics of the users, the tasks they carry out, and the technical, organisational and physical environment in which the product is used. However, before any usability design or evaluation activity can begin, it is necessary to understand the Context of use for the product, i.e. the goals of the user community, and the main user, task and environmental characteristics of the situation in which it will be operated. This paper presents a suitable method for identify key usability factors of Web applications.*

### UVOD

Uporedo sa rastom popularnosti Web aplikacija rasla je pažnja koja se poklanja vrednovanju upotrebljivosti u svim fazama životnog ciklusa. Upotrebljivost se smatra važnim atributom za prihvatanje sistema od strane krajnjih korisnika.

Kvalitet u upotrebi se smatra ključnim faktor kvaliteta proizvoda koji ima presudnu ulogu za prihvatanje Web aplikacije i koji će odrediti njihov uspeh odnosno dalju sudbinu. Kada se radi o Web aplikacijama, analiza nameravanog konteksta upotrebe ukazuje da mogu biti korišćene od strane velikog broja korisnika sa različitim sklonostima ili kulturama, ili čak različitim nivoima invaliditeta.

Iako se intuitivno zna šta je to upotrebljivost, nije lako formalno definisati skup karakteristika koje doprinose

dobroj upotrebljivosti. Priroda karakteristika i potrebni atributi zavise od konteksta u kome se proizvod koristi [1]. Mnogi atributi mogu potencijalno doprineti kvalitetu Web aplikacije ali njihov relativni značaj varira i zavisi od cilja i obima, tipa aplikacije i domena primene i korisničkog stanovišta.

Kvalitet u upotrebi, može da se meri kao ishod interakcije kroz efektivnost, efikasnost i zadovoljstvo, pri čemu efektivnost predstavlja meru dostizanja ciljeva, efikasnostje mera za utrošene resurse (vreme, novac ili mentalni napor) da se postignu željeni ciljevi i zadovoljstvo predstavlja meru korisničkog celokupnog prihvatanja. Međutim, ukupan sistem se sastoji od korisnika, zadataka, opreme (hardver, softver i materijal) i fizičkog i organizacionog okruženja koje utiče na interakciju. Zbog toga kvalitet u upotrebi celokupnog sistema obuhvata sve faktore koji mogu da utiču na korišćenje proizvoda u stvarnom svetu, uključujući faktore okruženja, izgled proizvoda i individualne razlike između korisnika (kulturene razlike ili predrasude). Tako širok pristup ima prednost jer se koncentriše na projektovanje proizvoda realnih potreba, koji će biti upotrebljiv od stvarnih korisnika koji obavljaju realne poslove u realnom tehničkom, fizičkom i organizacionom okruženju. Izbor odgovarajućih vrsta korisnika, zadataka i sredine zavisi od ciljeva evaluacije i u kom kontekstu se očekuje da se proizvod koristi. Za raznovrsne primene proizvoda može biti potrebno da se upotrebljivost meri u nekoliko različitih konteksta u kojima zadaci mogu biti izvršavani.

### METOD

Tokom nekoliko decenija, u različitim literaturama su opisane različite definicije i atributi upotrebljivosti. Mnogi istraživači su identifikovali različite dimenzije upotrebljivosti na osnovu definicija upotrebljivosti na polju interakcije čoveka i računara.

Uzimajući u obzir ovu činjenicu, Dubey i dr. u svojoj studiji [2] daju retrospektivu formalnih definicija upotrebljivosti i njihovih atributa sa namerom da pokažu kako se pogled istraživača na upotrebljivosti promenio tokom više od tri decenije.

Uporednom analizom sadržaja formalnih definicija i ključnih atributa upotrebljivosti u modelima upotrebljivosti predloženih od strane istraživača i međunarodnih organizacija za standarde ( Shackel (1991) [3], ISO 9241-11(1998) [4], ISO 9126 (2001) [5], QUIM model (2006) [6], ISO 25010 (2011) [7]) izveden je zaključak da karakteristika *fleksibilnost* ima značajan

uticaj na upotrebljivost Web aplikacija. Iako ovi modeli imaju dosta različitih atributa, analizom zajedničkih osobina ustanovljene su sličnosti.

Iako istraživači prepoznaju značaj fleksibilnosti [3], [6], [7], [8], među istraživačima nedostaje konsenzus o definisanju i proceni fleksibilnosti, što dovodi do zaključka da fleksibilnost softverskih sistema još uvek predstavlja problem. Pored brojnih definicija fleksibilnosti, u ovom delu rada navedene su hronološki samo reprezentativne definicije korišćene u različitim istraživanjima u poslednje tri decenije.

Shackel je (1986) u [8] predstavio operativnu definiciju upotrebljivosti koja omogućava da se proceni sistem tokom životnog ciklusa razvoja. On je predstavio jedan od najčešće korišćenih definicija upotrebljivosti. On ukazuje da je sistem upotrebljiv u meri u kojoj je on efikasan, lak za učenje, fleksibilan i subjektivno prijatan. Shackel je 1991. godine u [3] definisao fleksibilnost kao „dozvoljenu adaptaciju na određeni nivo varijacije u zadatku i/ili okruženju”. Očito da je pri formulisanju ove definicije ključni uticaj imala ergonomija, jer se govori o adaptaciji proizvoda zadatku a ne korisniku, dakle ne govori se o svesnoj operaciji „adaptiranja” od strane korisnika. Međutim, proizvod se može koristiti u različitim okruženjima, sa različitim zadacima i korisnicima, što može uticati na upotrebljivost. Naime, veliki broj programa se prodaju danas kao izvršni fajlovi, što znači da se oni mogu izvršavati samo na određenoj familiji procesora i pod određenim operativnim sistemom. Ako želimo da te programe prebacimo da se izvršavaju na nekom drugom procesoru naići ćemo na nepremostive teškoće. Zato se mora imati u vidu kontekst u kome se namerava upotreba proizvoda, jer proizvod koji je upotrebljiv u jednom kontekstu upotrebe ne mora biti upotrebljiv u drugom kontekstu. Zato je neophodno proširiti definiciju fleksibilnosti tako što će se uključiti i mogućnost korišćenja proizvoda u različitim kontekstima upotrebe. Bevan i dr. (1991) u [9] raspravljaju da se upotrebljivost zasniva na proizvodu, korisniku, jednostavnosti upotrebe i prihvatljivosti proizvoda za određenu klasu korisnika za obavljanje specifičnih zadataka u specifičnom okruženju. Dix i dr. (1998) su u [10] predstavili model upotrebljivost sistema u tri kategorije: lakoća učenja, fleksibilnost i robusnost. Doniaee i dr. (2001) su u [11] razvili integrisani model merjenja kvaliteta u upotrebi (QUIM). Atributi uključeni u QUIM su: efektivnost, efikasnost, zadovoljstvo, produktivnost, bezbednost, dostupnost i internacionalnost. Studija CUNY+ (2002) u [12] primarno koristi upitnik kao metod procene upotrebljivosti. Autori sprovode studiju u dve faze da uporede upotrebljivost tekst-zasnovanih i Web zasnovanih CUNY Web sajtova. Kriterijumi koji su primenjivani su uticaj, efikasnost, kontrola, predusretljivost i prilagodljivost. Seffah i dr. razvijaju 2006 godine [13] konsolidovani model za merenje upotrebljivosti i metrika, skraćeno nazvan QUIM (eng. Quality in Use Integrated Measurement). On kombinuje različite standarde i modele, kao što su ISO 9241 i ISO 9126 i objedinjuje u jedan konsolidovani,

hijerarhijski model. On navodi metode za utvrđivanje zahteva kvaliteta kao i identifikovanje, implementaciju, analiziranje i vrednovanje i procesa i metrika kvaliteta proizvoda. Ovaj model je pogodan početnim korisnicima koji imaju malo znanja o upotrebljivosti i može biti primenjivan i od strane stručnjaka upotrebljivosti i ne stručnjaka. QUIM model se sastoji od 10 faktora (efikasnost, efektivnost, zadovoljstvo, lakoća učenja, produktivnost, bezbednost, poverenje, pristupačnost, korisnosti i univerzalnost), podeljenih na 26 merljivih kriterijuma koji sadrže 127 specifičnih metrika. Model se koristi za merenje stvarne upotrebe softvera u radu i identifikovanje problema. QUIM model povezuje faktore sa kriterijumima i metrikama na jasan i konzistentan način. Može se koristiti uopšten ili se može prilagoditi da se u specifičnom kontekstu.

Prva definicija upotrebljivosti u ISO/IEC 9126 (1991), posmatrala je upotrebljivost kroz attribute korisničkog interfejsa koji doprinose sposobnosti softverskog proizvoda da bude razumljiv, upotrebljiv i atraktivan za korisnika, kada se koristi pod specificiranim uslovima. Međutim, ova definicija upotrebljivosti je u suprotnosti sa definicijom upotrebljivosti u ISO 9241-11 (1998), koji upotrebljivost posmatra sa ergonomске tačke gledišta kao „stepen do kojeg proizvod može da se koristi od strane početnika i iskusnih korisnika da obavljaju zadatke za postizanje željenih funkcionalnosti proizvoda sa merenjem efikasnošću, efektivnošću i zadovoljstva u određenom kontekstu korišćenja“. Prema međunarodnom standard u ISO 9241-11, "Merenje performansi i zadovoljstva korisnika može da obezbedi osnovu za poređenje relativne upotrebljivosti proizvoda sa različitim tehničkim karakteristikama koji se koriste u istom kontekstu". Kvalitet u upotrebi je rezultat interakcije između korisnika i proizvoda dok obavlja zadatke u tehničkom, fizičkom, socijalnom i organizacionom okruženju.

TABELA 1. FLEKSIBILNOST KAO ATRIBUT UPOTREBLJIVOSTI U RAZLIČITIM STANDARDIMA, MODELIMA I DEFINICIJAMA

Izvor	Atributi
(Shackel, 1986,1991) [3], [8]	lakoća korišćenja, efektivnost, lakoća učenja, fleksibilnost, korisnički stav
(Bevan et al., 1991) [9]	proizvod, korisnik, jednostavnost upotrebe i prihvatljivost proizvoda
(Preece, 1994) [14]	lakoća učenja, propusnost, stav, fleksibilnost
(Dix et al., 1998) [10]	lakoća učenja, fleksibilnost, robusnost
(Donyaee et al., 2001) [11]	efektivnost, efikasnost, zadovoljstvo, produktivnost, bezbednost, dostupnost i internacionalnost
(Oulanov and Pajarillo, 2002) [12]	uticaj Web sajta, efikasnost, kontrola, predusretljivost, prilagodljivost
(Seffah et al., 2006) [13]	efikasnost, efektivnost, produktivnost, zadovoljstvo, lakoća učenja, bezbednost, poverenje, pristupačnost, univerzalnost i korisnost.
(ISO 25010, 2009, 2011)	efektivnost, efikasnost, zadovoljstvo, bezbednost, prilagođenost kontekstu

Ova šira interpretacija upotrebljivosti je ugrađena u promenjenom ISO 9126-1 (2001), nazvana "kvalitet u upotrebi" kao kvalitet iz perspektive korisnika kada

koristi proizvod [15]. Međutim, kada je model kvaliteta iz ISO/IEC 9126-1 ugrađen u ISO/IEC 25010 [7], radi usklađivanja definicije, karakteristika *upotrebljivost* je preimenovana u *operabilnost* i ima šire značenje. To je omogućilo da se karakteristika *upotrebljivost* definiše kao *kvalitet u upotrebi*, sa podkarakteristikama efektivnost, efikasnost i zadovoljstvo preuzetih iz standarda ISO 9126-1, kome su dodate još dve karakteristike: *bezbednost* iz 9126-1, kao i *fleksibilnost u upotrebi* kako bi se obuhvatili različiti konteksti upotrebe.

Prema tome, kvalitet u upotrebi predstavlja stepen do kog korisnici mogu postići svoje ciljeve u određenom okruženju tj. kvalitet softverskog proizvoda sa korisničkog aspekta kada se koristi u specifičnom okruženju i u kontekstu specifične upotrebe.

Potrebno da se razmotri kontekst je izričit u novoj definiciji kvaliteta u upotrebi u ISO/IEC CD 25010.3. Zato je **Fleksibilnost** uključena kao treća karakteristika kvaliteta u upotrebi, sa podkarakteristikama *usaglašenost sa kontekstom*, *proširivost na kontekst* i *pristupačnost* u upotrebi.

*Usaglašenost sa kontekstom* se definiše kao stepen do kojeg upotrebljivost i bezbednost ispunjavaju uslove u svim kontekstima namenjene upotrebe. Ovo obezbeđuje osnovu za merenje stepena u kome je upotrebljivost postignuta u nameranim kontekstima upotrebe.

*Proširivost konteksta* se definiše kao stepen upotrebljivosti i bezbednosti izvan prvobitno nameranih konteksta. Proširivost konteksta se može postići prilagođavanjem proizvoda za dodatne korisničke grupe, zadatke i kulture. Proširivost konteksta omogućava proizvodima da uzmu u obzir okolnosti, mogućnosti i individualne želje koji ne mogu biti predviđeni unapred. Ako proizvod nije namenjen za proširivost konteksta, neće biti bezbedno koristiti proizvod u kontekstima za koje nije namenjen. Proširivost konteksta je teže odrediti i meriti unapred, kao što je u pitanju upotreba u neočekivanim kontekstima upotrebe. Zahtevi dizajna koji olakšavaju proširivosti konteksta obuhvataju projektovanje proizvoda, tako da može da se konfigurise za specifične potrebe (npr. jezik, kultura, radni koraci), ili se mogu prilagoditi od strane korisnika da odgovaraju individualnim mogućnostima i potrebama. Proizvodi se često koriste za nepredviđene svrhe, tako da sposobnost proizvoda da se prilagodi novim potrebama znatno proširuje upotrebljivost. To se jedino može pravilno oceniti preko modela stvarne upotrebe, ali potencijalno može biti procenjen stepen u kojoj meri je dizajn otvoren za konfiguraciju i adaptaciju. Kao i kod usklađenosti sa kontekstom, identifikovanje zahteva za proširivost konteksta može imati veliki uticaj na dizajn.

*Pristupačnost* je definisana kao stepen upotrebljivosti za korisnike sa posebnim potrebama. Identifikovanje opsega nameranih konteksta upotrebe može da otkrije dodatne korisnike, zadatke i okruženja koji mogu da budu prioritet za testiranje. *Pristupačnost* može biti određena uspostavljanjem ciljeva upotrebljivosti za korisnike sa

posebnim potrebama, dajući cilj dizajnu za uspešnost i produktivnost koja se očekuje od korisnika sa invaliditetom.

Iz perspektive krajnjih korisnika Web aplikacija, na fleksibilnost najviše utiču: *usaglašenost sa kontekstom*, *proširivost na kontekst* i *personalizacija* u upotrebi. Podkarakteristika *Personalizacija* predstavlja stepen do kojeg korisnici mogu da izmene Web aplikaciju da odgovara njihovim specifičnim željama i potrebama. Ova podkarakteristika nije bila definisana u ISO/IEC 25010 standardom, ali je i jasno pominjana u kontekstu upotrebe krajnjih korisnika i također podržana prethodnim studijama.

## REZULTATI ISTRAŽIVANJA

Upotrebljivost je definisana u odnosu na performanse i zadovoljstvo korisnika u određenom kontekstu upotrebe. Važnost konteksta se mora imati u vidu, jer proizvod koji je upotrebljiv u jednom kontekstu upotrebe ne mora biti upotrebljiv u drugom kontekstu sa različitim korisnicima, zadacima ili okruženjem. Međutim, posledica toga može biti vrlo visoka upotrebljivost za proizvod sa pažljivo odabranim, ali nereprezentativnim, korisnicima, zadacima i okruženjem korišćenja. Zato je neophodno da potencijalni kupac prosudi da li korisnici, zadaci i okruženja za koje je upotrebljivost pokazana, odgovaraju njihovim potrebama [16].

Iz tog razloga veoma je važno uspostaviti metod za merenje sposobnosti prilagođavanja aplikacije zahtevima koji su specifični za kontekst u kome će se koristiti ili se namerava njeno korišćenje.

Osnovne metrike fleksibilnost za ispitivanje i merenje su:

- stepen postignute upotrebljivosti u nameranom kontekstu upotrebe.
- stepen postignute upotrebljivosti izvan prvobitno nameranog konteksta.
- stepen do kojeg korisnici mogu da izmene aplikaciju radi prilagođenja specifičnim željama i potrebama korisnika

Fleksibilnost se može dobiti direktnim merenjem subjektivne procene eksperta a može i indirektno izračunavanjem relativne efikasnosti. Direktno merenje podrazumeva da se za odabrane korisnike meri vreme izvršavanja određenih zadataka. Može se posmatrati kao stepen u kome korisnici koriste pojedine proizvode u određenim kontekstima. Potrebno je napraviti razliku između korisnika sa određenim iskustvom u korišćenju računara i korisnika koji ne poseduju takvo iskustvo. Dakle, relativna efikasnost ekspertske korisnika se definiše kao odnos (izražen u procentima) efikasnosti ekspertske korisnika izvan nameranih konteksta i efikasnosti ekspertske korisnika u prvobitno nameranim kontekstima upotrebe.

Dakle, da bi se izračunao stepen prilagođenja kontekstima za koje nije namenjen, utvrđuje se promena produktivnosti izmerene u dve uzastopne pojedinačne

ponovljene sesije evaluacije istog zadatka u nameravanom i ne nameravanom kontekstu.

Najpre se meri Relativna Efikasnost svakog pojedinačnog ekspertskog korisnika u nameravanom kontekstu, a zatim se izračunava prosečan broj svih korisnika za određenu grupu korisnika. Ekspertski korisnik je definisan kao lice koje je potpuno obučeno i ima značajno iskustvo za korišćenje proizvoda. Ako je na raspolaganju više stručnjaka, onda ekspertaska efektivnost i ekspertsko vreme na zadatku može biti prosek rezultata postignutih od strane svih eksperata. Očigledno, ako su na raspolaganju više stručnjaka, mogu se dobiti pouzdaniji prosečni podaci.

Za vrednovanje *Fleksibilnosti* specificirana je indirektna metrika nazvana *stepen prilagođavanja kontekstima*, prikazana u Tabeli 2 a koja se dobija izračunavanjem preko zadatih formula

TABELA 2: SPECIFIKACIJA METRIKE FLEKSIBILNOSTI

Metrika	Tip podatka	Metod merenja/izračunavanja	Jed mere	Skala
Stepen prilagođavanja kontekstu	Kontinuirani	Utvrdjuje se izračunavanjem Relativne eksperstske efikasnosti kao odnos efikasnosti ekspertskog korisnika van nameravanog konteksta i efikasnosti ekspertskog korisnika u prvobitno nameravanom kontekstu upotrebe	%	Skup celih, pozitivnih brojeva Opseg mera se kreće od 0 do 100%

*Stepen prilagođavanja kontekstima* se matematički izračunava preko formule (1):

$$\text{StepenPrilagođavanjaKontekstima} = \frac{\partial(\text{TES})}{\partial t} \quad (1)$$

U ovoj formuli TES predstavlja efektivnost zadatka (eng. *Task Effectiveness*),  $t$  predstavlja broj ponavljanja evaluacionog zadatka, tj. broj sesije zadatka a  $\partial$  je standardna matematička oznaka za stepen promene.

Matematički, Relativna Ekspertska Efikasnost (REE) se može izračunati preko sledećih formula:

$$\text{REE} = \frac{\text{Efikasnost eksperta izvan nameravanih konteksta}}{\text{Efikasnost eksperta u nameravanim kontekstima}} \times 100\% \quad (2)$$

$$\text{REE} = \frac{\text{EfektivnostEkspertaIzvanNamKont} \times \text{EkspertskoVremeNaZadtkuUNamKont}}{\text{EfektivnostEkspertaUNamKont} \times \text{EkspertskoVremeNaZadtkuIzvanNamKont}} \times 100\% \quad (3)$$

Postoje brojni pristupi koji se koriste za definisanje, merenje i procenu fleksibilnosti. Mora se imati u vidu da procena fleksibilnosti softvera treba da obezbedi kvantitativne i kvalitativne rezultate koji su razumljivi, prihvatljivi i ponovljivi, da bi se dokazao ključni pokretač za poboljšanje fleksibilnosti, a samim tim i kvaliteta softvera. Sve referencirane metodologije zahtevaju od korisnika da prepoznaju probleme fleksibilnosti ili subjektivno ili objektivno procene fleksibilnost merenjem

vremena na zadatku, korektnost, brojanju grešaka ili subjektivnim odgovorima korisnika.

## DISKUSIJA

Fleksibilnost u upotrebi se definiše kao stepen u kome je upotrebljivost postignuta u nameravanim kontekstima upotrebe ili izvan prvobitno nameravanih konteksta.

Zato je veoma važno da se preciziraju karakteristike nameravanog konteksta upotrebe. Širi opseg korisničkih grupa, zadataka i okruženja može da se prevede u dodatnim zahtevima za dizajn proizvoda sa potrebnim karakteristikama da podrže korišćenje za sve identifikovane kontekste upotrebe. Usaglašenost sa kontekstima koji ne mogu biti testirani mogu se ceniti sudovima eksperata.

Dobra fleksibilnost ne samo da brzo dovodi do bolje produktivnosti, već igra važnu ulogu u početnom usvajanju ili odbacivanju tehnologije.

Postoje brojni pristupi koji se koriste za definisanje, merenje i procenu fleksibilnosti. Mora se imati u vidu da procena fleksibilnosti softvera treba da obezbedi kvantitativne i kvalitativne rezultate koji su razumljivi, prihvatljivi i ponovljivi, da bi se dokazao ključni pokretač za poboljšanje fleksibilnosti, a samim tim i kvaliteta softvera. Sve referencirane metodologije zahtevaju od korisnika da prepoznaju probleme fleksibilnosti ili subjektivno ili objektivno procene fleksibilnost merenjem vremena na zadatku, korektnost, brojanju grešaka ili subjektivnim odgovorima korisnika.

Objektivnim metodatama testiranja, fleksibilnosti se može meriti vremenom potrebnim za postizanje performansi navedenih kriterijumom.

Takođe, fleksibilnost kao podkarakteristika upotrebljivosti može biti ocenjivana pomoću subjektivnih upitnika. Mnogi aspekti upotrebljivosti najbolje se mogu proučavati ispitivanjem korisnika. Korišćenje subjektivnih upitnika je uvek bio veoma efikasan i popularan metod za procenu onih aspekata upotrebljivosti koje je teško objektivno izmeriti.

Iako se često zanemaruje, mnogi istraživači ističu fleksibilnost kao ključni atribut stvarne upotrebljivosti i najuticajni faktor uspeha softverskih aplikacija posebno Web aplikacija.

## ZAKLJUČAK

Rad doprinesi sublimiranju i proširenju teoretskih i praktičnih saznanja o upotrebljivosti, razumevanju pojma upotrebljivosti, terminologije i faktora koji doprinose kvalitetu u upotrebi i može da koristi onima koji izučavaju upotrebljivost.



U radu su sagledani aktuelni radovi istraživača iz oblasti upotrebljivosti i važeći standardi iz oblasti kvaliteta u upotrebi kao i različiti aspekti uticaja fleksibilnosti na upotrebljivost Web aplikacija.

## ZAHVALNICA

Ovaj rad je rezultat istraživanja sprovedenih u okviru biletateralnog projekta srpsko-nemačke saradnje: "Flood Prediction and Alerting System" koji je podržan od strane DAAD fondacije i Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

## LITERATURA

[1] Abran, A. Khelifi, A. Suryan, W. and Seffah, A. (2003) "Usability Meanings and Interpretations in ISO Standards," *Software Quality Journal*, vol. 11, pp. 325-338.

[2] Dubey, S.K. and Rana, A. (2010) "Analytical Roadmap to Usability Definitions and Decompositions," vol. 2, no. 9, pp. 4723-4729.

[3] Shackel, B. (1991): Usability – Context, framework, definition, design and evaluation. In *Human Factors for Informatics Usability*, ed. Brian Shackel and Simon J. Richardson, 21-37. New York, Cambridge University Press.

[4] ISO 9241-11, "Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability," Geneva, Switzerland: Author., 1998.

[5] ISO/IEC 9126: 1991/2001.

[6] Seffah, A., Donyaee, M., Kline, R.B. and Padda, H.K. (2006): Usability measurement and metrics: A consolidated model, *Software Quality Control*, Vol. 14, No. 2, pp. 159-178.

[7] ISO/IEC CD 25010.3: 2011, "Systems and software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Software product quality and system quality in use models",. ISO (2011).

[8] Shackel, B. (1981): The concept of usability. *Proceedings of IBM Software and Information Usability Symposium*, Poughkeepsie, NY, September 15-18, 1-30; and in J. L. Bennett, D. Case, J. Sandelin, and M. Smith eds. 1984. *Visual Display Terminals: Usability Issues and Health Concerns*, Englewood Cliffs, NJ: Prentice-Hall, pp. 45-88.

[9] Bevan, N., Kirakowski, J. and Maissel, J., (1991) "What is Usability?," in *Proceedings of the 4th International Conference on HCI*, Stuttgart.

[10] Dix, A., Finley, J., Abowd, G. and Beale, R. (1998): *Human-Computer Interaction*, 2nd edition, Prentice-Hall.

[11] Donyaee, M. and Seffah, A. (2001): QUIM: An Integrated Model for Specifying and Measuring Quality in Use, *Eighth IFIP Conference on Human Computer Interaction*, Tokyo, Japan.

[12] Oulanov, A. and Edmund F. Y. P. (2002): CUNY+ Web: Usability study of the Web-based GUI version of the bibliographic database of the City University of New York (CUNY), *The Electronic Library*, Vol. 20 (6), pp. 481-87.

[13] Seffah, A., Donyaee, M., Kline, R.B. and Padda, H.K. (2006): Usability measurement and metrics: A consolidated model, *Software Quality Control*, Vol. 14, No. 2, pp. 159-178.

[14] Preece, J. Y. Rogers, H. Sharp, D. Benyon, S. Holland, T. Carey, *Human-Computer Interaction*, Addison Wesley, 1994.

[15] Bevan, N., "Quality in Use: Meeting User Needs for Quality," *Journal of Systems and Software*, vol. 1, no. 49, pp. 89-96, 1999.

[16] Stone, R., (2001) "Learning and the importance of interactivity information design becomes interaction design", *Information Visualization*, *Proceedings, Fifth International Conference*, pp 624-629.

# Primena Labview-a u proceni obeležja pokretnog cilja u sistemu sa jednim infracrvenim video senzorom

## The LABVIEW application in parameter estimation of moving target in mono infrared video sensor system

Davorin Mikluc<sup>1</sup>, Milenko Andrić<sup>1</sup>, Boban Bonžulić<sup>1</sup>, Srđan Mitrović<sup>1</sup>  
*Vojna akademija, Univerzitet odbrane<sup>1</sup>*

**Sadržaj** – U radu su analizirane tri video sekvence koje su snimljene sistemom za praćenje cilja sa jednim infracrvenim video senzorom. Obeležja cilja dobijena direktnom obradom slike su: površina cilja, dimenzije cilja, granične vrednosti intenziteta sivog, pozicija cilja na slici, dok su neka obeležja dobijena indirektnim proračunima, a to su daljina do cilja i stav cilja. Procenjena obeležja se mogu koristiti u opisu kinematičkih parametara cilja. Softver LABVIEW® je upotrebljen u kompletnoj analizi i grafičkoj ilustraciji dobijenih rezultata.

**Abstract** – Three video sequences recorded with a target tracking system with one infrared video sensor have been analysed in the paper. Target features obtained in direct image processing are the number of pixels, target size, target dimensions, gray intensity boundaries, target position in the image, while some features result from indirect calculations, and these are target distance and orientation. The estimated features can be used in a kinematic description of target parameters. LABVIEW® software was used throughout the analysis and graphical representation of the obtained results.

### 1. UVOD

Pasivni senzori koji su sastavni deo sistema za praćenje ciljeva se mogu koristiti u različitim primenama, npr. video nadzor i sigurnost, kontrola brzine kretanja ciljeva, kontrola vazdušnog saobraćaja, vođenje projektila, otkrivanje prepreka, robotika i sl.. Sistemi za praćenje sa pasivnim sensorima moraju da zadovolje mnogobrojne zahteve koji se postavljaju u njihovom projektovanju. Karakteristike senzora utiču značajno na kvalitet rezultata. Međutim, jednako tako sistemi sa pasivnim sensorima imaju problem u proceni parametara koji su nedostupni, kao što je procena daljine do cilja, [1-4]. Iz navedenog su proistekla mnogobrojna istraživanja čija je iz oblasti sistema za praćenje cilja sa jednim pasivnim senzorom, bilo u dnevnim ili noćnim uslovima, [5-7]. Jasno je da u noćnim uslovima standardni video senzori imaju još jednu manu više, zbog čega se češće u takvim okolnostima koriste infracrveni video senzori. Međutim, da infracrveni video senzori nisu savršeni govori problem zasićenja, [8].

Prva istraživanja u kojima su predložena rešenja o pasivnom određivanju daljine do cilja na osnovu video sekvenci je data u [9], dok su poboljšanja predstavljena u [10]. S željom da se poveća kvalitet procene daljine do cilja potrebno je unaprediti metode, [11], ili poboljšati

tehnološki razvoj senzora. Primene sofisticiranije metode zasnovane na čestičnom filteru, [12], za sada ima prednost u primeni u odnosu na prethodne metode.

Procena daljine do cilja jeste jedan od najvećih izazova ali nije i jedini. Pokušaj da se objedini više procenjenih obeležja cilja i time da detaljniji opis njegovih kinematičkih parametara, od pozicije cilja, preko stava pa sve do odgovora na pitanje da li cilj manevriše je dat u [13]. U većini istraživanja upotrebljen je softver MATLAB® kao alat za simulacije. Na osnovu prethodnog proistekla je ideja za analiziranjem mogućnosti softvera LABVIEW® u proceni različitih obeležja cilja na osnovu obrade infracrvenih video sekvenci.

### 2. OBELEŽJA CILJA

Podaci o cilju, koji se prati sistemom sa infracrvenim video senzorom, su bogatog sadržaja, na osnovu kojih se mogu izdvojiti i proceniti mnoga obeležja. Veći broj istraživanja se zasniva na primeni različitih matematičkih aparata kako bi se unapredio kvalitet procene obeležja cilja. U ovom radu će biti predstavljene procene obeležja koje će biti dobijene obradom slike u softveru LABVIEW®. Opis i upotreba izdvojenih i procenjenih obeležja cilja su data u narednom delu teksta.

a) Pozicija centra cilja na slici po obe koordinate,  $X_c$ ,  $Y_c$ .

b) Dimenzija cilja na slici po obe koordinate,  $X$ ,  $Y$ .

Obeležja navedena pod a) i b) su važna za prozoranje, odnosno za procenu očekujuće zone pojavljivanja cilja u narednom frejmu. Zona očekivanja se zasniva na pravougaonom prozoru sa težištem u procenjenoj poziciji centra cilja.

c) Srednja vrednost intenziteta cilja,  $\bar{I}$ .

d) Standardna devijacija intenziteta cilja,  $\sigma_I$ .

Obeležja pod c) i d) predstavljaju opis intenziteta sivog cilja na slici, koji se može upotrebiti za proračun raspodele intenziteta cilja, zatim za dalju analizu kontrasta ili gradijent. Krajnji rezultat procene raspodele intenziteta i njegove promene su u direktnoj vezi sa uticajem na procenu površine cilja i procenu praga detekcije piksela.

e) Stav cilja, ugao  $\alpha$ .

f) Odnos dimenzija  $Y$  i  $X$ ,  $\rho$ .

Obeležja pod e) i f) govore o orijentaciji cilja na slici. Odnos dimenzija  $Y$  i  $X$  je proporcionalan tangensu ugla  $\alpha$ . Drugim rečima, ukoliko cilj vrši manevar ili promenu stava, mogu se oba navedena obeležja analizirati u nameri da se proceni da li i kakav tipa manevra je izvršio cilj.

g) Površina cilja,  $S_c$ .

h) Daljina do cilja,  $D_c$ .

U radovima [8-12] je data poznata relacija na osnovu koje se određuje daljina do cilja pomoću procenjene površine. Upravo su obeležja pod g) i h) u navedenoj vezi koja glasi:

$$D_e(k) = D_0 \sqrt{\frac{S_0}{S_e(k)}} \quad (1)$$

gde su:  $D_e(k)$  procenjena daljina do cilja, a  $S_e(k)$  procenjena površina cilja u  $k$ -toj slici, dok su  $D_0$  i  $S_0$  daljina do cilja i površina cilja u početnom trenutku praćenja cilja.

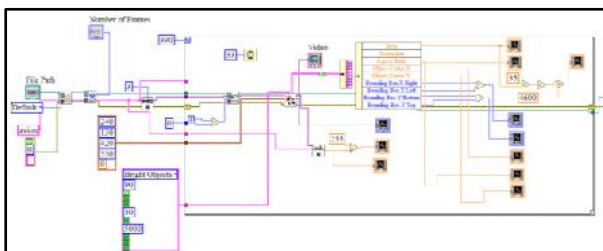
Poslednje obeležje se odnosi na broj ciljeva.

j) Broj ciljeva, N.

Ovo obeležje je samo pokazatelj da se u softveru LABVIEW® može pratiti i više ciljeva.

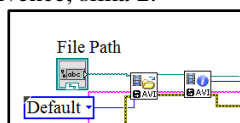
### 3. LABVIEW STRUKTURNI BLOK DIJAGRAM

Softver LABVIEW je veoma pristupačan inženjerima, jer je zasnovano na objektno orijentisanom programiranju. Pri tome se mora napomenuti da je pomoć u vidu opisa bloka kao i potrebnih ulaza vrlo informativna i pristupačna. U radu su analizirana tri različita scenarija sa istim strukturnim blok dijagramom kod kojih se menjaju vrednosti za podešavanje prozora za praćenje cilja i početne vrednosti za daljinu do cilja. Strukturni blok dijagram je dat na slici 1.



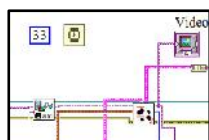
Slika 1. Strukturni blok dijagram za procenu obeležja cilja

Strukturni blok dijagram će ukratko biti objašnjen kroz nekoliko osnovnih delova koji ga čine. Prvi deo se odnosi na unos video sekvence, slika 2.



Slika 2. Strukturni blok dijagram za unos video sekvence

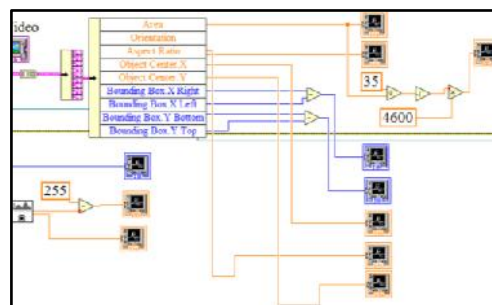
Zatim sledi blok za obradu slike, slika 3. Na istoj slici se vidi i blok za kasnjenje od 33 ms, što odgovara brzini od 30 slika u sekundi.



Slika 3. Strukturni blok dijagram za obradu i prikaz slike

Sledeći blok je izdvajanje i procenu obeležja cilja, slika 4.

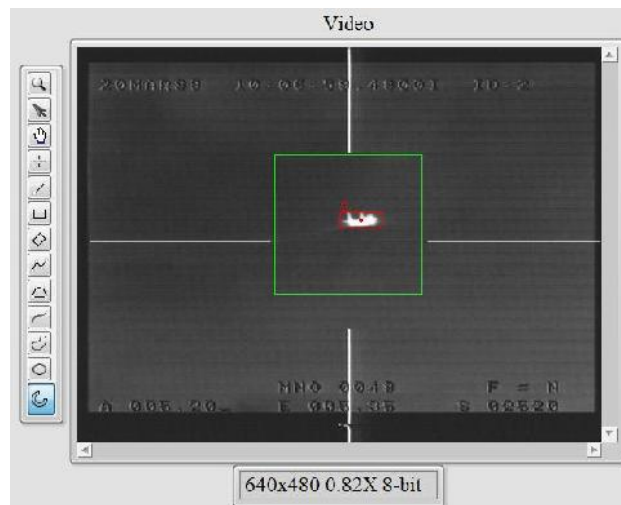
Ostali delovi strukturnog blok dijagrama sa slike 1, koji nisu pomenuti služe za fina podešavanja u zavisnosti od video sekvence koja se analizira.



Slika 4. Strukturni blok dijagram izdvajanje i prikaz obeležja cilja

### 4. PROCENJENA OBELEŽJA CILJA

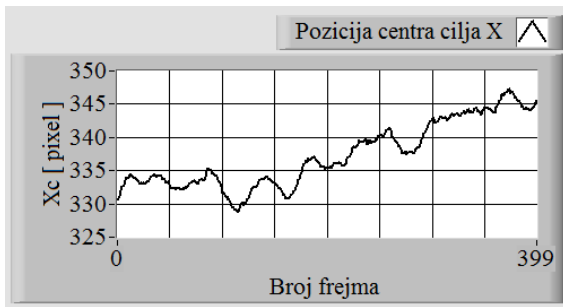
Navedena obeležja u drugom odeljku su procenjena pomoću strukturnog blok dijagrama a na osnovu slike iz unete video sekvence, slika 1. Rezultati predstavljaju deo Front panela u LABVIEW®-u, ali zbog većeg broja obeležja i bolje preglednosti, svaki od rezultata je pojedinačno predstavljen. Prva analizirana video sekvenca je sadržavala ukupno 400 slika u kojoj je praćen cilj sa manje zašumljenom pozadinom. Jedna od slika iz video sekvence je prikazana na slici 5.



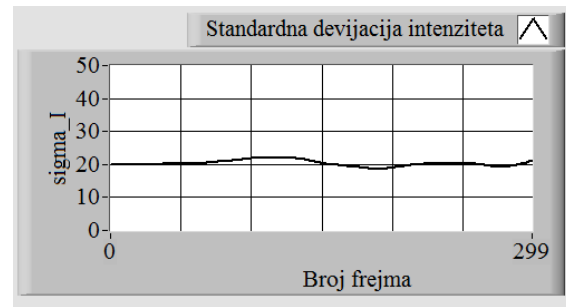
Slika 5. Slika iz video sekvence 1

Na slici 5 se vidi da je rezolucija slike 640x480 piksela i da je sadržaj 8-bitni, što odgovara vrednosti intenziteta 0-255. S obzirom da je sistem za praćenje generisao dodatne linije na video sekvenci, morao se formirati manji prozor na osnovu koga je sprovedena analiza. Taj prozor je obojen zelenom bojom, dok prozor crvene boje predstavlja pravougaoni prozor na osnovu procenjene dimenzije cilja. U narednim slikama 6-15 su prikazana izdvojena i procenjena obeležja cilja.

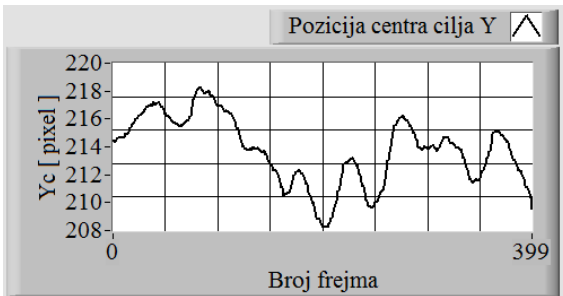
Na osnovu slika 6. i 7. može se zaključiti da je pozicija cilja za vreme trajanja sekvence na približno istom mestu. Procenjene dimenzije po koordinatama, slike 8. i 9., su u skladu sa slikom 14., što govori o povećanju površine cilja.



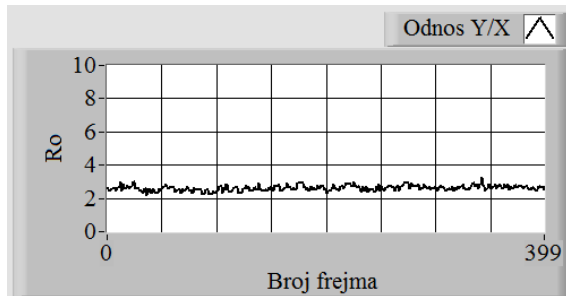
Slika 6. Centar cilja po X koordinati u video sekvenci 1



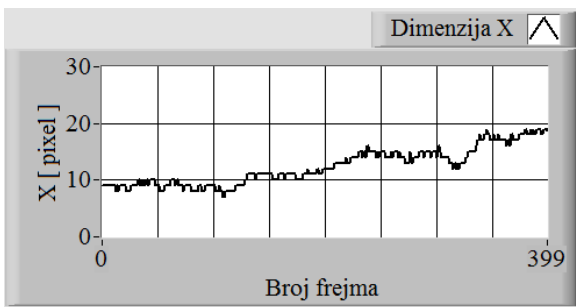
Slika 11. Standardna devijacija intenziteta u video sekvenci 1



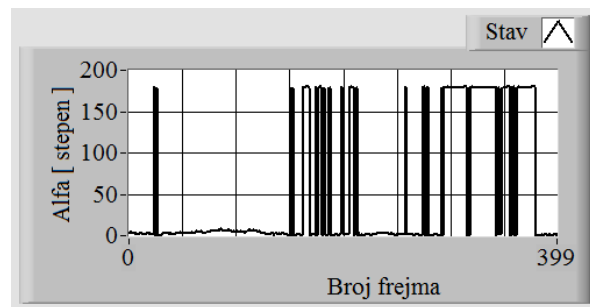
Slika 7. Centar cilja po Y koordinati u video sekvenci 1



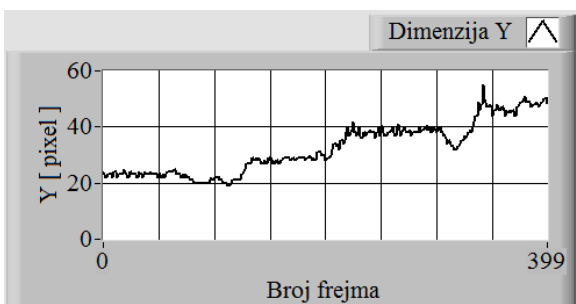
Slika 12. Odnos dimenzija u video sekvenci 1



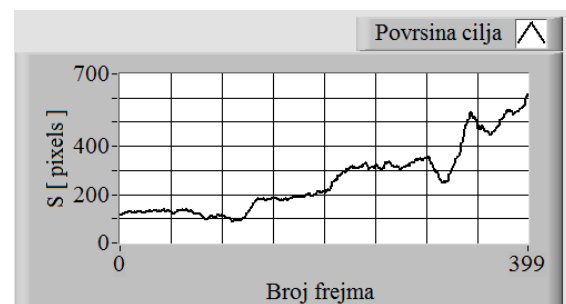
Slika 8. Dimenzija cilja po X u video sekvenci 1



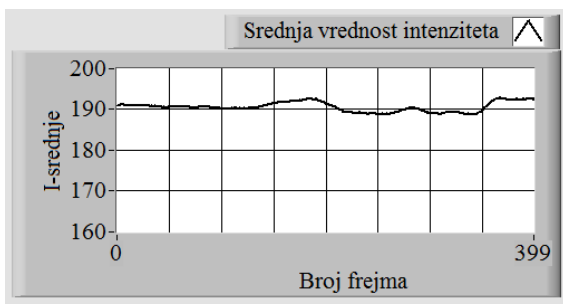
Slika 13. Stav cilja u video sekvenci 1



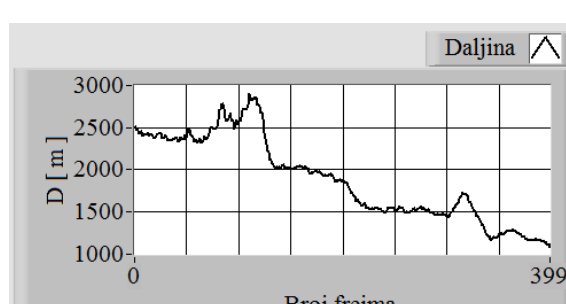
Slika 9. Dimenzija cilja po Y u video sekvenci 1



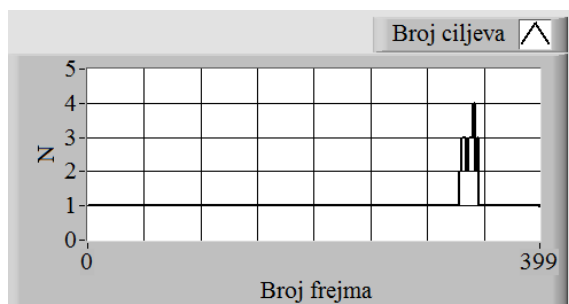
Slika 14. Površina cilja u video sekvenci 1



Slika 10. Srednja vrednost intenziteta u video sekvenci 1



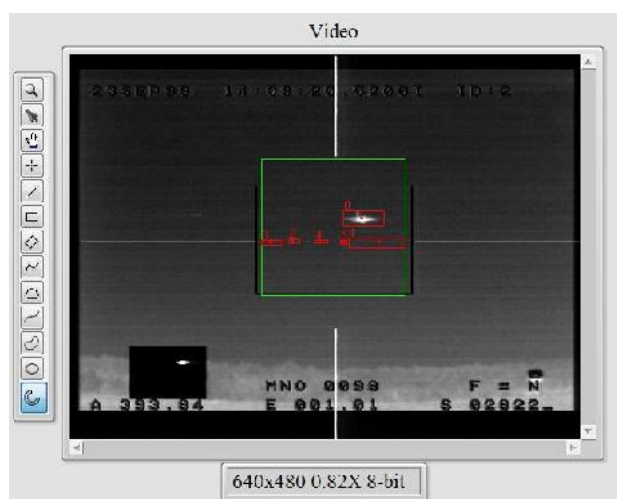
Slika 15. Daljina do cilja u video sekvenci 1



Slika 16. Broj ciljeva u video sekvenci 1

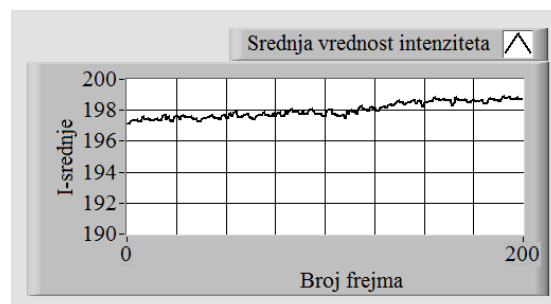
Povećanje dimenzija cilja je linearno jer je njihov odnos, slika 12, konstantan. Takođe konstantne vrednosti su obeležja za srednju vrednost i standardnu devijaciju intenziteta sivog, slike 10. i 11. Promene u proceni stava su posledica matematičkih operacija, jer stav od 0 i 180 stepeni govori da je istog značanja odnosno da je cilj na slici vodoravan, slika 13. Povećanje površine utiče na procenu daljine, izraz (1). Manja promena u periodu od 80.-120. slike video sekvence je posledica promene intenziteta pozadine što je uticalo na prag detekcije i uslovalo povećanje površine odnosno smanjenje procenu daljine do cilja, slike 14. i 15. Konačno, slika 16. objašnjava kvalitet blok za izdvajanje cilja na slici, gde je došlo izdvajanje lažnih ciljeva samo u periodu 330. - 345. slike. Analiza prve video sekvence ukazuje da se cilj ravnomerno kretao prema senzoru, bez manevara i promene stava bez obzira na manju promenu pozadine.

Sledeća video sekvenca, broj 2, sadrži 200 slika, u kojoj cilj ne vrši manevar, ali je primetan problem niskog intenziteta cilja u odnosu na pozadinu, što će se odraziti na broj lažnih ciljeva. Slika 17. je prikaz jedne slike iz video sekvence 2.

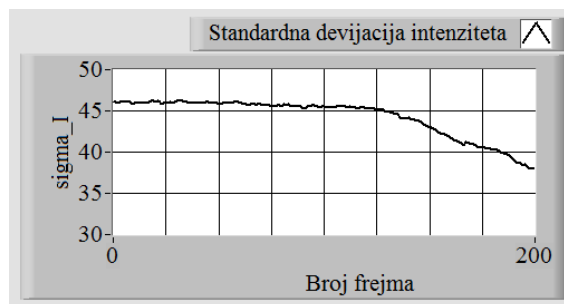


Slika 17. Slika iz video sekvence 2

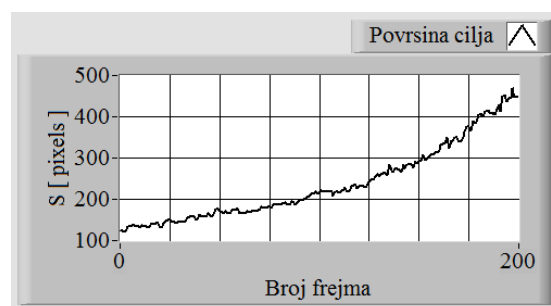
Usled velikog broja obeležja u ovom delu rada će se prikazati samo nekoliko karakterističnih obeležja. Kretanje cilja je ravnomerno kao i u video sekvenci 1, zbog čega su pozicija, dimenzija, odnos i stav cilja istih karakteristika pa je iz tog razloga izostavljen njihov grafički prikaz.



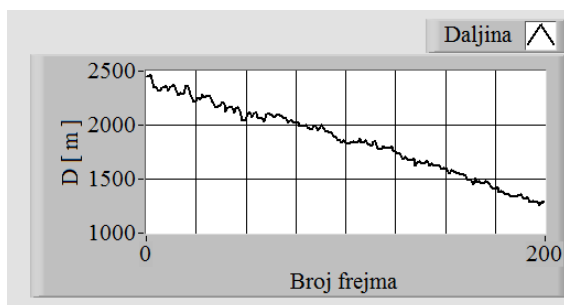
Slika 18. Srednja vrednost intenziteta u video sekvenci 2



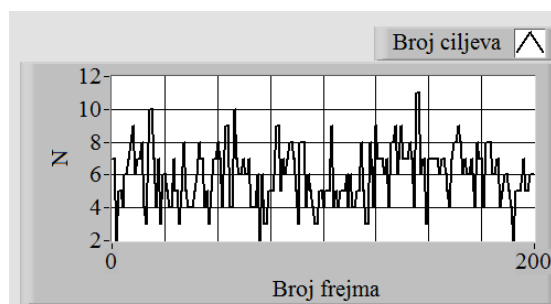
Slika 19. Standardna devijacija intenziteta u video sekvenci 2



Slika 20. Površina cilja u video sekvenci 2



Slika 21. Daljina do cilja u video sekvenci 2

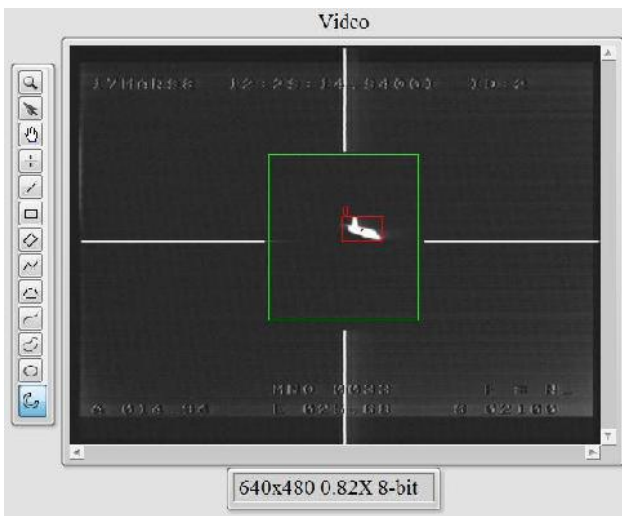


Slika 22. Broj ciljeva u video sekvenci 2

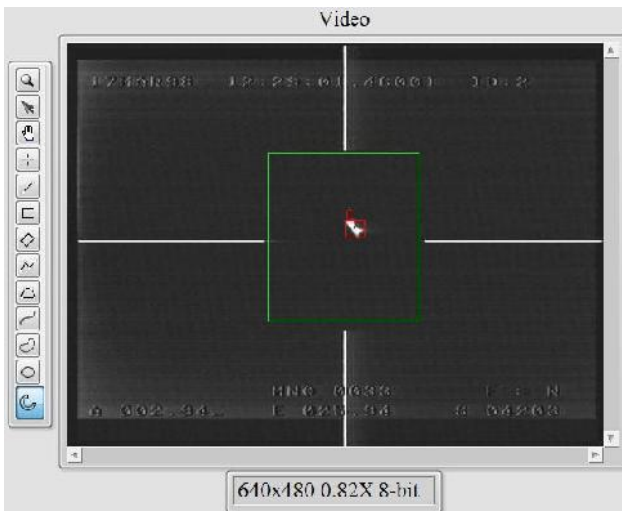


Srednja vrednost i standardna devijacija intenziteta cilja, slika 18. i 19., pokazuju da se cilj u toku trajanja video sekvence 2, jasnije izdvaja iz pozadine zbog čega opada standardna devijacija. U ovoj video sekvenci se u potpunosti vidi linearno smanjenje daljine do cilja, slika 21, i ujedno pokazuje validnost izraza (1) posmatrajući sliku 20. Vrlo bitno je da se formiranim strukturnim blok dijagramom, slika 1, može izdvajati i procenjivati obeležja više ciljeva istovremeno. Slika 22. pokazuje da uticaj većeg broja lažnih ciljeva nije uticao na procene.

Poslednja video sekvenca 3 je trajanja 13 s i sadrži kretanje cilja sa manebrima i promenom stava, što je predstavljeno na slikama 23. i 24.

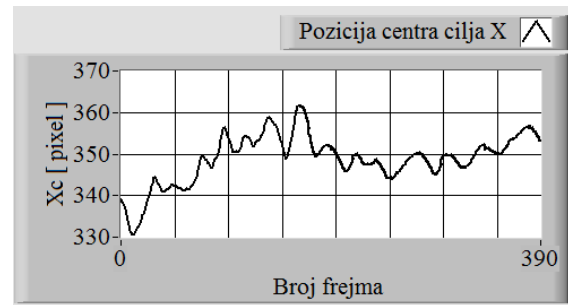


Slika 23. Početni stav cilja u video sekvence 3

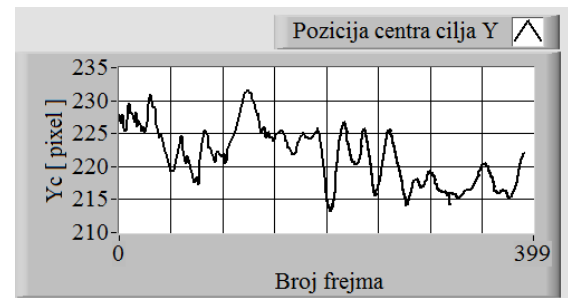


Slika 24. Cilj nakon u manebrima u video sekvence 3

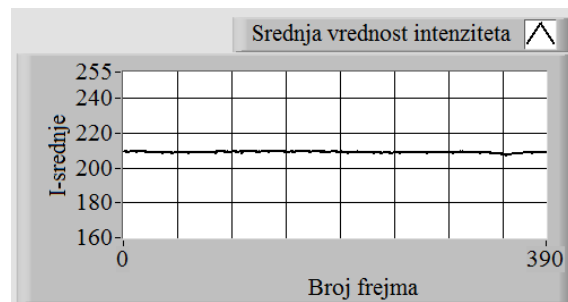
Problem praćenja cilja koji izvodi maneuvre je veoma zahtevan za sistem koji ga prati. Iz tog razloga je veoma teško održavati poziciju senzora kako bi pozicija cilja bila uvek u centru slike, što ilustruju slike 25. i 26. Istovremeno vrednosti intenziteta i standardne devijacije, su konstante, slike 27. i 28., a to znači da je praćen isti cilj sa istom raspodelom intenziteta i ne zavise od manevara.



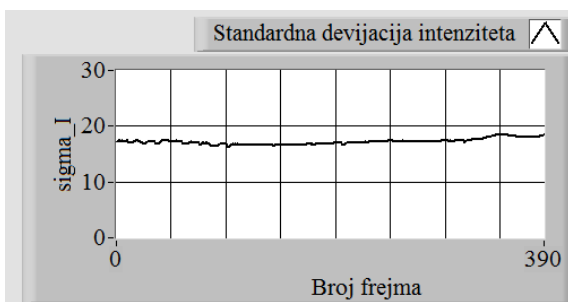
Slika 25. Centar cilja po X koordinati u video sekvenci 3



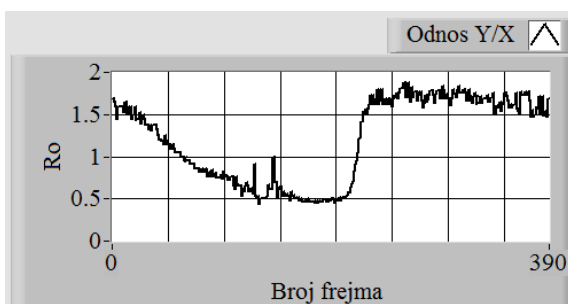
Slika 26. Centar cilja po Y koordinati u video sekvenci 3



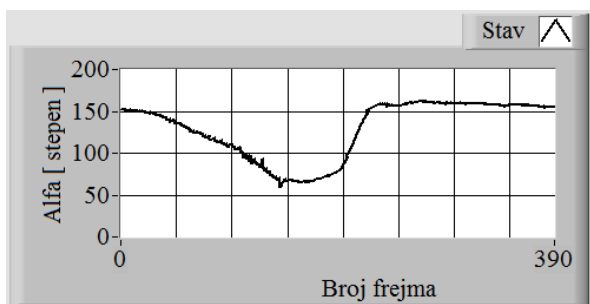
Slika 27. Srednja vrednost intenziteta u video sekvenci 3



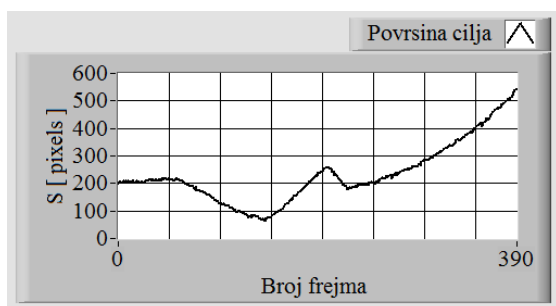
Slika 28. Standardna devijacija intenziteta u video sekvenci 3



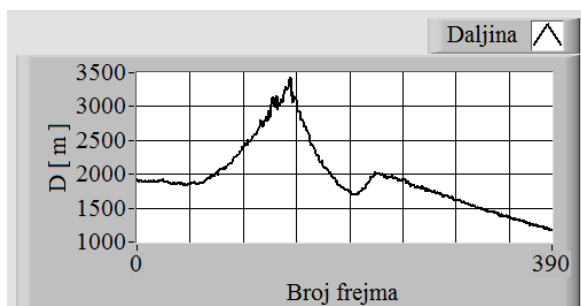
Slika 29. Odnos dimenzija u video sekvenci 3



Slika 30. Stav cilja u video sekvenci 3



Slika 31. Površina cilja u video sekvenci 3



Slika 32. Daljina do cilja u video sekvenci 3

Ostale slike 29. – 32. pokazuju da li je izvršen manevar i koji. Na osnovu obeležja stava i odnosa  $\rho$  se tačno vidi koji je manevar izvršen i u kom trenutku, a potvrda toga je očigledna i u rezultatima vrednosti površine i daljine do cilja.

## 5. ZAKLJUČAK

U ovom radu je prikazana mogućnost primene softvera LABVIEW®-a u izdvajanju i proceni obeležja. Formiran je strukturni blok dijagram koji je primenjen na tri različite infracrvene video sekvence. Analizom procenjenih obeležja su potvrđene pretpostavke o kretanju cilja. Dalja istraživanja u vidu primene softvera LABVIEW® bi se zasnivala na izdvajanju i proceni obeležja cilja u realnom vremenu i u različitim sistemima za praćenje sa infracrvenim video senzorima.

## LITERATURA

[1] J. R. Anderson, M. R. Hawks, K. C. Gross, G. P. Perram, *Flight test of an imaging O2 (Xb) monocular passive ranging instrument*, in: SPIE Defense, Security,

and Sensing, International Society for Optics and Photonics, 2011, pp. 802005–802005. doi:10.1117/12.883484.

[2] W.-H. Diao, X. Mao, L. Chang, L. Jiang, *Operating distance evaluation method for infrared imaging system under complicated backgrounds*, *Electronics letters* **45**(25), pp. 1309–1310. (2009), doi:10.1049/el.2009.0882.

[3] Benet, Gines, et al., *Using infrared sensors for distance measurement in mobile robots*, *Robotics and autonomous systems* **40**(4) (2002): 255-266.

[4] Xu, Jian-Zhong, et al., *A distance estimation algorithm based on infrared imaging guided*, 2009 International Conference on Machine Learning and Cybernetics. Vol. 4. IEEE, 2009.

[5] Zappi, Piero, Elisabetta Farella, and Luca Benini, *Tracking motion direction and distance with pyroelectric IR sensors*, *IEEE Sensors Journal* **10**(9) (2010): 1486-1494.

[6] Srivastava, Hari Babu, et al., *Airborne Infrared Search and Track Systems*, *Defence Science Journal* **57**(5) (2007): 739.

[7] De Visser, Maarten, et al., *Passive ranging using an infrared search and track sensor*, *Optical Engineering* **45**(2) (2006): 026402-026402.

[8] B. P. Bondžulić, S. T. Mitrović, Ž. P. Barbarić, M. S. Andrić, "A comparative analysis of three monocular passive ranging methods on real infrared sequences", *Journal of Electrical Engineering* **64**(5), pp. 305–310, (2013), doi:10.2478/jee-2013-0044.

[9] Atherton, Tim J., Darren J. Kerbyson, and Graham R. Nudd, *Passive estimation of range to objects from image sequences*, BMVC91. Springer London, 1991. 343-346.

[10] S. T. Mitrović, B. P. Bondžulić, M. S. Andrić, Ž. P. Barbarić, *The statistical approach for overcoming the sensor saturation effect in passive ranging*, *Elektronika ir Elektrotehnika* **20**(2), pp. 52–57, (2014), doi:10.5755/j01.eee.20.2.3788.

[11] Z. P. Barbaric, B. P. Bondzulich, S. T. Mitrovic, *Passive ranging using image intensity and contrast measurements*, *Electronics Letters*, **48**(18), pp. 1122–1123, (2012), doi:10.1049/el.2012.0632.

[12] Mikluc, D. L., Andrić, M. S., Mitrović, S. T., & Bondžulić, B. P. (2017). Improved method for passive ranging based on surface estimation of an airborne object using an infrared image sensor. *Optica Applicata*, **47**(3), 383-394.

[13] Davorin M., Srđan T. M., Boban B., *Analiza mogućnosti detekcije manevra aviona praćenog infracrvenim video senzorom*, ETRAN 2017, Kladovo, 05.-08. jun 2017, ISBN 978-86-7466-692-0, str. AU1.3.1-5.

# ОБЈЕКТИВНА ПРОЦЕНА КВАЛИТЕТА СЛИКА СА ВИШЕСТРУКИМ ДИСТОРЗИЈАМА OBJECTIVE QUALITY ASSESSMENT OF MULTIPLY DISTORTED IMAGES

Ненад Стојановић<sup>1</sup>, Бобан Бонцулић<sup>2</sup>, Владимир Петровић<sup>3</sup>, Даворин Миклуц<sup>2</sup>  
Војска Србије<sup>1</sup>

Универзитет одбране у Београду, Војна академија<sup>2</sup>  
Универзитет у Новом Саду, Факултет техничких наука<sup>3</sup>

**Садржај** – У раду је извршена упоредна анализа перформанси знатног броја мера за објективну процену квалитета слике. Анализа је извршена на једној јавно доступној бази слика, а која се састоји од великог броја слика које су деградирани са једном или две дисторзије. Перформансе објективних мера за процену квалитета слике су представљене кроз степен слагања са субјективним скоровима (линеарна корелација и корелација рангова).

**Abstract** – A comparative analysis of a significant number of objective quality assessment metrics performance is described in this paper. The analysis was performed on a publicly available image database, consisting of a large number of images degraded by one or two distortions. Test results of objective image quality assessment measures are presented through correlation with subjective scores.

## 1. УВОД

Експанзија коришћења различитих типова камера које се уграђују у мобилне телефоне и таблет рачунаре довеле су до тога да се слике непрекидно и са сваког места шаљу и објављују путем Интернета. Потребна за квалитетним снимцима је све већа. Међутим, током аквизиције, складиштења, обраде, преноса и приказивања могу се јавити деградације које значајно утичу на квалитет слике.

Током обраде и преноса слике јављају се различити типови и нивои деградација. Често се може јавити случај где је слика оштећена са више од једне деградације. Такви су случајеви када се прво изврши компресија слике, па се након тога слика преноси, а током преноса се додатно јављају различите врсте шума.

Објективне мере за процену квалитета слике морају се суочити са проблемом појаве више од једне дисторзије на слици. Такође, алгоритми за процену квалитета не могу разматрати само утицаје свих појединачних дисторзија на слику, већ се морају узети у разматрање и ефекти које присутне дисторзије изазивају једна другој [1].

Перформансе објективних мера процене квалитета су најчешће тестиране на базама слика са једноструком дисторзијом, као што су LIVE, CSIQ, IVC, Тоуама, TID и сл. Како би се стекло боље разумевање перформанси објективних мера процене квалитета у реалним системима преноса, у овом раду су

анализиране перформансе објективних мера процене квалитета на једној јавно доступној бази слика са једноструким и вишеструким дисторзијама.

У раду је коришћено 19 познатих објективних мера за процену квалитета слике. Све коришћене мере су мере са потпуним референцирањем на изворни сигнал (*Full-Reference*, FR), односно приликом процене квалитета слике са дисторзијом потребно је потпуно познавање изворне слике од које је настала.

Најједноставнија и најчешће коришћена мера је вршни однос сигнал-шум (*Peak Signal to Noise Ratio*, PSNR). PSNR заснива процену квалитета на разлици између изворне и слике са дисторзијом. Мере које се заснивају на информацијама о структури приближније су људском визуелном систему (*Human Visual System*, HVS). Такве мере су UIQI (*Universal Image Quality Index*) [2] и њена чувена проширења SSIM<sub>index</sub> и SSIM (*Structural Similarity Index Metric*) [3]. Из ових метрика је настао значајан број модификација, од којих су у овом раду коришћене MS-SSIM (*Multiscale SSIM*) [4] и IW-SSIM (*Information Content Weighted SSIM*) [5].

Мера која поред структуре, за процену квалитета користи и информације о градијенту је FSIM (*Feature Similarity*) и њено проширење за процену квалитета слика у боји FSIM<sub>c</sub> (*Feature Similarity Color*) [6]. Поред ове мере, коришћено је још неколико мера које се заснивају на очувању информација о градијенту. Једна је GMSD (*Gradient Magnitude Similarity Deviation*) са изведеном GMSM мером (*Gradient Magnitude Similarity Mean*) [7]. GMSD и GMSM мере за анализу очувања информација о градијенту користе SSIM индекс, где се крајња вредност квалитета изводи на основу средње вредности локалних скорова (GMSM) и стандардне девијације локалних скорова квалитета (GMSD). Очување амплитуда и оријентација градијента је основа објективних мера процене квалитета слике  $Q$ ,  $Q_{w1}$  и  $Q_{w2}$  [8, 9], код којих се крајња вредност квалитета добија усредњавањем локалних скорова квалитета (мера  $Q$ ), односно увођењем мапа значаја (мере  $Q_{w1}$  и  $Q_{w2}$ ). GSM мера (*Gradient Similarity Metric*) [10], такође користи очување информација о градијенту, а при поређењу информација изворне и тест слике користи се мера слична индексу структурне сличности.

Поред наведених мера коришћене су још и ADM (*Additive Impairments and Detail Losses Metric*) [11], MAD (*Most Apparent Distortion*) [12, 13], VSI (*Visual Saliency-Induced Index*) [14] и мера заснована на



очувању визуелних информација – VIF (*Visual Information Fidelity*) [15]. Поред VIF мере дати су и резултати њене поједностављене верзије VIFp.

У остатку рада извршена је анализа перформанси мера за објективну процену квалитета слике, где је у другом поглављу дат опис базе слика са вишеструким дисторзијама. Резултати тестирања и најзначајнији закључци дати су у трећем и четвртном поглављу рада.

## 2. ОПИС КОРИШЋЕНЕ БАЗЕ СЛИКА

База слика је развијена у LIVE лабораторији (*Laboratory of Image and Video Engineering*) Универзитета у Тексасу (*University of Texas at Austin*) [16]. Изведена је на основу 15 изворних слика високог квалитета, резолуције 1280x720 пиксела. Сlike су одабране тако да обухватају широк спектар садржаја, боја и нивоа осветљаја. Коришћена су три типа дисторзија за генерисање базе слика и то замрљање (*blurring*), JPEG компресија и адитивни Гаусов шум.

У бази се симулирају два реална сценарија деградација слика. Први сценарио је складиштење слика, где су слике најпре замрљане, а након тога и компримоване JPEG типом компресије. Други сценарио представља снимање слике апаратом, где су слике најпре замрљане и у такве слике је додат бели Гаусов шум како би се симулирао шум сензора. Ова два сценарија су организована кроз две студије.

Коришћена су четири нивоа сваког типа дисторзије означених од 0 до 3, где 0 означава непостојање

дисторзије, док 3 означава највиши степен дисторзије. Сlike су креиране тако што су комбиновани нивои дисторзија и на тај начин је комплетирана база слика. Тако се од 15 референтних слика, за једну студију, генерише 240 слика, од чега је 135 слика са две дисторзије, а по 45 слика је са једноструком дисторзијом. С обзиром да постоји случај да су обе дисторзије означене степеном 0, преосталих 15 слика су идентичне изворним сликама. У другој студији слике се генеришу на исти начин, али уз различите деградације. Укупан број слика на којима је вршено субјективно тестирање је 450, по 225 у обе студије. Због начина креирања слика у бази (студијама), јављају се идентичне слике у ситуацији када је замрљање једина деградација примењена на сликама. Из тог разлога база се састоји од 405 деградираних слика.

У евалуацији квалитета је учествовало 37 посматрача, у првој студији 19, а у другој 18.

На слици 1 приказана је изворна слика LIVE базе слика са вишеструким дисторзијама и три њене деградираних верзије. За деградираних слике заједничко је замрљање другог нивоа. Замрљана слика другог нивоа (слика 1(б)) је додатно деградирана адитивним Гаусовим шумом највишег, трећег степена (слика 1(в)), односно компресијом највишег, трећег степена (слика 1(г)). Субјективне импресије квалитета дате су кроз вредности DMOS (*Differential Mean Opinion Score*) скорова (ниже DMOS вредности одговарају бољем квалитету слике).



(а) изворна слика

(б) замрљање=2; DMOS=43.63



(в) замрљање=2, шум=3; DMOS=50.28

(г) замрљање=2, JPEG=3; DMOS=52.42

Слика 1. Изворна слика LIVE базе и њене три деградираних верзије

Са слике 1 се уочава разлика у квалитету тест слика, а што су уочили и посматрачи. По њиховом мишљењу најбољи квалитет има слика са једноструком дисторзијом (DMOS=43.63). Сlike са вишеструким дисторзијама су по мишљењу посматрача приближно истог квалитета (DMOS=50.28 и DMOS=52.42), а који је лошији од квалитета слике са једноструком дисторзијом.

### 3. АНАЛИЗА ПЕРФОРМАНСИ ОБЈЕКТИВНИХ МЕРА ПРОЦЕНЕ КВАЛИТЕТА

Степен слагања субјективних и објективних скорова квалитета одређен је помоћу линеарне корелације (*Pearson Linear Correlation Coefficient, PLCC*) и корелације рангова (*Spearman Rank Order Correlation Coefficient, SROCC*).

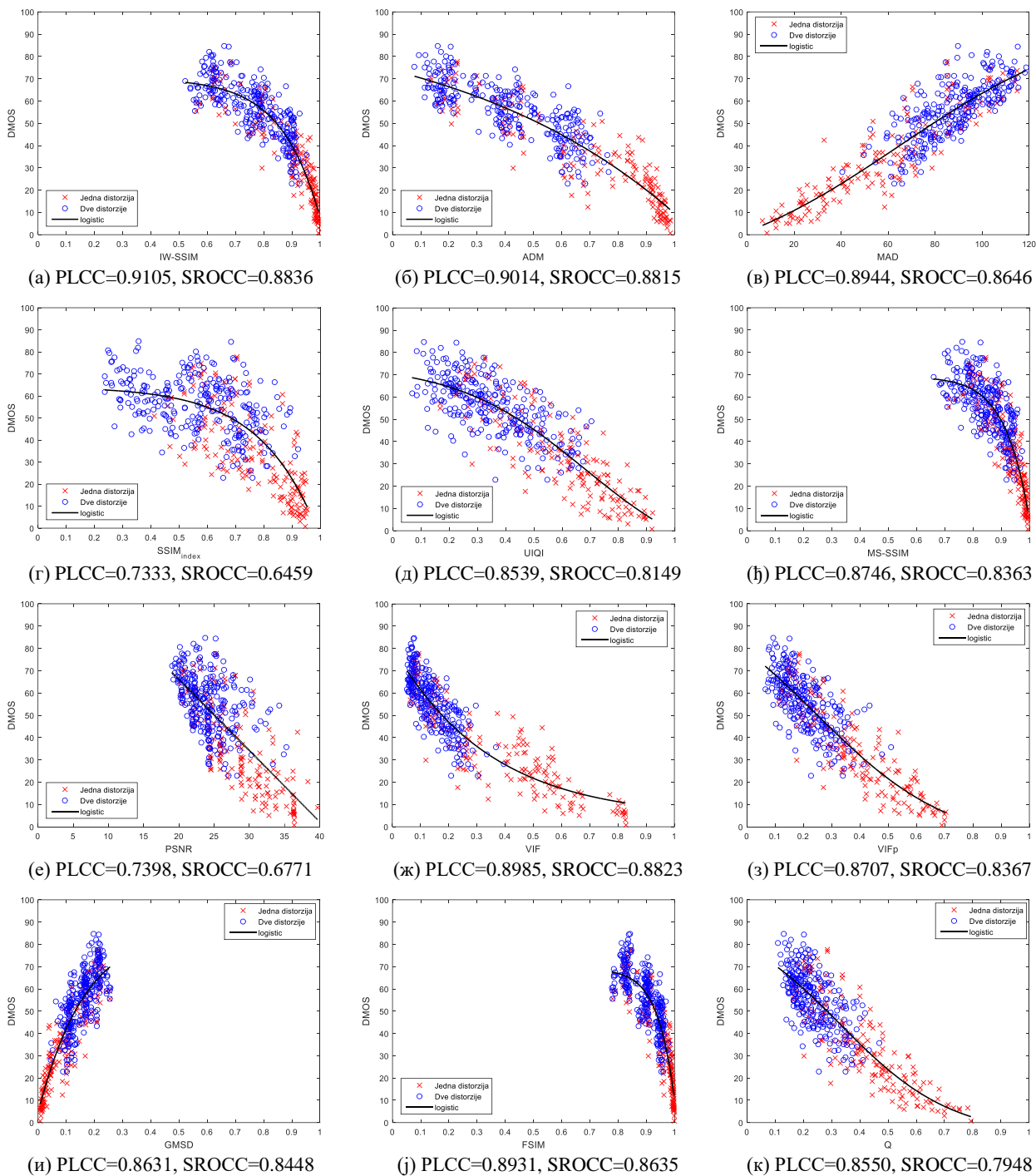
Табела 1 – Коefицијенти линеарне корелације субјективних и објективних скорова квалитета на LIVE бази

Редни број	PLCC	Замрљање	JPEG	Замрљање + JPEG	Студија 1	Замрљање	Гаусов шум	Замрљање + Гаусов шум	Студија 2	Једна дисторзија	Две дисторзије	Цела база
1.	PSNR	0.5269	0.0573	0.4227	0.7272	0.5288	0.9168	0.5358	0.7741	0.7937	0.4691	0.7398
2.	UIQI	0.7676	0.6137	0.7454	0.8847	0.7842	0.8571	0.7288	0.8578	0.8581	0.6822	0.8539
3.	SSIM <sub>index</sub>	0.7110	0.3251	0.5609	0.7990	0.7209	<b>0.9436</b>	0.6072	0.7697	0.7499	0.4280	0.7333
4.	SSIM	0.7932	0.5499	0.7168	0.8969	0.8184	0.9195	0.7898	0.8962	0.9076	0.7416	0.8914
5.	MS-SSIM	0.7734	0.5103	0.6968	0.8873	0.7962	0.9334	0.7735	0.8913	0.8967	0.6986	0.8746
6.	IW-SSIM	<b>0.8419</b>	0.6408	0.7713	0.9162	<b>0.8643</b>	0.9382	<b>0.8262</b>	<b>0.9111</b>	<b>0.9224</b>	<b>0.7899</b>	<b>0.9105</b>
7.	FSIM	0.8066	0.6866	0.7469	0.9063	0.8399	0.9294	0.7811	0.8801	0.9014	0.7606	0.8931
8.	FSIMc	0.8066	0.7065	0.7461	0.9070	0.8400	0.9298	0.7873	0.8864	0.9064	0.7633	0.8963
9.	GMSD	0.7741	0.6265	0.6992	0.8747	0.8046	0.9195	0.7102	0.8518	0.8997	0.6996	0.8631
10.	GMSM	0.7553	0.6721	0.6838	0.8868	0.7831	0.9417	0.7386	0.8708	0.9008	0.7053	0.8774
11.	Q	0.6848	0.6459	0.6623	0.8755	0.6958	0.9182	0.7570	0.8660	0.8676	0.6423	0.8550
12.	Q <sub>w1</sub>	0.7203	0.5705	0.6816	0.8837	0.7373	0.9223	0.7941	0.8795	0.8868	0.7037	0.8751
13.	Q <sub>w2</sub>	0.7186	0.5624	0.6825	0.8825	0.7376	0.9219	0.7840	0.8805	0.8861	0.6807	0.8705
14.	GSM	0.6757	<b>0.7504</b>	0.7065	0.7541	0.7128	0.8752	0.6539	0.7455	0.8003	0.6411	0.7497
15.	ADM	0.8297	0.7310	0.7726	0.9132	0.8557	0.9302	0.8164	0.8913	0.9024	0.7893	0.9014
16.	VIF	0.8372	0.6652	0.7754	0.9189	0.8526	0.9272	0.7996	0.8804	0.8955	0.7836	0.8985
17.	VIFp	0.7594	0.3736	0.7122	0.8800	0.7720	0.9177	0.7659	0.8844	0.8881	0.6921	0.8707
18.	MAD	0.7194	0.6465	<b>0.8175</b>	<b>0.9197</b>	0.7543	0.9367	0.7205	0.8684	0.9023	0.7559	0.8944
19.	VSI	0.7693	0.6091	0.6742	0.8815	0.8021	0.8714	0.7507	0.7591	0.9032	0.7081	0.7441

Табела 2 – Коefицијенти корелације рангова субјективних и објективних скорова квалитета на LIVE бази

Редни број	SROCC	Замрљање	JPEG	Замрљање + JPEG	Студија 1	Замрљање	Гаусов шум	Замрљање + Гаусов шум	Студија 2	Једна дисторзија	Две дисторзије	Цела база
1.	PSNR	0.4883	0.1100	0.3868	0.6621	0.4810	0.8194	0.5193	0.7088	0.8039	0.4469	0.6771
2.	UIQI	0.7462	0.5615	0.7347	0.8533	0.7771	0.8331	0.6984	0.8215	0.8613	0.6697	0.8149
3.	SSIM <sub>index</sub>	0.7272	0.3636	0.5535	0.7443	0.7083	0.9007	0.5656	0.7022	0.7607	0.4186	0.6459
4.	SSIM	0.7606	0.5295	0.6968	0.8488	0.7901	0.8769	0.7836	0.8760	0.9102	0.7381	0.8604
5.	MS-SSIM	0.7596	0.5450	0.6844	0.8399	0.7857	0.8933	0.7614	0.8629	0.9061	0.6941	0.8363
6.	IW-SSIM	0.7917	0.6137	0.7389	0.8700	0.8185	0.8894	0.8175	<b>0.8933</b>	<b>0.9220</b>	0.7804	<b>0.8836</b>
7.	FSIM	0.7620	0.6947	0.7052	0.8544	0.7965	0.8690	0.7776	0.8642	0.9081	0.7465	0.8635
8.	FSIMc	0.7594	0.7184	0.7066	0.8556	0.7947	0.8671	0.7850	0.8691	0.9095	0.7517	0.8665
9.	GMSD	0.7725	0.6577	0.6989	0.8470	0.8092	<b>0.9048</b>	0.7291	0.8366	0.9152	0.7144	0.8448
10.	GMSM	0.7440	0.6828	0.6627	0.8305	0.7652	0.9043	0.7354	0.8429	0.9119	0.6980	0.8378
11.	Q	0.6544	0.6124	0.6456	0.8123	0.6783	0.8842	0.7188	0.8214	0.8788	0.6240	0.7948
12.	Q <sub>w1</sub>	0.6936	0.5729	0.6741	0.8286	0.7177	0.8708	0.7845	0.8578	0.8924	0.7042	0.8355
13.	Q <sub>w2</sub>	0.6792	0.5621	0.6716	0.8275	0.7053	0.8806	0.7600	0.8479	0.8923	0.6720	0.8224
14.	GSM	0.7484	0.7277	0.6892	0.8441	0.7719	0.9001	0.7348	0.8395	0.9086	0.7152	0.8454
15.	ADM	<b>0.8066</b>	<b>0.7414</b>	0.7486	0.8713	<b>0.8330</b>	0.8982	<b>0.8235</b>	0.8878	0.9152	<b>0.7883</b>	0.8815
16.	VIF	0.7836	0.6934	0.7566	0.8788	0.8180	0.8601	0.7928	0.8806	0.8963	0.7793	0.8823
17.	VIFp	0.7485	0.3655	0.7099	0.8452	0.7738	0.8315	0.7464	0.8541	0.8911	0.6919	0.8367
18.	MAD	0.7623	0.7046	<b>0.8220</b>	<b>0.8906</b>	0.6729	0.8798	0.7232	0.8376	0.9096	0.7618	0.8646
19.	VSI	0.7445	0.7191	0.6570	0.8300	0.7695	0.8733	0.7467	0.8509	0.9061	0.7045	0.8413





Слика 2. Дијаграми расипања субјективних и објективних скорова квалитета на LIVE бази

У табели 1 дате су перформансе објективних мера добијене помоћу линеарне корелације. Осенчени резултати представљају најбољи резултат за одређени подскуп слика, односно за целу базу. Уочава се да мера IW-SSIM има највећи степен слагања са субјективним скоровима у највећем броју случајева (подскупова), док PSNR има најнижи степен корелације на највећем броју подскупова.

За случај када се јављају две дисторзије, мера IW-SSIM има најбоље перформансе. Најбоље перформансе има и у случају комбинације замрљања и Гаусовог шума, док за комбинацију замрљања и JPEG компресије има висок степен корелације у

односу на остале тестиране мере – за овај подскуп слика мера MAD даје најбоље резултате.

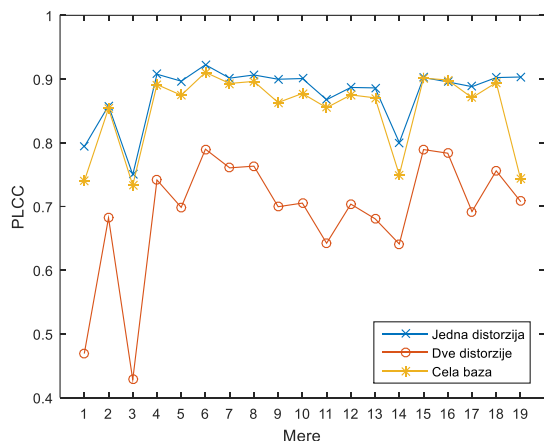
У табели 2 дате су перформансе објективних мера добијене помоћу корелације рангова. Најбоље перформансе на читавој бази слика има IW-SSIM мера. За подскуп слика са вишеструким дисторзијама мера ADM је остварила најбоље резултате (IW-SSIM је на другом месту).

Лоше резултате, поред PSNR, даје SSIM<sub>index</sub> и то за сва три подскупа слика са вишеструким дисторзијама. Ове две мере имају најлошије перформансе и на читавој бази слика (табеле 1 и 2). PSNR и SSIM<sub>index</sub>

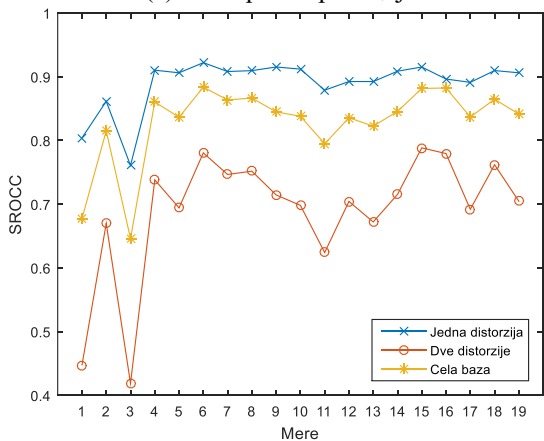
имају боље перформансе на појединачним студијама, где се приближавају коефицијенту корелације за слике са једноструком дисторзијом.

Дијаграми расипања субјективних и неких од објективних мера процене квалитета слике дати су на слици 2 (свака тачка представља једну тест слику). На дијаграмима су различитим симболима обележене тест слике са једноструком и вишеструком дисторзијом. На дијаграмима се уочава да је расипање скорова око логистичке (интерполационе) криве значајно веће за слике са две дисторзије него за слике са једноструком дисторзијом. Ефекат расипања је најизраженији за  $SSIM_{index}$  (слика 2(г)). Такође, на свим дијаграмима расипања уочава се да су посматрачи значајно лошије оцене давали сликама са вишеструким деградацијама у односу на једноструке.

Илустрације на слици 3 приказују односе коефицијената корелација субјективних и објективних скорова квалитета за слике са једноструком дисторзијом, двоструком дисторзијом и комплетном базом (редни бројеви на слици 3 одговарају редним бројевима објективних мера из табела 1 и 2). Слика 3(а) приказује однос коефицијената линеарне корелације, а слика 3(б) однос коефицијената корелације рангова.



(а) линеарна корелација



(б) корелација рангова

Слика 3. Степен слагања субјективних и објективних скорова квалитета на подскуповима слика са једном, две дисторзије и на комплетној LIVE бази слика

На слици се уочава да све мере имају боље перформансе за слике са једноструким дисторзијама, у односу на слике са двоструким дисторзијама и у односу на комплетну базу слика. Резултати добијени за целу базу се налазе између резултата добијених за слике са једном и две деградације, при чему су перформансе на глобалном плану (комплетној бази) ближе перформансама за подскуп слика са једноструком дисторзијом. Слике са једноструком дисторзијом значајно утичу на резултате добијене на комплетној бази, а због значајног проширења динамичког опсега квалитета субјективних и објективних скорова.

Разлике у перформансама објективних мера процене квалитета постају израженије (већа је варијација корелација) у случају присуства више дисторзија, односно, степен квалитета слика са вишеструком дисторзијом се боље естимира коришћењем објективних мера са редним бројевима 6 (IW-SSIM), 15 (ADM) и 16 (VIF).

Степен слагања субјективних и објективних скорова квалитета на подскупу слика са две дисторзије је мањи од 80%, а што је значајно ниже од степена слагања на базама слика са једноструком дисторзијом (LIVE, CSIQ, TID, IVC, Тоуама, ...), где је степен слагања субјективних и објективних скорова квалитета и преко 95%.

#### 4. ЗАКЉУЧАК

Анализа перформанси објективних мера процене квалитета слике показала је да све мере имају нижи степен слагања са субјективним скоровима у случају присуства вишеструких деградација него у случају присуства једноструких деградација. Већина тестираних мера има коефицијент корелације у опсегу од 80% до 90% на комплетној бази, а на сликама са две дисторзије у опсегу од 60% до 80%. Резултати говоре да постоји доста простора за унапређење објективних мера процене квалитета у случају присуства вишеструких деградација, односно присуство вишеструких деградација представља изазов у процени квалитета слике.

У оквиру анализираних базе слика присутне су тест слике са две дисторзије, па је у даљем раду потребно анализирати перформансе објективних мера са више од два типа деградације. Од посебног интереса је пронаћи међусобни утицај различитих типова деградације.

Такође, у даљем раду планира се развој објективне мере процене квалитета слика са вишеструком дисторзијом.

#### НАПОМЕНА

Ово истраживање је део пројекта ВА-ТТ/1-17-19, подржаног од стране Министарства одбране Републике Србије.

## ЛИТЕРАТУРА

- [1] Chandler, D.M., "Seven challenges in image quality assessment: past, present, and future research." *ISRN Signal Processing*, Article ID 905685, pp. 1-53, 2013.
- [2] Wang, Z. and Bovik, A.C., "A universal image quality index." *IEEE Signal Processing Letters*, Vol. 9, No. 3, pp. 81-84, March 2002.
- [3] Wang, Z., Bovik, A.C., Sheikh, H.R. and Simoncelli, E.P., "Image quality assessment: from error visibility to structural similarity." *IEEE Transactions on Image Processing*, Vol. 13, No. 4, pp. 600-612, 2004.
- [4] Wang, Z., Simoncelli, E.P. and Bovik, A.C., "Multiscale structural similarity for image quality assessment." *Conference Record of the 37<sup>th</sup> Asilomar Conference on Signals, Systems and Computers*, pp. 1398-1402, November 2004.
- [5] Wang, Z. and Li, Q., "Information content weighting for perceptual image quality assessment." *IEEE Transactions on Image Processing*, Vol. 20, No. 5, pp. 1185-1198, 2011.
- [6] Zhang, L., Zhang, L., Mou, X. and Zhang, D., "FSIM: A feature similarity index for image quality assessment." *IEEE Transactions on Image Processing*, Vol. 20, No. 8, pp. 2378-2386, 2011.
- [7] Xue, W., Zhang, L., Mou, X. and Bovik, A.C., "Gradient magnitude similarity deviation: A highly efficient perceptual image quality index." *IEEE Transactions on Image Processing*, Vol. 23, No. 2, pp. 684-695, 2014.
- [8] Bondzulić, B. and Petrović, V., "Edge-based objective evaluation of image quality." *18th IEEE International Conference on Image Processing*, pp. 3305-3308, 2011.
- [9] Бонцулић, Б., Петровић, В., Антонић, М., "Увод у објективну процену квалитета слике." *XVII научна и бизнис конференција YUINFO 2011*, Зборник радова, стр. 389-394, 2011.
- [10] Liu, A., Lin, W. and Narwaria, M., "Image quality assessment based on gradient similarity." *IEEE Transactions on Image Processing*, Vol. 21, No. 4, pp. 1500-1512, 2012.
- [11] Li, S., Zhang, F., Ma, L. and Ngan, K.N., "Image quality assessment by separately evaluating detail losses and additive impairments." *IEEE Transactions on Multimedia*, Vol. 13, No. 5, pp. 935-949, 2011.
- [12] Larson, E.C. and Chandler, D.M., "Most apparent distortion: A dual strategy for full-reference image quality assessment." *International Society for Optics and Photonics*, Vol. 7242, pp. 72420S, January 2009.
- [13] Larson, E.C. and Chandler, D.M., "Most apparent distortion: Full-reference image quality assessment and the role of strategy." *Journal of Electronic Imaging*, Vol. 19, No. 1, Article ID 011006, 2010.
- [14] Zhang, L., Shen, Y. and Li, H., "VSI: A visual saliency-induced index for perceptual image quality assessment." *IEEE Transactions on Image Processing*, Vol. 23, No. 10, pp. 4270-4281, 2014.
- [15] Sheikh, H.R. and Bovik, A.C., "Image information and visual quality." *IEEE Transactions on Image Processing*, Vol. 15, No. 2, pp. 430-444, 2006.
- [16] Jayaraman, D., Mittal, A., Moorthy, A.K. and Bovik, A.C., "Objective quality assessment of multiply distorted images." *Conference Record of the 46<sup>th</sup> Asilomar Conference on Signals, Systems and Computers*, pp. 1693-1697, November 2012.

# ZNAČAJ UPRAVLJANJA DOKUMENTIMA U MO I VS I DOSTIGNUTI STEPEN RAZVOJA

## IMPORTANCE OF DOCUMENT MANAGEMENT IN MoD AND SAF AND ACHIEVED DEGREE OF DEVELOPMENT

Dejan Milenković<sup>1</sup>, Dejan Kršljanin<sup>1</sup>

*Generalštab Vojske Srbije, Uprava za telekomunikacije i informatiku<sup>1</sup>*

**Sadržaj** – Neophodnost unapređivanja poslovanja i prilagođavanja trendovima savremenog digitalnog sveta zahteva sve veću primenu tehnologija upravljanja dokumentima. Adekvatnim planiranjem i postavljanjem zahteva i uslova za uvođenje naprednih informacionih tehnologija može se doprineti znatno efikasnijoj realizaciji aktivnosti poslovnih procesa na svim nivoima upravljanja.

Implementacija sistema za upravljanje dokumentacijom u okviru poslovnih organizacija, naročito onih sa velikim brojem zaposlenih, velikim brojem dislociranih poslovnih jedinica i velikom količinom poslovne dokumentacije, treba da bude prioritet. U ovom radu akcenat je na prikazu dostignutog stepena razvoja upravljanja dokumentima u Ministarstvu odbrane (MO) i Vojski Srbije (VS).

**Abstract** - The necessity of improving performance and adapting to the modern trends of the digital world requires greater application of document management technology. Adequate planning and setting the requirements and conditions for the introduction of advanced information technologies can make significant contributions to a more efficient implementation of the activities of business processes at all levels of governance.

Implementation of systems for document management in business organizations, especially those with a large number of employees, a large number of remote business units, and a large amount of business documents, should be a priority. In this paper, the emphasis is on the presentation of the achieved level of development of document management in the Ministry of Defense (MoD) and the Serbia Armed Forces (SAF).

### 1. UVOD

Polazeći od činjenice da upotreba elektronskih sadržaja predstavlja imperativ današnjeg vremena, kao i od opšteg stava da se primenom savremenih informacionih tehnologija može uspostaviti rešenje za pouzdano i jednostavno organizovanje i sistematizaciju dokumentacije, zaključujemo da uspeh svake poslovne organizacije, pa tako i vojne organizacije, direktno zavisi od dostignutog stepena upravljanja informacijama sadržanim u dokumentaciji.

Imajući u vidu da su za procese donošenja odluka, naročito u kritičnim momentima, više nego potrebni pravovremeni, tačni, proverljivi, lako dostupni i

konzistentni podaci, osnovni problem upotrebe tih podataka nije njihovo postojanje, već mesto i način na koji su ti podaci smešteni i organizovani u distribuiranim sistemima i na koji način se njima upravlja.

### 2. ZNAČAJ UPRAVLJANJA DOKUMENTIMA U PROCESIMA UPRAVLJANJA INFORMACIJAMA

Razvoj informaciono-komunikacionih tehnologija uslovljava prilagođavanje poslovanja organizacija kako bi na tržištima bile konkurentne i kompatibilne, sa neprekidnim ciljem da budu bolje i efikasnije. U svim tržišnim utakmicama savremenog sveta, obavijenim informaciono-komunikacionim tehnologijama, informacija ima presudnu ulogu u njihovim konačnim ishodima. Slična situacija je i sa poslovnim organizacijama u kojima su pravovremeno dobijanje informacija i njihova obrada presudni za ostvarivanje prednosti na tržištu [1].

Savremeni menadžment ima sve manje vremena za donošenje odluka o aktivnostima svojih poslovnih procesa. Opterećen je velikim brojem podataka koje je potrebno obraditi i preneti. U prednosti je poslovna organizacija koja odluke o svojim aktivnostima donosi na osnovu pravovremenih, pouzdanih, tačnih, proverljivih, lako dostupnih i konzistentnih podataka.

Uspešnost savremenih poslovnih organizacija u velikoj meri oblikuje način korišćenja informacija koje predstavljaju bitan faktor upravljanja poslovnim procesima. Informacije se ispoljavaju kao znanje i potreba za uspešno rukovođenje na svim nivoima, što smanjuje neizvesnost u delatnostima poslovne organizacije, omogućava uštedu materijalnih resursa i racionalno angažovanje kadrovskih kapaciteta. U realizaciji poslovnih procesa izražena je potreba podele i korišćenja informacija između poslovnih jedinica, a u zavisnosti od dostupnosti, tačnosti i pravovremenosti, informacija može da utiče na ubrzavanje ili usporavanje izvršenja pojedinih aktivnosti.

Povezivanje poslovnih jedinica putem informaciono-komunikacionih tehnologija pruža mogućnost sveobuhvatnog pristupa relevantnim podacima, omogućava međusobnu koordinaciju, objedinjavanje, dostavljanje, analizu i prikazivanje informacija, što sve zajedno doprinosi da se ključne odluke donose pravovremeno i kvalitetno. Jedan od ciljeva poslovnih organizacija je promena svesti zaposlenih da rad sa

papirnim primercima dokumenata ne predstavlja pouzdan i brz način dolaska do aktuelnih informacija. Naprotiv, dokumenta u papirnom obliku su podložna gubljenju, izmenama i uništenju, zahtevaju više vremena za pronalaženje i upotrebu informacija iz njihovog sadržaja. Velike poslovne organizacije zahtevaju dobar i pouzdan sistem za skladištenje i organizaciju dokumenata. Spora administracija, gubljenje podataka i dokumenata, arhiviranje i drugi problemi sa kojima se suočava svaka poslovna organizacija, a naročito veliki i organizacijski distribuirani poslovni sistemi, upravo dovode do usporavanja njegove operabilnosti i opterećuju ljudske potencijale.

Imajući u vidu da poslovna dokumentacija uglavnom nastaje na računarima, upravljanje elektronskom dokumentacijom primenom savremenih informaciono-komunikacionih tehnologija predstavlja rešenje za njeno pouzdano, brzo i jednostavno organizovanje i sistematizaciju. Upotreba sistema za upravljanje elektronskom dokumentacijom ima za cilj rešavanje problema upravljanja strukturnim i nestrukturnim tipovima informacija, njihovog arhiviranja i ponovnog korišćenja. Takođe, doprinosi da komunikacija i interoperabilnost između poslovnih organizacija na regionalnom i globalnom nivou bude na visokom nivou.

### **3. EDMS - EFIKASNO REŠENJE UPRAVLJANJA DOKUMENTIMA**

Problemi u radu sa dokumentacijom u poslovnim organizacijama su mnogobrojni. Dokumentacija se izrađuje u elektronskoj formi, ali se nakon toga štampa i razmenjuje u papirnoj, što znatno usporava razmenu informacija sadržanih u dokumentaciji i povećava troškove. Procedura toka dokumentacije od izrade dokumenata, potpisivanja, distribucije i postupanja po njima ne samo što je dugotrajna već i postoji mogućnost da se izgubi [1]. To doprinosi neracionalnom trošenju vremenskih i kadrovskih resursa u pronalaženju potrebne dokumentacije, otežanom izvršavanju postavljenih zadataka i neefikasnom donošenju poslovnih odluka. Konačno, procedura arhiviranja i ponovni pristup dokumentaciji otežani su i zahtevaju vremenske i kadrovske resurse, dok je kontrola pristupa dokumentaciji, naročito poverljivoj, zastarela i nedovoljno efikasna.

Rešenje za pouzdano, brzo i jednostavno organizovanje i sistematizaciju poslovne dokumentacije jeste upravljanje elektronskom dokumentacijom primenom savremenih tehnoloških rešenja. Rezultati efikasnog upravljanja elektronskom dokumentacijom su povećanje raspoloživosti dokumenata za korisnike, unapređenje kontrole pristupa informacijama sadržanih u dokumentaciji, kao i efikasnije i ekonomičnije poslovanje. [2]

U organizacijama čije su poslovne funkcije razgranate i deluju na više distribuiranih lokacija, efikasno nadgledanje i upravljanje procesima, u skladu sa poslovnim zahtevima i standardima, još uvek predstavlja

jedan od najvećih organizacionih izazova. Sistemi za upravljanje (elektronskom) dokumentacijom (Electronic Document Management Systems – EDMS), predstavljaju kategoriju informacionih sistema specijalizovanih za upravljanje dokumentima i njihovim metapodacima u svim fazama životnog ciklusa dokumenta isključivo u elektronskom okruženju [3]. EDMS obezbeđuju sistematsko rešenje za unos, organizaciju, upravljanje i skladištenje sadržaja unutar poslovnog okruženja. Njihovim korišćenjem, nestrukturnim informacijama sadržanim u dokumentaciji upravlja se u skladu sa predefinisanim poslovnim pravilima i procedurama. Adekvatnim upravljanjem metapodacima dokumenata kroz EDMS moguće je istu informaciju sadržanu u dokumentima koristiti u različitim poslovnim kontekstima, što je česta poslovna potreba. Takođe, EDMS obezbeđuje upravljanje korisnicima.

Uspostavljanjem sistema za upravljanje elektronskom dokumentacijom poslovna organizacija postiže sledeće rezultate:

- efikasnije realizuje svoje zadatke i uspešnije ostvaruje poslovne ciljeve;
- operabilnost u komunikacijama na poslovnom tržištu podiže se na viši nivo;
- planiranje zadataka i izveštavanje o njihovoj realizaciji je kvalitetnije, ekonomičnije i efikasnije;
- automatizacijom upravljanja dokumentacijom poslovnih i radnih procesa skraćuje se vreme njihove realizacije i utiče se na efikasnije donošenje poslovnih odluka;
- informacije sadržane u dokumentaciji dostupne su u skoro realnom vremenu;
- relevantnoj dokumentaciji pristupa se sa udaljenih (distribuiranih) lokacija;
- povećava se efikasnost kadrovskih resursa, čime se smanjuju troškovi za radno osoblje;
- redukuje se trošenje vremenskih i materijalnih resursa (prostorni zahtevi za arhivu, telefaks, papir, uređaji za kopiranje, održavanje opreme za kancelarijsko poslovanje);
- ostvaruje se centralizovano automatsko skladištenje i upravljanje dokumentacijom i onemogućeno je multipliciranje dokumenata;
- obezbeđuje se visoki stepen kontrole pristupa i sigurnosti elektronskog sadržaja i elektronske arhive;
- preventivno delovanje i blagovremeno otkrivanje slučajeva zloupotrebe pristupa dokumentaciji;
- standardizacija forme dokumenata;
- unapređenje kulture upravljanja informacijama u okviru poslovne organizacije.

### **4. PROCESI AUTOMATIZACIJE U MO I VS PRIMENOM EDMS**

Sistem za upravljanje elektronskom dokumentacijom predstavlja automatizaciju procesa za upravljanje dokumentacijom i procesa komunikacije koji se realizuju u okviru MO i VS. Globalni procesi upravljanja dokumentima su:

- upravljanje dokumentima unutar konkretne organizacijske jedinice MO i VS;



- upravljanje dokumentima između svih organizacijskih jedinica MO i VS;
- upravljanje dokumentima između MO i VS i subjekata iz spoljnog okruženja;
- upravljanje elektronskim kopijama papirnih dokumenata nastalih unutar ili izvan MO i VS;
- upravljanje sigurnosnim kopijama elektronske dokumentacije, podacima o realizovanim transakcijama prepiske i metapodacima dokumenata (*backUp/Recovery system*).

Navedeni procesi su složeni i sastoje se od podprocesa:

- upravljanje fazama životnog ciklusa dokumenta, kao i o njegovim statusima;
- upravljanje metapodacima dokumenta (a naročito priložima i primaocima svakog od dokumenata);
- upravljanje ulogama i pravima pristupa nad dokumentima i procedurama kolaboracije;
- upravljanje procesima prevođenja papirnih dokumenata u elektronski oblik nastalih iz okvira specifičnih radnih procesa jedinica MO i VS ili primljenih iz spoljnog okruženja (digitalizacija);
- skladištenje dokumenata na repozitorijum podataka poslovne jedinice;
- evidentiranje i upravljanje svim aktivnostima korisnika EDMS (pristup sistemu i akcije nad dokumentima);
- upravljanje aktivnostima administriranja (korisnici, uloge, prava pristupa); i
- generisanje izveštaja koji se odnose na statuse dokumenata, aktivnosti korisnika, obim obrađene dokumentacije, analiza (ne)realizovanih zadataka.

Podproces backUp/Recovery sistema imaju specifičan za cilj obezbeđivanja sigurnog i pouzdanog upravljanja sigurnosnim kopijama elektronskih dokumenata, podacima o realizovanim transakcijama prepiske, relevantnim metapodacima i deduplikacijom podataka na svim nivoima skladištenja

## 5. STEPEN DOSTIGNUTOG NIVOA REALIZACIJE REŠENJA EDMS U MO I VS

Zbog nedostatka finansijskih sredstava za realizaciju kompletnog projekta EDMS u okviru Ministarstva odbrane i Vojske Srbije (u daljem tekstu: MO i VS), 2011. godine je uspostavljen *Servis za razmenu elektronski potpisanih dokumenata*. Ovaj Servis predstavlja način razmene dokumenata u okviru kancelarijskog poslovanja MO i VS i zasniva se na primeni elektronskog identifikacionog dokumenta kao nosača elektronskog sertifikata za sprovođenje postupka elektronskog potpisivanja i upotrebu sistemskog servisa za razmenu elektronske pošte [4]. Prilikom uspostavljanja Servisa identifikovani su i problemi koji su se pre svega ogledali u [5]:

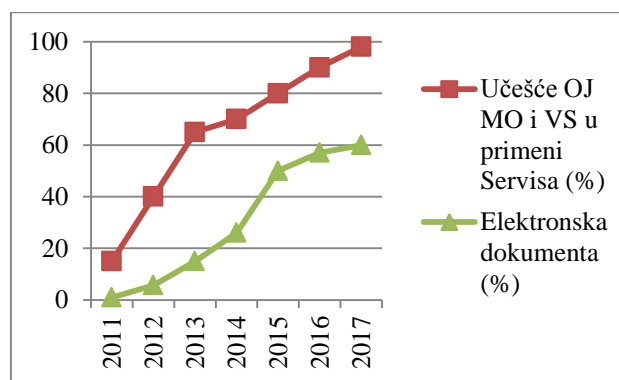
- prilagođavanju zaposlenih na nov način rada sa elektronskim dokumentima i
- nepoverljivosti zaposlenih prema tehnologiji elektronskog potpisa i servisu elektronskog potpisivanja.

U tabeli 1 je predstavljena dinamika širenja upotrebe Servisa postepenim prevazilaženjem navedenih problema izražena kroz:

- procenat organizacionih jedinica koje su vremenom pristupale upotrebi Servisa i
- procenat od ukupnog broja dokumenata koje su sve jedinice razmenjivale elektronskim putem primenom Servisa..

**Tabela 1:** Dinamika uvođenja servisa sa efektima primene

Godina	Učešće OJ MO i VS u primeni Servisa (%)	Elektronska dokumenta (%)
2011	15	< 1
2012	40	5,7
2013	65	15
2014	70	26
2015	80	50
2016	90	57
2017	98	60



Slika 1. Grafički prikaz rezultata iz Tabele 1

Na slici 1 se uočava očigledan trend povećanja broja elektronski potpisanih i razmenjenih dokumenata u MO i VS ali samo do određenog nivoa, iako je gotovo kompletna organizacijska struktura MO i VS (98%) „prihvatila“ savremene načine razmene dokumenata. Međutim, iako u poslednjim godinama (2016. i 2017.) gotovo sve organizacione jedinice MO i VS koriste Servis, broj elektronski potpisanih i razmenjenih dokumenata se ne povećava srazmerno broju novopriključenih jedinica. Razlozi tome su nepostojanje automatizacije većine procesa bitnih za upravljanje dokumentima, a sam Servis je postao usko grlo u obradi dokumenata.

## 6. ZAKLJUČAK

Budući da je pravovremeno dobijanje kvalitetnih informacija bitno za ostvarenje prednosti nad konkurencijom, poslovna organizacija ih mora dobiti u skoro realnom vremenu i u obliku koji je u datom momentu najjednostavniji za njihovo praćenje i razumevanje. Iz toga proizlazi da se od informacionih sistema poslovnih organizacija očekuje da obezbede informacije čiji sadržaj, brzina pristupa i način prikaza odgovaraju trenutnim potrebama u procesu odlučivanja.

Na primeru MO i VS, primena Servisa za razmenu elektronski potpisanih dokumenata je postala usko grlo u procesima razmene informacija (sadržanih u dokumentima službene prepiske). Ta činjenica se svakako negativno odražava na funkcionisanje sistema, ali isto tako može da deluje i pozitivno na dalji razvoj upravljanja informacijama. Sa jedne strane predstavlja kritičnu tačku u funkcionisanju sistema, jer je sistem brzu i efikasnu razmenu informacija elektronskim putem „usvojio kao nešto što se podrazumeva i ne dovodi se u pitanje“. Sa druge strane taj kritični momenat doprinosi podsticanju rukovodilaca da aktivnije i ozbiljnije razmišljaju u smeru unapređivanja elektronskog poslovanja u MO i VS investiranjem u informacione tehnologije.

## LITERATURA

- [1] Milenković D., Upravljanje dokumentacijom u poslovnim organizacijama, Zadužbina Andrejević, Beograd, 2015.
- [2] Cameron S. A., Enterprise content management – a business and technical guide. The Chartered Institute for IT, Swindon, UK, 2011.
- [3] Milenković D., Statističko upravljanje repozitorijumima elektronskih dokumenata primenom koeficijenata preferencije, doktorska disertacija, Fakultet organizacionih nauka, Beograd, 2013.
- [4] Azad A., Implementing Electronic Document and Record Management Systems, Hardcover, 2007.
- [5] Milenković D., Đorđević I., Jovanović-Milenković M., Razmena elektronski potpisanih dokumenata u Ministarstvu odbrane i Vojsci Srbije, XLI simpozijum o operacionim istraživanjima SYM-OP-IS 2014, str. 37–41, Divčibare, 2014.

# ANALIZA MOGUĆNOSTI PRIMENE KROS-KORELACIJE U VERIFIKACIJI KORISNIKA NA OSNOVU OTISKA PRSTA

## ANALYSIS OF THE POSSIBILITY OF CROSS-CORRELATION APPLICATION IN USER VERIFICATION BASED ON THE FINGERPRINT

Lazar Đorđević, Lazar Stevanović, Boban Bondžulić, Ivan Tot, Mladen Trikoš  
*Vojna akademija, Univerzitet odbrane u Beogradu*

**Sadržaj** – Sa konstantnim razvojem informacionih sistema, problem zaštite i kontrole pristupa sve je više dobijao na značaju, posebno kod sistema koji sadrže poverljive informacije. Kao jedan od načina kontrole pristupa nametnula se biometrijska zaštita, gde se najčešće koriste tehnike kontrole pristupa na osnovu otiska prsta. Razvijen je veliki broj algoritama za poređenje otisaka zasnovanih na obradi slike otiska i izdvajanju značajnih obeležja. U ovom radu analizirana je mogućnost primene kros-korelacije u verifikaciji korisnika na osnovu otiska prsta. Formirana je baza otisaka prstiju, analizirana njihova međusobna sličnost na osnovu kros-korelacije i analiziran uticaj rotacije otiska i aditivnog šuma na vrednosti kros-korelacije.

**Abstract** – With a constant development of information systems, access control and security gained more and more on its importance, especially on systems which contain confidential information. As a solution for access control, biometric protection using fingerprints was introduced. Large number of algorithms for fingerprint comparison were built based on fingerprint image processing and extraction of important parts. In this paper, the possibility of applying cross-correlation in the verification of users based on the fingerprint was analyzed. A fingerprint database was formed, their cross-correlation similarity was analyzed and the influence of the rotation of the fingerprint and additive noise on the cross-correlation value was analyzed.

### 1. UVOD

Detaljnim izučavanjem ljudskog organizma došlo se do zaključka da se pojedine karakteristike ljudskog tela mogu iskoristiti za autentifikaciju. To je dovelo do značajnog razvoja biometrije i do sve većeg korišćenja biometrijske zaštite podataka i informacionih sistema. Naučnici su došli do zaključka da su pojedini delovi tela kao što su: uši, lice, zenica i rožnjača oka, glas, otisak šake ili otisak prsta karakteristični za svakog čoveka ponaosob i mogu da se upotrebe kao najbolji načini za identifikaciju [1].

Relativno mala promenljivost karakteristika nabrojanih delova tela, najviše je uticala da baš oni budu izabrani kao jedinstveni identifikator svake osobe. U zavisnosti od parametara koji se posmatraju, svaki od identifikatora ima svoju specifičnost i identifikacionu vrednost. Među njima se izdvaja otisak prsta, kao jedan od najpouzdanijih [2, 3].

Otisci prstiju su najstarija biometrijska metoda. Sa naučnim pristupom u izučavanju i klasifikaciji otisaka krenulo se još u 19. veku. Tada se došlo do zaključka da

svaki čovek na svetu ima različit otisak. Otisci su relativno otporni na promene tokom vremena i samo usled nekih ozbiljnijih povreda (npr. opekotina) mogu značajno da se promene. Od tada pa do danas, otisci prstiju postali su neizostavni deo prilikom identifikacije i jedan od najupotrebljavanijih metoda u kriminalistici [4, 5].

Otisak prsta je otisak koji ostavlja spoljašnji sloj kože odnosno pokožica ili epidermis. Sam sloj sastoji se od isprepletenog niza udubljenja (eng. *valleys*) i uzvišenja (eng. *ridges*) koji se naizmenično smenjuju [6]. Oblik i raspored su proizvoljni i neponovljivi, tj. za svakog čoveka na svetu se razlikuju. Sama širina ovih udubljenja i uzvišenja je veoma mala i kreće se između 100 μm i 300 μm. Pored njih na svakom otisku mogu se izdvojiti i sitni karakteristični delovi koji se nazivaju minucije. U potpunim otiscima može ih biti i više od 100 zbog čega se uzimaju kao bitan faktor prilikom poređenja dva otiska [1].

Osnovni cilj ovog rada je pronalazak brzog i efikasnog načina kojim bi se moglo utvrditi da li neki otisak pripada skupu poznatih otisaka. Zbog brzine rada, bilo je potrebno izbeći složene algoritme predobrade i obrade otiska i poređenja karakterističnih obeležja. Ukoliko bi se testirano rešenje pokazalo kao dobro, moglo bi se iskoristiti za biometrijsku kontrolu pristupa informacionim sistemima, a koji zahtevaju brz odgovor da li je pristup odobren ili odbijen.

U drugom delu rada opisan je eksperiment tokom koga su prikupljeni otisci prstiju. U trećem delu rada izvršeno je međusobno poređenje otisaka prstiju, a radi određivanja njihove međusobne sličnosti. U četvrtom delu rada analiziran je uticaj rotacije i aditivnog šuma na određivanje sličnosti dva otiska. Najbitniji zaključci i pravci daljeg rada dati su u poslednjem, petom delu rada.

### 2. OPIS EKSPERIMENTA

Prvi korak predstavljao je formiranje baze sa poznatim otiscima koji će biti korišćeni u daljoj analizi. Od deset osoba uzet je otisak kažiprsta i palca i time je formirana polazna baza. Kao skener korišćen je *FingerPrint click* modul, uz koji se dobija i prateća aplikacija – slika 1. Sam modul omogućava povezivanje sa računarom preko USB HID-a i korišćenje aplikacije. Aplikacija omogućava prihvatanje skeniranog otiska i čuvanje na odabranoj lokaciji u računaru [7].

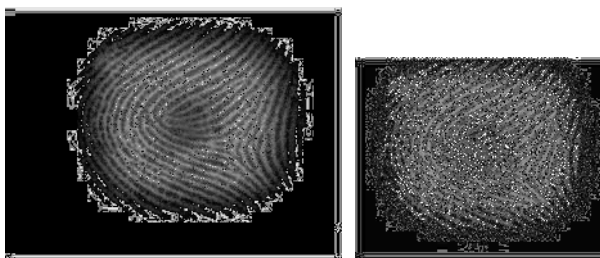
Fingerprint click ima GTS-511E2 CMOS senzor. Dimenzije modula su 16 x 20 mm, a od toga je efikasni deo koji se skenira 12 x 14 mm. Napaja se jednosmernim

naponom od 3,3 V. Skenirana slika je rezolucije 240 x 320 piksela (430 DPI). Na njemu se nalazi STM32F415RG mikrokontroler koji reguliše rad modula, a napaja se naponom od 1,8 V do 3,6 V. Jezgro mikrokontrolera predstavlja ARM 32-bit Cortex sa FPU, frekvencijom rada do 168 MHz i fleš memorijom od 1Mb [8].



Slika 1. FingerPrint click modul sa pratećom aplikacijom

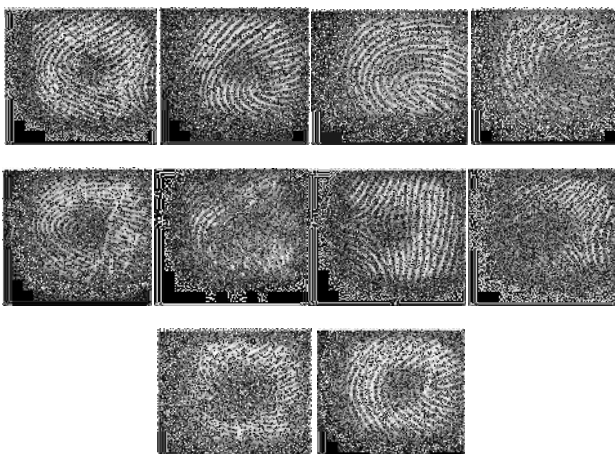
Zbog postojanja nekorisnog dela koji daje senzor prvo je izvršeno odsecanje tog dela kod svakog uzetog otiska i sa takvim slikama otisaka krenulo se u dalju analizu. Na slici 2 prikazan je izgled slike otiska pre i posle odsecanja. Odsecanjem je značajno istaknut sam otisak i njegove karakteristike.



a) originalna slika otiska      b) korisni deo otiska

Slika 2. Otisak prsta

Na slici 3 prikazani su otisci prstiju (kažiprst) svih učesnika eksperimenta nakon izdvajanja korisnog dela. Sa slike se vidi da svaka osoba ima jedinstven otisak prsta.



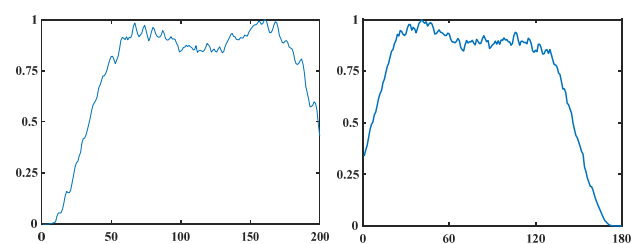
Slika 3. Otisci prstiju učesnika eksperimenta

### 3. POREĐENJE OTISAKA PRSTIJU

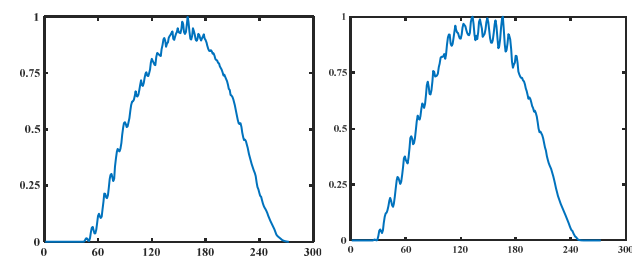
Za softversku realizaciju poređenja otisaka prstiju korišćen je MATLAB 2016a. U MATLAB-u je realizovano međusobno poređenje otisaka i izvršena analiza otpornosti tehnika poređenja otisaka prstiju na rotaciju i šum [9]. Analizirana su tri pristupa poređenja otisaka prstiju, zasnovanih na kros-korelaciji. Kod prvog pristupa korišćene su slike otisaka koje daje senzor bez bilo kakve obrade. Kod drugog pristupa izvršena je predobrada otiska primenom morfoloških operacija dilatacije i erozije, dok je kod trećeg pristupa pre poređenja izvršena detekcija ivica.

Kako slika otiska predstavlja dvodimenzionalnu (2D) matricu i poređenje slika zahteva veliku računarsku moć, analizirana je i predstava slike preko njenih projekcija – jednodimenzionalnih (1D) signala. Naime, izvršeno je sumiranje (projekcija) intenziteta piksela slike po horizontalnoj osi, vertikalnoj osi i po dijagonalama (projekcije intenziteta za orijentacije od  $-45^\circ$  i  $45^\circ$ ). Ovakav pristup je zasnovan na činjenici da se u otisku prsta pojavljuju udubljenja i uzvišenja različitih orijentacija, pa je za očekivati da će se kroz četiri projekcije uočiti njihov dominantan smer. U daljem radu dijagonalne projekcije biće obeležene sa  $D_1$  (orijentacija  $-45^\circ$ ) i  $D_2$  (orijentacija  $45^\circ$ ). Za određivanje dijagonalnih projekcija korišćena je MATLAB funkcija `radon` pomoću koje se određuje Radon transformacija (projekcija intenziteta) za zahtevani ugao.

Sumiranjem intenziteta slike otiska po horizontalnoj, vertikalnoj i dve dijagonalne ose dobijaju se 1D signali. Za otisak prsta sa slike 2b, normalizovane projekcije intenziteta prikazane su na slici 4.



a) horizontalna projekcija      b) vertikalna projekcija



c) projekcija  $D_1$       d) projekcija  $D_2$

Slika 4. Normalizovane projekcije intenziteta otiska prsta sa slike 2b

Sa slike 4 se uočava da dijagonalne projekcije nose više informacija o otisku prsta od horizontalne i vertikalne projekcije. Naime, na dijagonalnim projekcijama se uočava periodičnost signala zbog postojanja periodičnosti

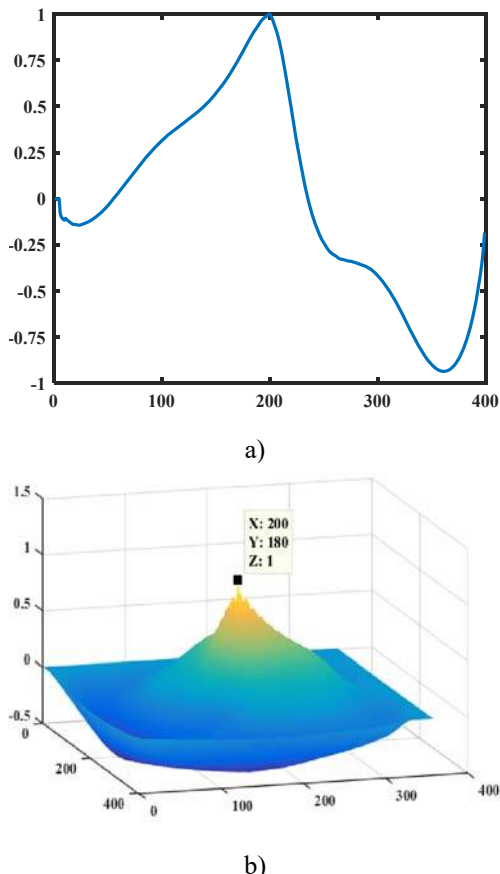
udubljenja i uzvišenja otiska prsta. Može se reći da je za dati otisak dominantan njihov dijagonalni smer, a što se uočava i sa slike 2b.

Normalizovana kros-korelacija se često koristi za poređenje dve slike (eng. *template matching*) i data je izrazom [10]:

$$\gamma(u, v) = \frac{\sum_{x,y} [f(x, y) - \bar{f}_{u,v}] [t(x - u, y - v) - \bar{t}]}{\left\{ \sum_{x,y} [f(x, y) - \bar{f}_{u,v}]^2 \sum_{x,y} [t(x - u, y - v) - \bar{t}]^2 \right\}^{0.5}} \quad (1)$$

gde je  $\bar{t}$  srednja vrednost intenziteta *template*-a, a  $\bar{f}_{u,v}$  srednja vrednost intenziteta regiona slike sa kojim se vrši poređenje. Kros-korelacija, kao mera sličnosti dva signala, daje kvantitativnu vrednost sličnosti na intervalu od -1 do 1, gde više vrednosti odgovaraju većoj sličnosti. Nezavisna je od srednje vrednosti osvetljaja i za njeno određivanje se mogu koristiti prednosti brze Furijeove transformacije [10]. Za određivanje normalizovane kros-korelacije korišćena je MATLAB funkcija `normxcorr2`. Ova funkcija se može koristiti za određivanje korelacije 2D signala – relacija (1), kao i za određivanje korelacije 1D signala.

Na slici 5 prikazana je kros-korelacija horizontalne projekcije otiska sa slike 2b i kros-korelacija otiska sa slike 2b. Rađena je korelacija otiska sa samim sobom, a radi ilustracije 1D i 2D korelacije.



Slika 5. Normalizovana kros-korelacija: a) horizontalne projekcije otiska 2b i b) slike otiska 2b

Na slici 5a se uočava da zbog poređenja istih vektora normalizovana korelacija dostiže maksimalnu vrednost, odnosno ima vrednost 1. Sličan zaključak može se izvesti i za sliku 5b.

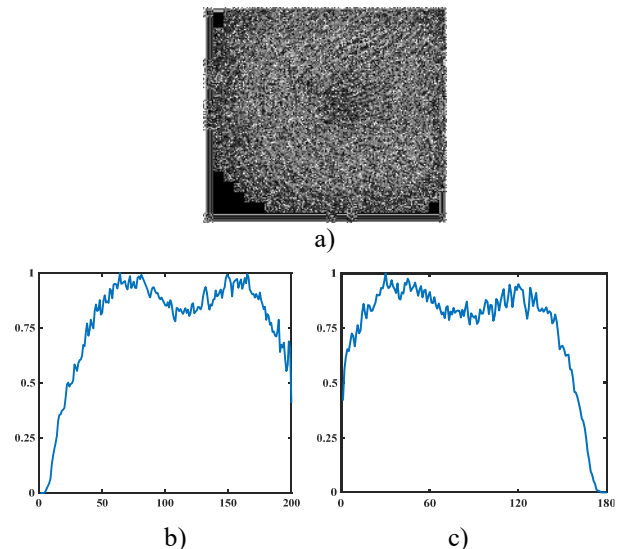
Kod drugog pristupa koji je korišćen u radu, za poređenje otisaka prstiju izvršena je obrada otiska prsta korišćenjem morfoloških operacija dilatacije i erozije [11].

Morfološke operacije koriste strukturni element koji se pozicionira na svim mogućim delovima originalne slike. Strukturni element je matrica piksela koji imaju vrednost 0 ili 1. U ovom radu korišćena je jedinična matrica 3x3 kao najčešće korišćeni strukturni element.

Kod dilatacije se strukturni element postavlja na početak slike i određuje se koja je najveća vrednost intenziteta piksela u lokalnom susedstvu definisanim strukturnim elementom (u našem slučaju lokalno susedstvo je 3x3 piksela). Maksimalna vrednost se dodeljuje centralnom pikselu slike koji je pokriven strukturnim elementom. Postupak se ponavlja za celu sliku. Ovom operacijom značajno se povećava intenzitet svetlijih delova slike. Dilatacijom se popunjavaju sitne praznine, odnosno potiskuje šum koji se javlja na slici. Erozijska slika radi na sličnom principu kao dilatacija, ali se umesto izračunavanja maksimalne vrednosti intenziteta piksela određuje najmanja vrednost, usled čega dolazi do smanjenja intenziteta tamnijih delova slike.

Za svaki otisak izvršeno je oduzimanje slike dobijene erozijom od slike otiska dobijene dilatacijom. Na tako dobijenim slikama vršena su sva izračunavanja i poređenja kao i na slikama otisaka bez obrade.

Na slici 6 prikazan je otisak sa slike 2b obrađen na opisani način, i prikazane su njegova horizontalna i vertikalna projekcija.



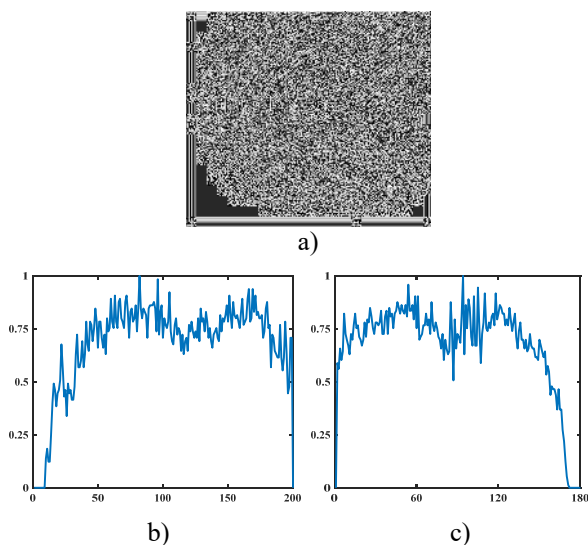
Slika 6. a) otisak sa slike 2b nakon primene dilatacije i erozije i njegova horizontalna b) i vertikalna c) projekcija

Sa slike 6 se uočava da se primenom opisanog pristupa ističu obeležja otiska prsta, tj. na projekcijama se uočava periodičnost signala zbog udubljenja i uzvišenja otiska.



Kod trećeg pristupa pre poređenja otisaka izvršena je detekcija ivica pomoću postupka opisanog u [12], a koji je u MATLAB-u implementiran pomoću funkcije `edge` (korišćene su predefinisane vrednosti neophodnih parametara). Ivice su izdvojene sa izvorne slike koju daje senzor. Detekcijom ivica dobija se binarna slika čije su vrednosti 0 ili 1. Ivice imaju vrednost 1, a ostatak slike 0.

Na slici 7 prikazane su ivice otiska sa slike 2b. Kao i kod prethodne dve analize, nad ovako obrađenim otiscima izvršeno je sumiranje intenziteta za četiri orijentacije. Na slikama 7b i 7c prikazane su projekcije po horizontalnoj i vertikalnoj osi dobijene binarne slike 7a. Sa slika se uočava da je izgled projekcija različit od projekcija prethodna dva pristupa, sa oscilacijama koje imaju slučajan karakter.



Slika 7. a) otisak sa slike 2b nakon detekcije ivica i njegova horizontalna b) i vertikalna c) projekcija

Poređenje otisaka prstiju sprovedeno je pomoću kros-korelacije, gde je korelacija određivana za projekcije uzoraka i za slike uzoraka (originalne slike, slike nakon primene morfoloških operacija i za binarne slike). Poređenja su izvršena tako što je određena sličnost jednog otiska sa preostalim otiscima iz prikupljene baze. U analizi su korišćene slike kažiprsta. Nakon određivanja sličnosti uzoraka, za svaki od pristupa određena je maksimalna vrednost međusobne sličnosti uzoraka. Maksimalna vrednost predstavlja granicu (prag) koju treba postaviti da bi se tvrdilo (sa određenom verovatnoćom), da otisak pripada osobi ili osobama koje bi imale pristup nekom objektu ili informacionom sistemu.

U tabeli 1 date su maksimalne vrednosti za svaki od pristupa. Pristup I predstavlja izračunavanja nad originalnim otiscima koji daje senzor, pristup II nad otiscima koji su obrađeni dilatacijom i erozijom i pristup III nad detektovanim ivicama.

Pristup	Horizontalna projekcija	Vertikalna projekcija	$D_1$	$D_2$	Slike otiska
I	0.9913	0.9946	0.9974	0.9973	0.8489
II	0.9783	0.9814	0.9964	0.9958	0.6101
III	0.8889	0.9104	0.9771	0.9716	0.1302

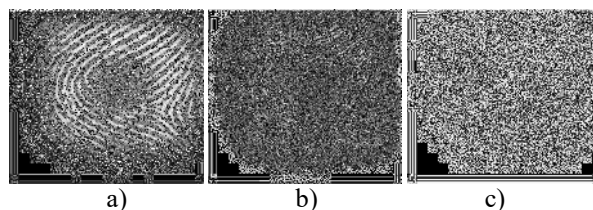
Tabela 1. Prikaz maksimalnih vrednosti sličnosti

Iz table 1 se vidi da se korišćenjem projekcija (1D predstava otisaka) dobija velika međusobna sličnost uzoraka. Zbog toga se u daljoj analizi (analizi robusnosti) projekcije slika nisu koristile. Poređenje slika (2D signala) omogućava veću marginu prilikom poređenja otisaka, tj. ostavlja se više prostora za dodatne degradacije otiska prsta koje se mogu javiti (rotacija, pomeraj, zamrljanje, uticaj šuma i sl. [13]). Margina se povećava (sličnost uzoraka se smanjuje) uvođenjem morfoloških operacija, odnosno poređenjem ivica otisaka prstiju.

#### 4. UTICAJ DEGRADACIJA NA KORELACIJU

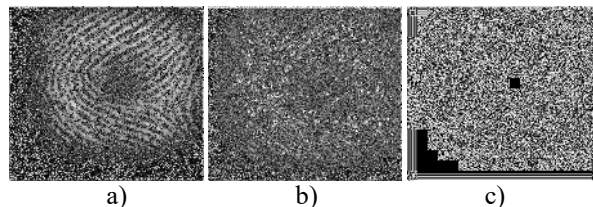
Kako se prilikom skeniranja otiska mogu javiti različite degradacije signala, u radu je analizirana robusnost kros-korelacije na uticaj rotacije otiska i na uticaj aditivnog šuma.

Kod analize uticaja rotacije, svaki otisak je zarotiran u opsegu od -10 do 10 stepeni, sa korakom od jednog stepena. Nakon toga je sračunata sličnost originalne slike i njenih rotiranih verzija. Uticaj rotacije je analiziran za sva tri pristupa poređenja slika. Na slici 8 prikazan je otisak sa slike 2b nakon rotacije za 3 stepena.



Slika 8. a) otisak prsta nakon rotacije, b) nakon primene morfoloških operacija i c) nakon detekcije ivica

Prilikom analize uticaja šuma, korišćen je aditivni Gausov šum nulte srednje vrednosti i standardne devijacije od 0 do 5 nijansi sive, sa korakom od 0.5 nijansi. Za svaku vrednost standardne devijacije šuma sračunata je sličnost originalne (nezašumljene) slike i njenih zašumljenih varijanti. Uticaj šuma je analiziran za sva tri pristupa poređenja slika. Na slici 9 prikazan je otisak sa slike 2b nakon dodavanja Gausovog šuma standardne devijacije od 2.5 nijansi sive.

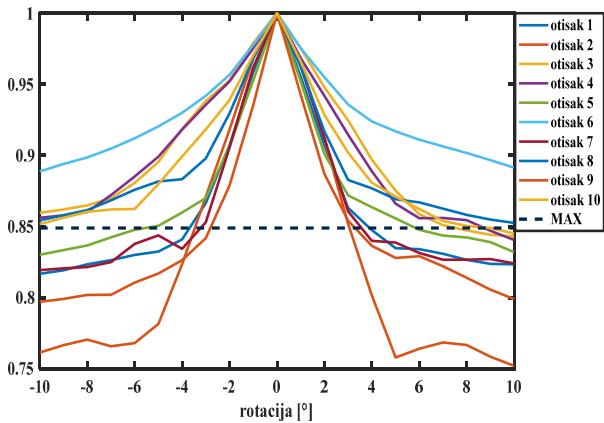


Slika 9. a) otisak prsta nakon dodavanja šuma, b) nakon primene morfoloških operacija i c) nakon detekcije ivica

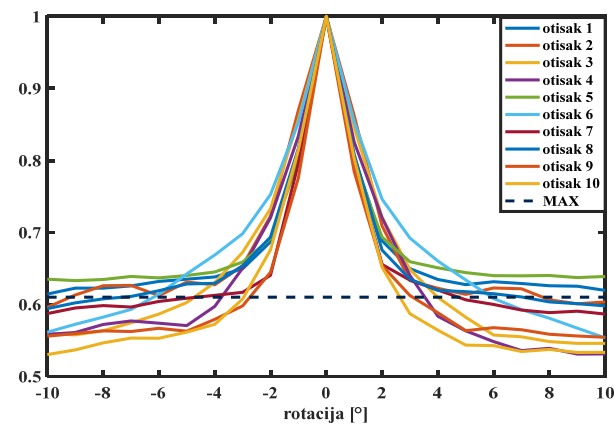
Sa slike se 9 uočava da šum negativno utiče na otisak tretiran dilatacijom i erozijom i stvara skoro nejasnu sliku. Pristup sa izdvajanjem ivica je značajno otporniji.

Na slici 10 prikazan je uticaj rotacije na sličnost originala i njegovih zarotiranih verzija, u sva tri pristupa obrade slika. Prikazane su vrednosti kros-korelacije za svih 10 učesnika u eksperimentu. Dodatno su obeležene maksimalne

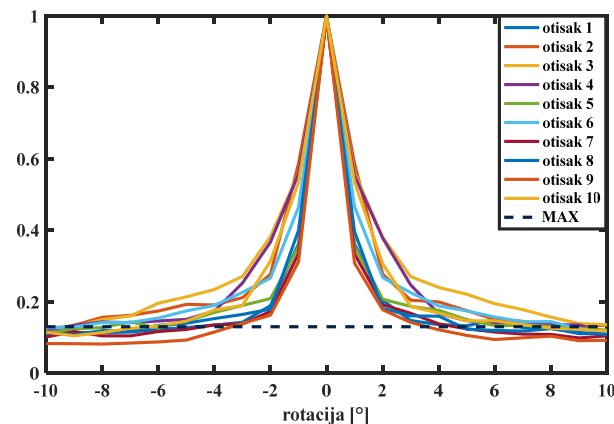
vrednosti međusobne sličnosti uzoraka (tabela 1), kao granica tolerancije rotacije.



a) kros-korelacija zarotiranih otisaka



b) kros-korelacija zarotiranih otisaka obrađenih primenom morfoloških operacija



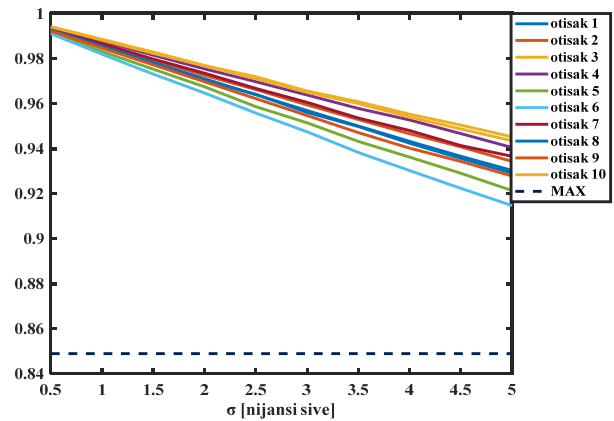
c) kros-korelacija zarotiranih otisaka nakon detekcije ivica

Slika 10. Uticaj rotacije na kros-korelaciju

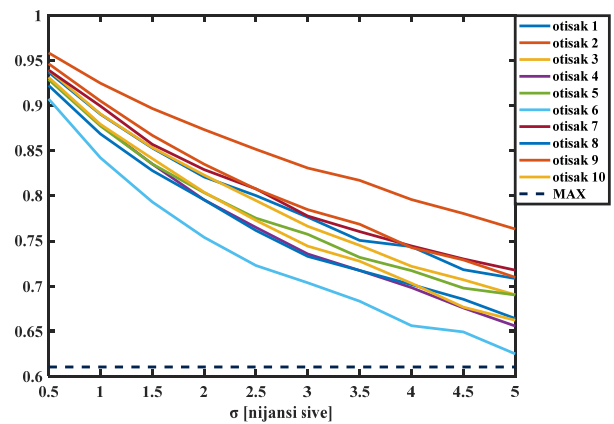
Sa slike 10 se uočava da su otisci različito otporni na uticaj rotacije (za sva 3 pristupa). Tako se sa slike 10a može zaključiti da je otisak obeležen sa 6 najotporniji na uticaj rotacije, dok rotacija ima veliki uticaj na otisak obeležen sa 9. Posmatranjem svih otisaka, za usvojene pragove tolerancije, može se zaključiti da se mogu tolerisati rotacije uzorka do 3 stepena.

Na slici 11 prikazan je uticaj šuma na sličnost originala i njegovih zašumljenih verzija, u sva tri pristupa obrade

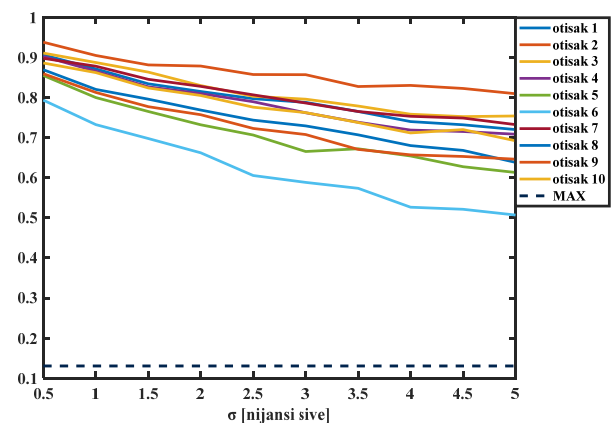
slika. Prikazane su vrednosti kros-korelacije za svih 10 učesnika u eskperimentu. Dodatno su obeležene maksimalne vrednosti međusobne sličnosti uzoraka (tabela 1), kao granica tolerancije uticaja šuma.



a) kros-korelacija zašumljenih otisaka



b) kros-korelacija zašumljenih otisaka obrađenih primenom morfoloških operacija



c) kros-korelacija zašumljenih otisaka nakon detekcije ivica

Slika 11. Uticaj šuma na kros-korelaciju

Sa slike 11 se uočava da su otisci različito otporni na uticaj šuma (za sva 3 pristupa). Kod sva tri pristupa može se zaključiti da vrednost sličnosti linearno opada sa povećanjem standardne devijacije šuma. Takođe, za usvojene pragove tolerancije iz tabele 1, može se zaključiti da je kros-korelacija kao mera sličnosti pogodna za verifikaciju korisnika – vrednost sličnosti originala i zašumljenih verzija je iznad usvojenog praga.

## 5. ZAKLJUČAK

U radu je analizirana mogućnost primene kros-korelacije za verifikaciju korisnika na osnovu slika otiska prsta. Analiza je sprovedena na uzorku od 10 osoba. Prvo je analizirana međusobna sličnost uzoraka u okviru grupe. Ova analiza je pokazala da se može usvojiti prag sličnosti koji omogućava verifikaciju korisnika, ali i robusnost procesa verifikacije na dodatne degradacije otiska prsta.

Analizirana je otpornost kros-korelacije na uticaj rotacije i aditivnog šuma. Pokazano je da je kros-korelacija otpornija na uticaj šuma nego na uticaj rotacije otiska. Takođe, pokazano je da se mogu tolerisati rotacije otiska do 3 stepena.

Analizirana su tri pristupa poređenja slika otiska prsta – poređenje originalnih slika, poređenje slika nakon primene morfoloških operacija i poređenje slika nakon detekcije ivica. Pokazano je da su sva tri pristupa upotrebljiva, a dodatni izbor jednog od njih biće uslovljen mogućnošću implementacije za rad u realnom vremenu i uticajem dodatnih izobličenja.

U daljem radu analiziraće se uticaj dodatnih izobličenja (zamrljanja, pomeraja i nekompletnog otiska) na kros-korelaciju kao meru sličnosti otisaka prstiju. Takođe, analiziraće se mogućnost primene kros-korelacije u identifikaciji osobe primenom otiska prsta.

## NAPOMENA

Ovaj rad je deo projekta „Upravljanje pristupom zaštićenim resursima računarskih mreža u Ministarstvu odbrane i Vojsci Srbije na osnovu multimodalne biometrijske identifikacije korisnika” – evidencioni broj VA-TT/3/18-20, 2018.-2021., Univerzitet odbrane.

## LITERATURA

[1] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., *Handbook of fingerprint recognition*, Springer Science & Business Media, 2009.

[2] Jojić, J., Babić, Z., Đurović, Ž. „Klasifikacija i prepoznavanje otisaka prstiju”, XIII međunarodni naučno-

stručni simpozijum INFOTEH 2014, Zbornik radova, str. 676-681, Jahorina, 19.-21. mart 2014.

[3] Stojanović, B. „Razdvajanje preklopljenih otisaka prstiju bazirano na tehnologiji mašinskog učenja”, Doktorska disertacija, Univerzitet u Beogradu, Elektrotehnički fakultet, 2017.

[4] Jain, A.K., Feng, J., Nandakumar, K. „Fingerprint matching”, *Computer*, vol. 43, no. 2, pp. 36-44, 2010.

[5] Borković, G., Vrankić, M., Sučić, V. „Usmjereni digitalni filtri za prepoznavanje otisaka prstiju”, *Engineering Review*, vol. 28, no. 1, pp. 39-50, 2008.

[6] Lee, W., Cho, S., Choi, H., Kim, J. „Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners”, *Expert Systems with Applications*, vol. 87, pp. 183-198, 2017.

[7] MikroElektronika, *FingerPrint click manual*, 2015.

[8] ADH Technology Co. Ltd, *Optical Fingerprint Sensor Module GTS-511E2 – Datasheet, Version V 1.1*

[9] Chen, S.M., Chiang, C.K. „Rotation, translation, and scale invariant bag of feature based on feature density”, 7th IEEE International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Proc. of papers, pp. 163-168, 2016.

[10] Lewis, J.P. „Fast normalized cross-correlation”, *Vision Interface*, vol. 10, no. 1, pp. 120-123, 1995.

[11] Gonzalez, R.C., Woods, R.E., *Digital image processing*, Third edition, Pearson International Edition, 2008.

[12] Canny, J. „A computational approach to edge detection”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 8, no. 6, pp. 679-698, 1986.

[13] Liu, X., Pedersen, M., Charrier, C., Bours, P., Busch, C. „The influence of fingerprint image degradations on the performance of biometric system and quality assessment”, *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1-6, 2016.

# Digitalna kontrola brzine jednosmernog motora primenom tiristora i softvera LABVIEW

## Digital DC motor speed control using thyristor and software LABVIEW

Milinko Srečković<sup>1</sup>, Davorin Mikluc<sup>1</sup>  
Vojna akademija, Univerzitet odbrane u Beogradu<sup>1</sup>

**Sadržaj** —U ovom radu je prikazan postupak upotrebe softvera LABVIEW i akvizicijske kartice NI USB-6212 u automatizaciji procesa i merenjima signala na primeru kontrole brzine DC motora. Izvršena je u potpunosti digitalna kontrola realnog sistema sa analognim komponentama. Upotrebljen je softver LABVIEW za generisanje pobude i obradu izmerenih signala. Upravljanje DC motorom je ostvareno preko A/D konvertora i tiristorskog kola. Detaljno je objašnjeno upravljanje uglom paljenja tiristora, formirani strukturni blok dijagrami, postupak i obrada merenja kao i uticaj poremećaju na rad sistema.

**Abstract** – The process of applying the LABVIEW software and NI USB-6212 acquisition card in process automation and signal measurements in the example of DC motor speed control has been shown in this paper. A complete digital control of a real system with analog components was performed. LABVIEW software was used for generating the impulse and processing the measured signals. DC motor was controlled via A/D converter and thyristor circuit. The control of thyristor ignition angle, the formed structure block diagrams, the measurement phases and processing, and the influence of disturbance on the system functioning were explained in detail.

### [1] UVOD

Oblast upravljanja jednosmernim motorima je široka. Mnogobrojna istraživanja su objavljena u upravljanju motori primenom različitih algoritama. Pregled nekih od metoda je dat u [1,2]. Problem upravljanja se mora kontrolisati, odnosno pobuda sistema mora da bude besprekorno tačna, zbog čega su vremenom računari našli svoje mesto [3], ali i mikrokontroleri, [4]. Upotrebom mikroracunara se dobilo umnogome na preciznijoj identifikaciji sistema, a zatim je usledilo i era adaptivnog upravljanja, [5]. Jedan od novijih primera u identifikaciji sistema upotrebom savremenih metoda je opisan u [6]. Dalja istraživanja u oblasti se mogu razvrstati u više podoblasti. U ovom radu je bila želja da se primeni tiristorsko kolo za upravljanje jednosmernim motorom, što je istraživanje u kojem nema mnogo prostora za doprinose u vidu poboljšanja hardvera, ali ima u vidu primene novijih tehnološki dostignuća ili novih matematičkih aparata. Radovi [7-11] pokazuju različite pristupe u upravljanju jednosmernim motorom pomoću tiristora. Upravo ti radovi su bili nadahnuće za formiranje sistema upravljanja kakav je opisan u ovom radu. Jednosmerni motor predstavlja glavni deo opreme u mnogim industrijskim projektima koji zahtevaju

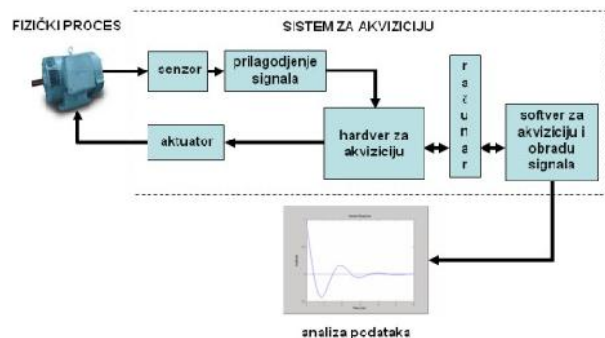
promenljive karakteristike brzine i opterećenja usled lake kontrole. Jednosmerni motor može da se kontroliše različitim metodama, kao što su kontrola polja, kontrola napona u rotorskom namotaju, kontrola otpornosti u rotorskom namotaju. Napon u rotoru se kontroliše koristeći različite AC/DC pretvarače (ispravljače). Polutaladni ispravljač, ispravlja

sa transformatorom sa srednjim izvodom, ispravljač sa Grecovim spojem neki su od tiristorskih sklopova koji se koriste za kontrolu brzine DC motora. Njihova poluprovodnička karakteristika je prethodnica današnjih p/n spojeva, odnosno dioda, međutim snaga koju ostvaruju je daleko veća. Druga uloga je princip primene tiristorskih kola. Upravljanje jednosmernim motorima se često izvršava primenom PWM (*Pulse Width Modulation* eng.) signala, što se ranije ostvarivala upravo tiristorskim kolima.

U ovom radu je prikazan jedan novi koncept a to je kombinacija savremenih softvera i akvizicijske kartice sa starijim pouzdanim hardverom. Ideja ovog rada je ostvarivanje komunikacije izmedju hardvera i softvera, kojom bi se upravljalo otvaranjem tiristorskih kola za upravljanje jednosmernim motorom, prema principu PWM signala, ali i kojom bi se prikupljali podaci koji nose informaciju o brzini obrtanja osovine motora sa tahogeneratorskog i optičkog enkodera. Komunikacija je ostvarena sa 8 bitnom magistralom i jednim okidačnim signalom.

### [2] OPIS I RAD SISTEMA

Opšti strukturni blok dijagram je dat na slici 1. Sistem se sastoji od računara, akvizicijske kartice koja prihvata naponske signale sa senzora, ali i generiše signale preko aktuatora, i na kraju objekta upravljanja-jednosmernog motora.



Slika 1. Opšta šema sistema upravljanja

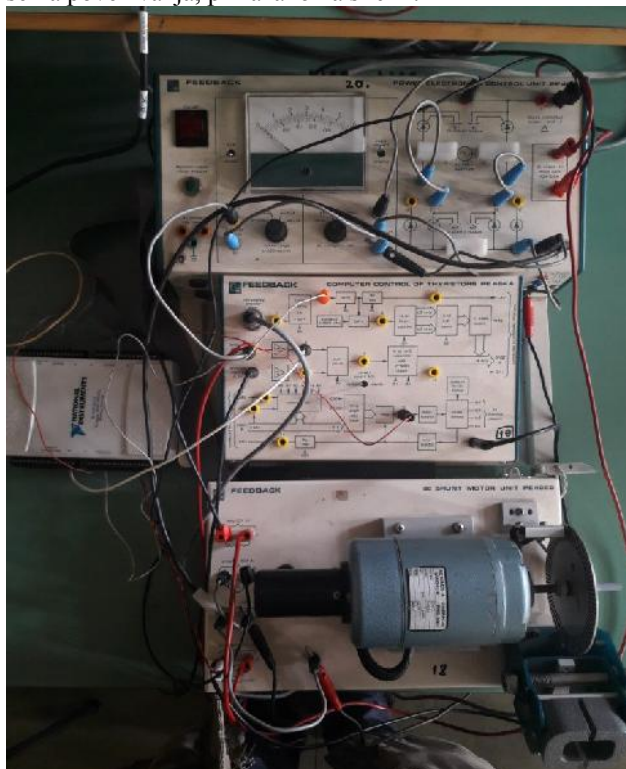


Komplet za kompjutersku kontrolu uređaja energetske elektronike PE484, prikazan na slici 2, deo je kompleta PE480. Osnovna namena ovog kompleta je upoznavanje studenata sa tehnologijom, realizacijom i relevantnim problemima koji se javljaju u tiristori upravljanim elektromotornim pogonima. Komplet-modul PE484 omogućuje upravljanje motorom i pretvaračem za napajanje motora iz računara-mikrokomputera.

Komplet za upravljanje jednosmernim motorom PE484 se sastoji od:

- PE482B - motor;
- PE482C - jedinica za kočenje;
- PE483 - kontrolna jedinica sa tiristorima;
- PE484A - modul za kompjutersko upravljanje;
- PE484B - inkrementalni enkoder;

Prvi doprinos ovog rada je shvatanje šeme aparature. Veoma detaljnim i strpljivim pristupom je napravljena šema povezivanja, prikazano na slici 2.



Slika 2. Komplet za upravljanje jednosmernim motorom PE484 povezan sa akvizicionom karticom

Slanje i priključenje podataka između računara i hardvera je ostvaren preko kartice firme National Instruments, NI USB-6212, slika 3. Akviziciona kartica NI USB-6212 je 16-bitna sa maksimalnom brzinom semplanja 200 kS/s. Neke od osnovnih karakteristika su:

- 8 analognih ulaza
- opseg ulaznih napona +/- 10 V,
- 2 analogna izlaza, 12 digitalnih ulaza/izlaza,
- 32 bitni counter/timer modul i dr.



Slika 3. Akvizicijska kartica NI USB 6212

Upotrebom kartice NI USB-6212 se ostvaruje veza sa računarom kome i omogućena je kontrola upravljanja motorom, kao i prikupljanje informacije o brzini obrtanja. Komunikacija pomoću navedene kartice je ostvarena preko digitalnih ulaza i izlaza. Upotrebom je 9 izlaznih portova kako bi se generisala 8 bitna reč i jedan bit koji služi kao okidač za prikupljanje podataka.

Fazna tiristorska (SCR) kontrola se bazira na podešavanju faznog ugla kod tiristori kontrolisanih ispravljača (AC/DC), podešavača napona (AC/AC). Fazni ugao se računa od trenutka kada su se stekli uslovi za uključanje. Ovo uslovljava sinhronizaciju trenutka uključanja tiristora u odnosu na mrežni napon. Uslovi za uključanje tiristora se stiču kada je napon između njegove anode i katode pozitivan, što ne mora da znači da će tiristor tada biti uključen. Njegovo uključanje se ostvaruje dovođenjem odgovarajućeg impulsa na gejt elektrodu, uz izvestan ugao kašnjenja u odnosu na prolazak mrežnog napona kroz nulu. Računar mora biti informisan o trenucima kada mreža prolazi kroz nulu i raspolagati programabilnim tajmerom koji će načiniti potrebno kašnjenje impulsa na gejt kako bi se ostvario željeni ugao paljenja. Tajmer je uključen u modul PE484A. Veličinu vremenskog kašnjenja računara saopštava preko porta B.

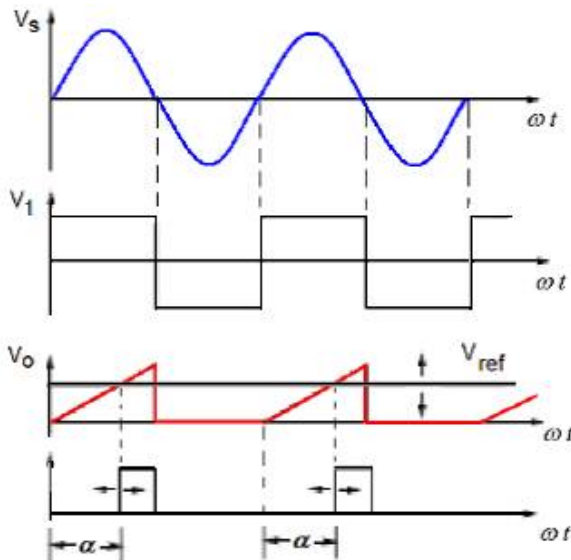
Motorom se upravlja uz pomoć 8-bitne reči, obradjene u softverskom paketu LABVIEW, koju računara šalje preko porta B na kontrolnu jedinicu sa tiristorima. Vrednosti zadatog ugla paljenja i brzina rotacije su recipročne. Ta konstatacija proizilazi iz definicije PWM signala, po kojoj je efektivna vrednost proporcionalna sa širinom impulsa. Dakle ukoliko je ugao paljenja manji, to znači da je širina impulsa veća, a time i efektivna vrednost što prouzrokuje veću brzinu obrtanja motora.

Motorom se upravlja uz pomoć

8-bitne reči, obradjene u softverskom paketu LABVIEW, koju računara šalje preko porta B na kontrolnu jedinicu sa tiristorima. Vrednosti zadatog ugla paljenja i brzina rotacije su recipročne. Ta konstatacija proizilazi iz definicije PWM signala, po kojoj je efektivna vrednost proporcionalna sa širinom impulsa. Dakle ukoliko je ugao paljenja manji, to znači da je širina impulsa veća, a time i efektivna vrednost što prouzrokuje veću brzinu obrtanja motora.

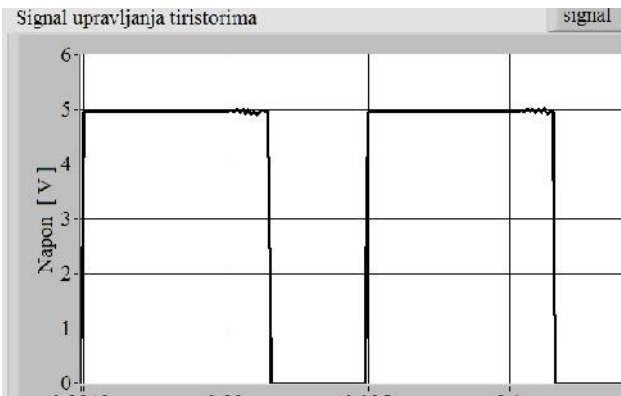
Pošto se motor upravlja 8-bitnom rečju, a MSB uvek ima vrednost 0, kako bi motor uopšte bio pokrenut, to znači da ugao paljenja može imati vrednost od 0 do 127, a to se jednostavnim matematičkim operacijama može prevesti u ugao  $\alpha \in [0, \pi]$ , slika 4.



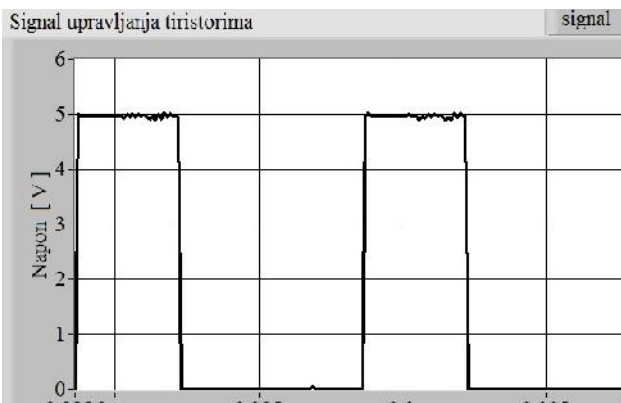


Slika 4. Primer kontrolisanja ugla paljenja

U ovom radu je analiziran odziv sistema za uglove paljenja od 10 do 100 diskretnih vrednosti sa korakom 10. Vrednosti za ugao paljenja manje od 10 nemaju primetnih razlika, jer je ugaona brzina rotora motora gotovo maksimalna, dok za vrednosti preko 100 motor nije reagovao jer je efektivna vrednost napona nedovoljna da pokrene motor. Slika 5. i Slika 6. predstavljaju izgled ulaznog signala za vrednosti ugla paljenja 40 i 80. Na slikama 5. i 6. je prikazan izgled signala za dve periode.



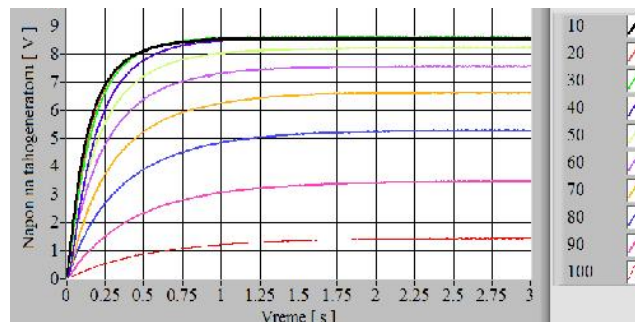
Slika 5. Prikaz signala ugla paljenja za vrednost  $40/127 \cdot \pi$  rad u trajanju od dve periode



Slika 6. Prikaz signala ugla paljenja za vrednost  $80/127 \cdot \pi$  rad u trajanju od dve periode

### [3] MERENJE I PROCENA PARAMETARA SISTEMA

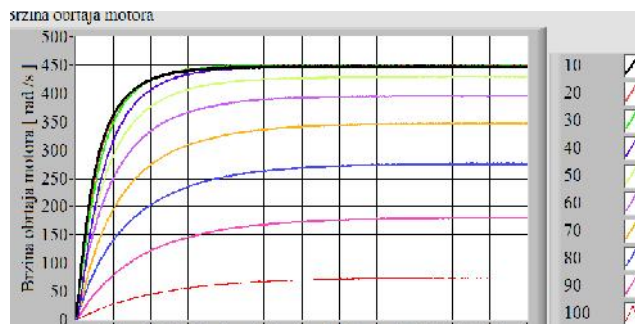
U zavisnosti od vrednosti zadanog ugla paljenja na izlazu cemo dobiti odredjene vrednosti odziva. Nakon obrade dobijenih podataka u softverskom paketu LABVIEW dobili smo izgled odziva i prikazali ih familijom krivi. Slika broj 7. predstavlja izgled vrednosti napona na tahogeneratoru



Slika 7. Vrednost napona na tahogeneratoru

Nakon što je izmerena vrednost napona na tahogeneratoru, a vrednost konstante tahogeneratora je data uz priručniku za rukovanje paketom PE484, jednostavnim računom se može odrediti vrednosti brzine obrtanja rotora za svaki od zadanatih uglova, slika 8.

(1)



Slika 8. Ugaona brzina obrtanja motora u zavisnosti od vrednosti ugla paljenja merena tahogeneratorom

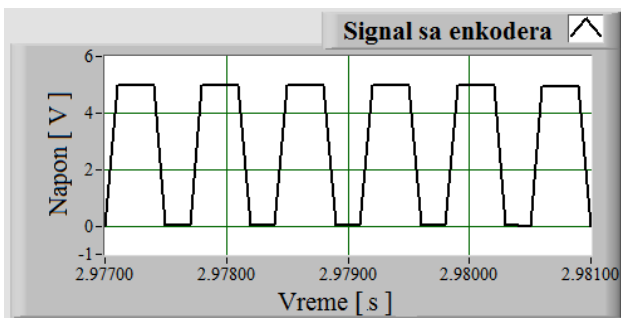
Na grafiku se može primetiti da za male vrednosti ugla paljenja (10, 20, 30 pa i 40) odziv ima približno isti izgled karakteristike. To je zato što je za te vrednosti mala razlika efektivnim vrednostima zadanog napona pa se ne gubi mnogo od prvobitne vrednosti signala. Razlika je uočljiva samo u brzini postizanja stacionarnog stanja.

Radi kontrole i poređenja rezultata merena je brzina na enkoderu PE484B. Disk enkodera poseduje nazubljeni obod i optički čitač koji pri obrtanju diska generiše digitalne impulse u toku prolaska svakog zuba na obodu, slika 9.



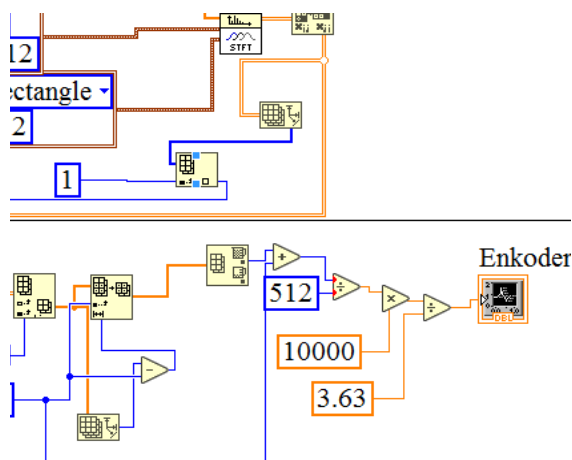
Slika 9. Enkoder PE484B, uokviren crvenim kvadratom

Brzina se meri tako što se digitalnim tajmerom izmeri vreme između nailaska sukcesivnih impulsa enkodera, slika 10. Gušća nazubljenost enkodera je poželjna radi veće preciznosti pri malim brzinama ali narušava tačnost merenja za veće brzine, kada se između sukcesivnih impulsa mere manja vremena. Zbog toga se na modulu PE484A primenjuje brojač/delilac sa 4 kako bi se obezbedila zadovoljavajuća tačnost pri velikim brzinama.



Slika 10. Prikaz dela signala sa optičkog enkodera

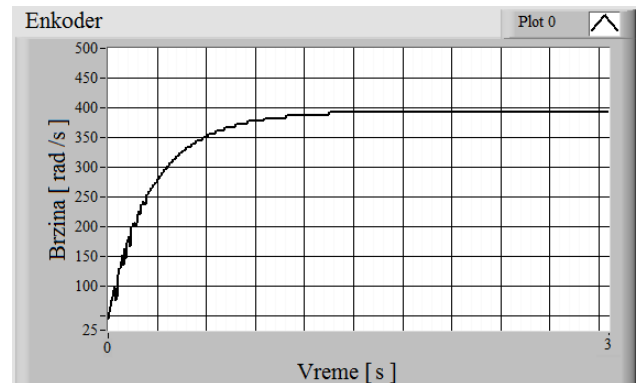
Računar iz ovog podatka izračunava brzinu motora, slika 11.



Slika 11. Strukturni blok dijagram za procenu kružne učestanosti signala sa enkodera

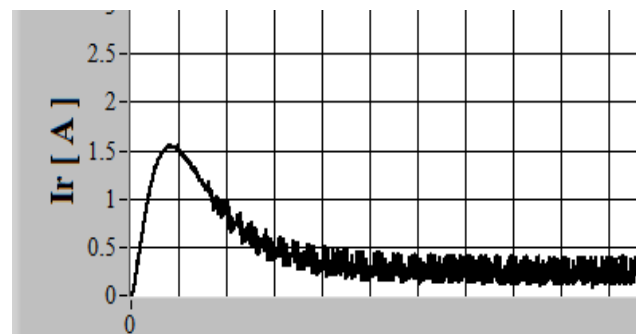
Nakon obrade i poredenja rezultata sledi da su brzina okretanja enkodera, slika 12., i brzina okretanja motora

merena na tahogeneratoru, slika 8., za zadati ugao identične.



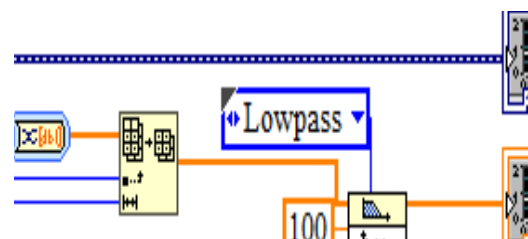
Slika 12. Procena kružne učestanosti signala sa enkodera za ugao  $60/127 \cdot \pi$  rad

Akvicijska kartica je upotrebljena u još jednoj nameni. Merena struja u rotorskom namotaju, slika 13.

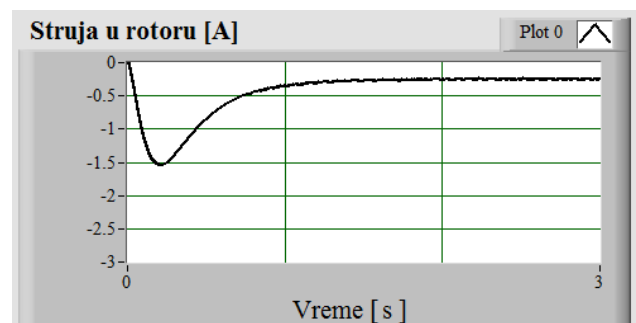


Slika 13. Izmerna struja u rotorskom namotaju

Radi lakše dalje obrade i korišćenja podataka o dobijenoj vrednosti filtrirano je merenje sa blokom na slici 14.



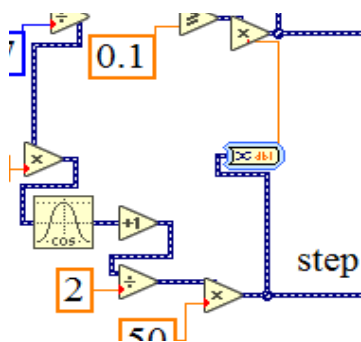
Slika 14. Strukturni blok dijagram filtera za izmerenu struju u rotorskom namotaju



Slika 15. Filtrirana struja u rotorskom namotaju

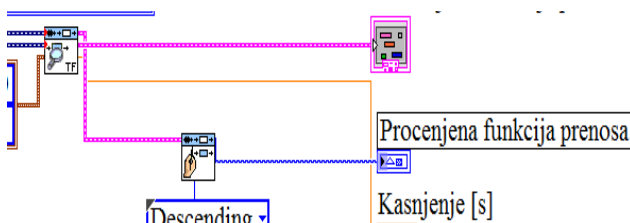
Dobijeni signal može da se koristi u daljim obradama podataka i daljim proračunima bez šuma koje su pri merenju zabeležene, slika 15.

Identifikacija funkcije prenosa uz pomoć programskog paketa LABVIEW je podrazumevalo modelovanje pobudnog step signala. Signal pobude je generisan prema strukturnog blok dijagramu, slika 16.



Slika 16. Model step pobude za procenu funkcije prenosa

Daljom obradom podataka pretpostavljen je red funkcije prenosa a zatim i koeficijenta funkcije prenosa za svaku od zadatih vrednosti ugla paljenja, slika 17. i slika 18.

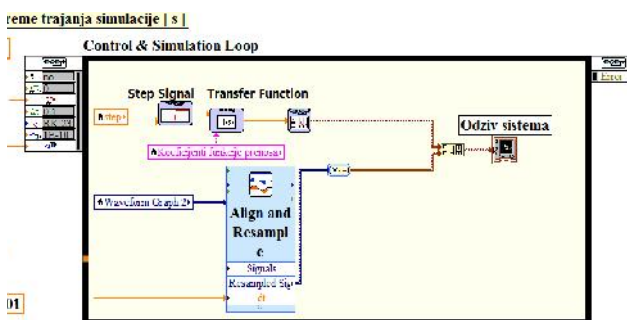


Slika 17. Deo strukturnog blok dijagrama za procenu funkcije prenosa

$$y(s) = \frac{14.4782}{0.255141s + 1}$$

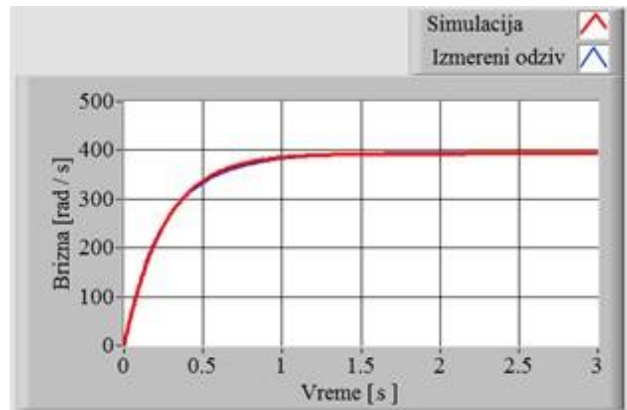
Kasnjenje [s]

Slika 18. Procenjena funkcija prenosa sistema za ugao paljenja  $60/128 \cdot \pi$  rad



Slika 19. Strukturni blok dijagram simuliranih i izmerenih brzina obrtanja

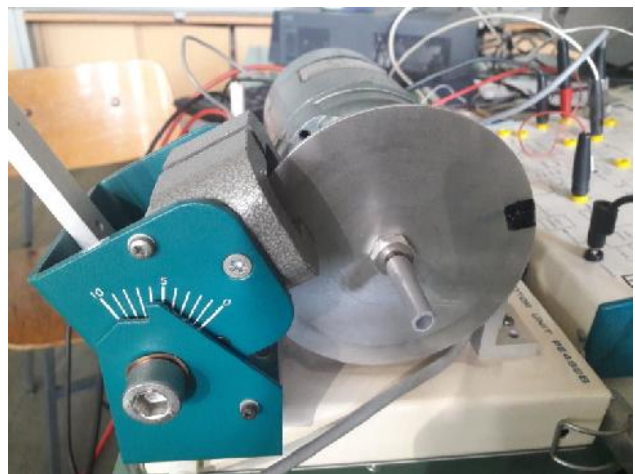
Nakon izvršene simulacije, slika 19, poređenjem izmerene i simulirane vrednosti na istom grafiku pokazano je da su simulirani i snimljeni odziv sistema identični, slika 20.



Slika 20. Odziv sistema

#### [4] RAD SISTEMA U PRISUSTVU POREMEĆAJA

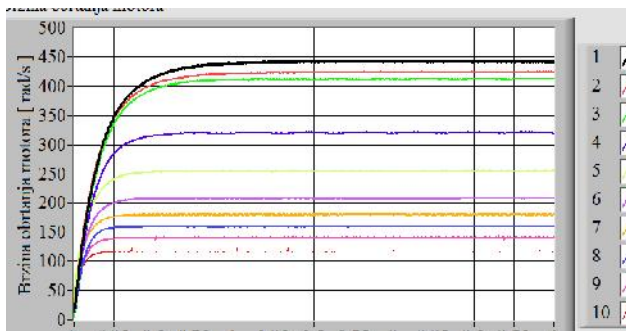
Na slici 21. prikazana je jedinica za kočenje PE482C. Kočnica je pričvršćena za PE484 na delu postolja neposredno uz enkoder. Kočnica se sastoji iz 2 stalna magneta koji nemaju nikakav uticaj na sistem dok se kočnica ne postavi na neki od ucrtanih 10 položaja.



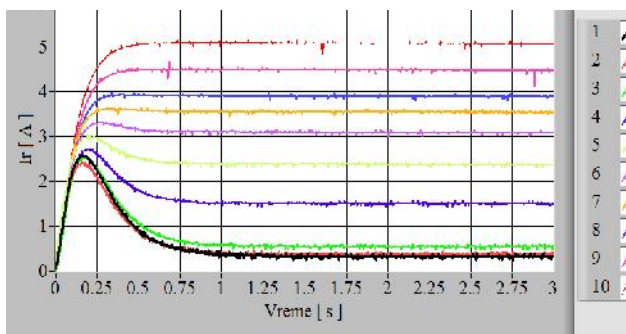
Slika 21. Jedinica za kočenje PE482C

U toku rada, položaje kočnice su redom postavljeni u označene položaje, što je uzrokovalo različite uticaje na rad sistema. Sa povećanjem opterećenja brzina opada, slika 22, ali isto tako je primetno da veći poremećaj prouzrokuje i veću vrednost struje rotora, slika 23. To je zato što sistem i dalje želi da postigne zahtevanu brzinu obrtanja.

Dobijena merenja, slika 22. I 23. Se mogu iskoristiti u daljim istraživanjima, kao što su adaptivna upravljanja ili primena PID regulacije brzine obrtanja.



Slika 22. Zavisnost brzine obrtanja od položaja kočnice



Slika 23. Izmerena struja rotora u zavisnosti od položaja kočnice

## [5] ZAKLJUČAK

U radu je upotrebljen softverski alat LABVIEW za digitalno upravljanje i merenje signala. Formirani su strukturni blok dijagrami za formiranje pobudnog signala u vidu 8 bitne digitalne reči, zatim dijagram za merenje izlaznih veličina i dijagram za njihovu obradu. Uspešno je izvršeno digitalno upravljanje jednosmernim motorom primenom tiristorskih kola. U potpunosti je digitalizovan proces merenja i njihova obrada. Identifikacija funkcije prenosa je zadovoljavajućeg kvaliteta. Pokazan je rad sistema u prisustvu poremećaj. Svi rezultati su ilustrovani kao pojedinalni grafici, koji su sastavni deo Front panela u LABVIEW-u.

## LITERATURA

- [6] Filatov, N. M., & Unbehauen, H. (2004). *Adaptive dual control: Theory and applications* (Vol. 302). Springer Science & Business Media.
- [7] WITTENMARK, Björn. Adaptive dual control methods: An overview. In: *Adaptive Systems in Control and Signal Processing 1995*. 1995. p. 67-72.
- [8] Ellis, G. (2012). *Control system design guide: using your computer to understand and diagnose feedback controllers*. Butterworth-Heinemann.
- [9] Ulrich Keuchel and Richard M. Stephan, *Microcomputer-Based Adaptive Control Applied to Thyristor-Driven DC-Motors*, 1993.
- [10] Keuchel, U., & Stephan, R. M. (2012). *Microcomputer-based adaptive control applied to thyristor-driven DC-motors*. Springer Science & Business Media
- [11] Stanković, M.; Manojlović, S.; Jovanović, Z. Acquisition system for analysis and design of electrical servo system based on USB DAQ card DT9812. *Facta Universitatis, Series: Automatic Control and Robotics*, 2012, 11: 69-79.
- [12] Stephan, R.M., V. Hahn and H. Unbehauen (1988), 'Cascade adaptive speed control of a thyristor driven DC-motor', *IEE Proc.*, 135, pp. 49-55.
- [13] Gupta, Rohit, Ruchika Lamba, and Subhransu Padhee. "Thyristor based speed control techniques of DC motor: A comparative analysis." *simulation* 3 (2012): 7.
- [14] Ringe, Ankita, Ragini Sonbarse, and Apurva Bhalerao. "Study On Speed Control of DC MOTOR Using Thyristor." (2017).
- [15] Samotyy, Volodymyr, and Ulyana Dzelendzyak. "Mathematical model of thyristor's system control of DC motor with independent excitation." *Czasopismo Techniczne* 2013. *Automatyka Zeszyt 1-AC* (2) 2013 (2013): 79-91.
- [16] Nedeljković, M., and Z. Stojiljković. "Fast current control for thyristor rectifiers." *IEE Proceedings-Electric Power Applications* 150.6 (2003): 636-638.



# ОБЈЕКТИВНА ПРОЦЕНА КВАЛИТЕТА ВИДЕО СЕКВЕНЦИ СА ПАКЕТСКИМ ГУБИЦИМА

## OBJECTIVE QUALITY ASSESSMENT OF VIDEO SEQUENCES WITH PACKET LOSSES

Марко Новчић, Бобан Бонцулић, Бобан Павловић, Јован Бајчетић, Иван Тот  
Војна академија, Универзитет одбране у Београду

*Садржај – У раду су анализирани три објективне мере за процену квалитета видео сигнала са потпуним референцирањем на изворни сигнал. Перформансе објективних мера анализирани су на три базе видео секвенци са доступним субјективним импресијама квалитета. Деградиције изворних секвенци настале су пакетским губицима.*

**Abstract** – *In this paper we analysed three objective full-reference video quality assessment metrics. Performance of the three metrics has been evaluated through three video datasets with available visual quality subjective scores. The used video quality datasets contain video sequences with degradation caused by packet losses.*

### 1. УВОД

Најпознатије мреже за пренос сигнала са пакетском комуникацијом су IP мреже. У случају видео, IP се користи за дистрибуцију у IPTV, видео позива преко мреже, разних видео стриминг сервиса преко Интернета. Провајдер не гарантује да ће садржај бити испоручен без грешака, иако он тежи да његова услуга има што бољи квалитет. Током преноса преко канала, може се десити да се у каналу неки пакети изгубе, што ће утицати на квалитет пренете секвенце. Уколико се сматра да је свака секвенца која се преноси деградирана због преноса кроз медијум, крајњи корисник на располагању има секвенцу са грешком.

У традиционалном мрежном приступу, перформансе мреже су представљене нивоом QoS (Quality of Service) израженог преко одговарајућих параметара, од којих су кључни кашњење и пакетски губици. Међутим, преко QoS се не може у потпуности омогућити објективна процена, јер није у великој сагласности са очекивањима корисника. Грешке које настају у IP мрежама, на видео секвенцама су временски краткотрајне, изненадне и појављују се на одређеним кадровима након чега нестају. Када је вредност пакетских губитака веома мала, људско око не може уочити да је дошло до деградације. Међутим, када су пакетски губици већи, долази до блоковских губитака, линијских деградација и артефаката боје [1].

У овом раду су анализирани три доступне базе видео секвенци чије су деградације настале пакетским губицима. Коришћењем три објективне мере процене квалитета и одређивањем степена слагања са субјективним проценама квалитета (Mean Opinion Scores, MOS), предложено је објективни начин мерења

квалитета видео, а који је најприближнији процени квалитета од стране посматрача.

Према доступности информација о изворном сигналу објективне мере процене квалитета слике и видео се могу поделити у три групе: без референцирања (No-Reference, NR), са потпуним референцирањем (Full-Reference, FR) и са делимичним референцирањем (Reduced-Reference, RR) на изворни сигнал [2]. У раду су коришћене објективне мере са потпуним референцирањем на изворни сигнал. Ове мере се користе у лабораторијским тестовима за избор система преноса, избор начина компресије, оптимизацију параметара преноса и оптимизацију параметара алгоритама обраде сигнала. Могу се користити и у анализи дефинисаног QoS, јер се у систему преноса јављају различите деградације изворног садржаја [3].

У другом делу рада описане су коришћене објективне мере процене квалитета. У трећем делу рада описане су базе видео секвенци и резултати поређења објективних и субјективних скорова квалитета. Најбитнији закључци и правци даљег рада дати су у последњем, четвртном делу рада.

### 2. ОБЈЕКТИВНЕ МЕРЕ ПРОЦЕНЕ КВАЛИТЕТА

За одређивање разлике две слике најчешће се користи средња квадратна грешка (Mean Squared Error, MSE), дефинисана као:

$$MSE = \frac{1}{MN} \sum_{m=1}^M \sum_{n=1}^N (R(m,n) - D(m,n))^2, \quad (1)$$

где је  $R$  изворна, а  $D$  слика са деградацијом.

Много погоднији за практичну примену је вршни однос сигнал-шум (Peak Signal to Noise Ratio, PSNR) [4], који се изражава у dB. За представу осветљености пиксела са  $p$  бита ( $2^p$  нивоа сивог), вршни однос сигнал-шум се добија као:

$$PSNR = 10 \log \frac{(2^p - 1)^2}{MSE}. \quad (2)$$

Један од стандардних објективних критеријума за процену квалитета слике је индекс структурне сличности (Structural Similarity Index, SSIM) [5]. Основна идеја која стоји иза SSIM технике је да је људско око осетљиво на деградације структура. Индекс описује квалитет поређењем локалних осветљаја, контраста и структуре између референтне и тест слике. За векторе  $x$  и  $y$ , SSIM се добија као:



$$SSIM(x, y) = l(x, y) \cdot c(x, y) \cdot s(x, y) \\ = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \cdot \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \cdot \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (3)$$

Кроз  $l(x, y)$ ,  $c(x, y)$  и  $s(x, y)$  се пореде локална обележја – осветљај, контраст и структура, тим редом. У претходном изразу,  $\mu_x$  и  $\mu_y$  су средње вредности вектора,  $\sigma_x^2$  и  $\sigma_y^2$  су варијансе вектора, а  $\sigma_{xy}$  је крос-корелација између  $x$  и  $y$ . Константе  $C_1$ ,  $C_2$  и  $C_3$  служе за стабилизацију SSIM индекса када су средње вредности и варијансе вектора мале. Често се користи поједностављена верзија SSIM индекса код које је  $C_3=C_2/2$ , па претходни израз постаје:

$$SSIM(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \cdot \frac{2\sigma_{xy} + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (4)$$

У процени квалитета слике, делови референтне и тест слике представљају векторе  $x$  и  $y$ . Средња вредност локалних SSIM вредности квалитета представља крајњу меру квалитета. Ова вредност се креће од -1 до 1, где веће вредности одговарају бољем квалитету.

У процени квалитета видео сигнала, PSNR и SSIM вредности су одређене на нивоу кадрова, а након тога су крајње вредности квалитета добијене њиховим усредњавањем (Frame PSNR и Frame SSIM вредности).

Објективна мера  $VQ^{AB}$  [6], је заснована на идеји да је систем преноса који пренесе више информација о градијенту изворне секвенце бољи. Вредност квалитета видео секвенце се добија као:

$$VQ^{AB} = k_s Q_s^{AB} + k_t Q_t^{AB} + k_c Q_c^{AB}, \quad (5)$$

где  $Q_s^{AB}$  говори о очувању просторних информација (структуре на сцени, просторне везе, ...),  $Q_t^{AB}$  о очувању временских информација (кретање објеката, оптички ток, промене у структурама и облицима током времена) и  $Q_c^{AB}$  говори о очувању боје. Очување просторних и временских информација разматра се кроз поређење просторног и временског градијента изворне и тест секвенце. Очување боје се посматра кроз промене настале у  $H$  (*hue*) и  $S$  (*saturation*) каналима HSV колор система.

Коефицијенти значаја  $k_s$ ,  $k_t$  и  $k_c$  ( $k_s+k_t+k_c=1$ ) су одређени кроз поступак оптимизације објективних скорова уз доступне субјективне резултате. Оптималне вредности коефицијената  $[k_s, k_t, k_c]=[0.8, 0.15, 0.05]$ , указују да просторни канал даје најпоузданије естимације квалитета, након чега следе временски, па хроматски канал. Динамички опсег индекса квалитета  $VQ^{AB}$  је  $[0, 1]$ , где се за тест секвенцу са већом вредношћу  $VQ^{AB}$  каже да је бољег квалитета. Додатно, мера  $VQ^{AB}$  узима у обзир промене квалитета кадрова током времена. Наиме, за крајњу вредност квалитета секвенце узима се средња вредност 20% кадрова са најнижим  $VQ^{AB}$  вредностима. Објективна мера  $VQ^{AB}$  се такође може сврстати у приступе који у процени квалитета користе очување информација о структури (кроз просторне градијенте) [6].

### 3. ОПИС БАЗА И АНАЛИЗА РЕЗУЛТАТА

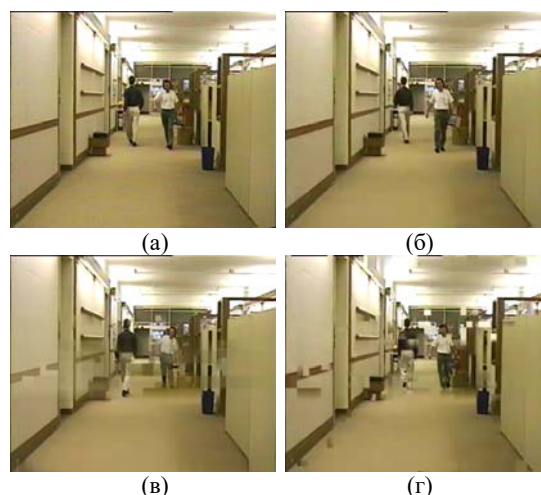
Две академске институције – Политехнички институт у Милану (Politecnico di Milano, Italy) и Политехничка школа у Лозани (Ecole Polytechnique Fédérale de Lausanne, Switzerland) направили су две базе видео секвенци кодованих са H.264/AVC енкодером и присутним пакетским губицима (Packet Loss Rate, PLR) од 0.1%, 0.4%, 1%, 3%, 5% и 10% [7]. Базе су познате као EPFL-PoliMi CIF и EPFL-PoliMi 4CIF, јер су коришћене секвенце у CIF просторној резолуцији (352x288) и у 4CIF просторној резолуцији (704x576). Саставни део база су резултати субјективних тестова.

У базама је коришћено по 6 изворних секвенци. За оригиналне секвенце прво су направљене секвенце настале компресијом. Након тога, за сваку вредност пакетских губитака направљене су по две реализације (тест секвенце). На тај начин се у базама налази по 78 секвенци (по 72 секвенце са пакетским губицима). Основни подаци о изворним секвенцама и секвенцама са компресијом су наведени у табели 1, из које се уочава да битске брзине одговарају реалним системима преноса секвенци CIF и 4CIF резолуције.

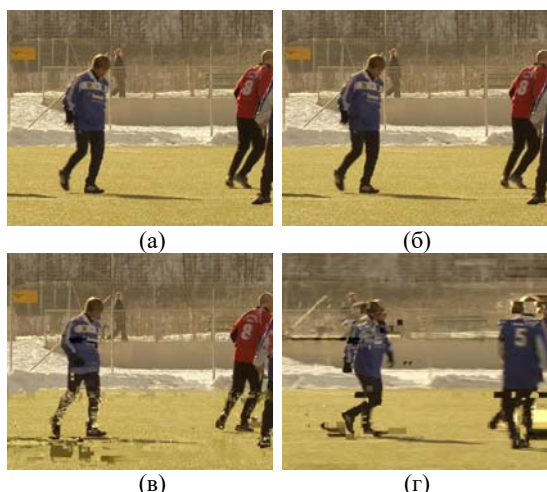
Табела 1. Приказ основних података о секвенцама из EPFL-PoliMi база

Секвенца	CIF		4CIF		
	Битска брзина [kb/s]	PSNR [dB]	Секвенца	Битска брзина [kb/s]	PSNR [dB]
Foreman	353	34.4	Ice	1325	40.8
News	283	37.3	Soccer	2871	37.2
Mobile	532	28.3	Harbour	5453	36.3
Mother	150	37.0	Crowd run	6757	33.47
Hall	216	36.2	Ducks	7851	30.43
Paris	480	33.6	Park joy	6187	31.46

На сликама 1 и 2 приказани су репрезентативни кадрови изворних и тест секвенци EPFL-PoliMi база, на којима се уочавају дисторзије настале пакетским губицима. Поред степена пакетских губитака, на сликама су дате и субјективне импресије квалитета.

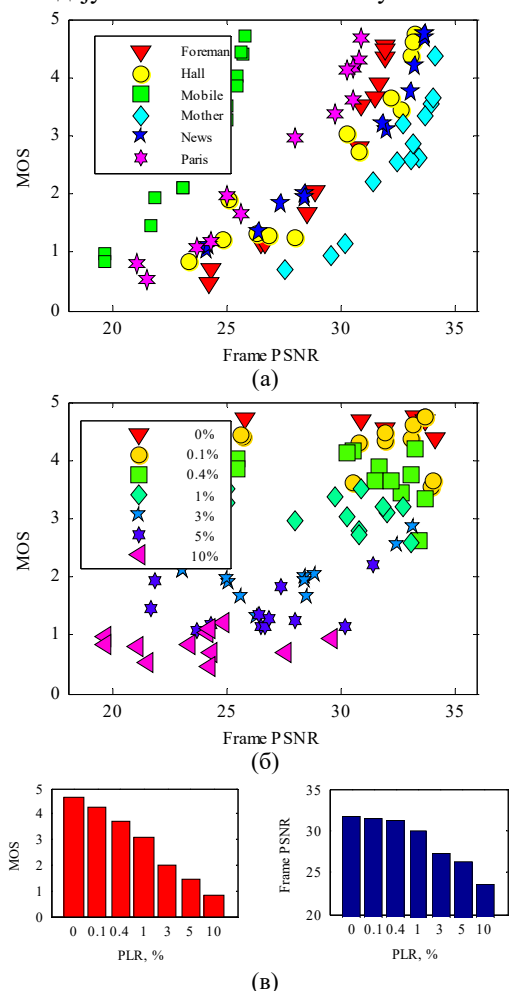


Слика 1. Приказ репрезентативних кадрова секвенце Hall са различитим нивоом деградација: (а) оригинал; (б) PLR=0%, MOS=4.74; (в) PLR=5%, MOS=1.25; (г) PLR=10%, MOS=0.84



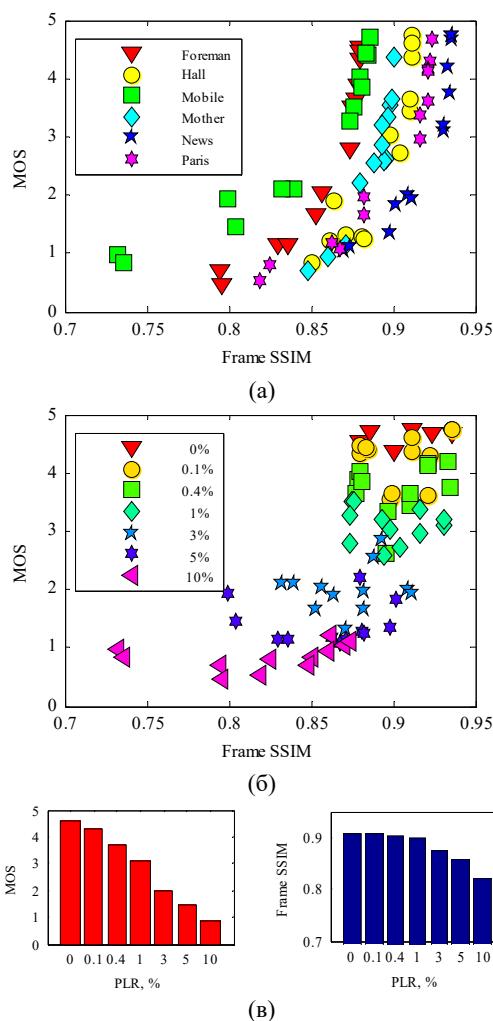
Слика 2. Приказ репрезентативних кадрова секвенце Soccer са различитим нивоом деградација: (а) оригинал; (б) PLR=0%, MOS=4.67; (в) PLR=5%, MOS=1.33; (г) PLR=10%, MOS= 0.77

Са слика 1 и 2 се уочава да се са повећањем степена пакетских губитака повећава и степен деградације сигнала. То су посматрачи учили, тако да вредности MOS опадају са повећањем степена губитака.



Слика 3. (а) (б) дијаграми расипања субјективних и Frame PSNR објективних скорова квалитета на EPFL-PoliMi CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака

На сликама 3, 4 и 5 приказани су дијаграми расипања субјективних и објективних скорова квалитета на EPFL-PoliMi CIF бази секвенци. Свака тачка на дијаграмима одговара једној тест секвенци. Дијаграми расипања приказани су према изворним секвенцама од којих су настале тест секвенце (слике (а)) и према степену пакетских губитака (слике (б)). Додатно су на сликама приказане средње вредности субјективних и објективних скорова квалитета секвенци са истим степеном пакетских губитака (слике (в)).

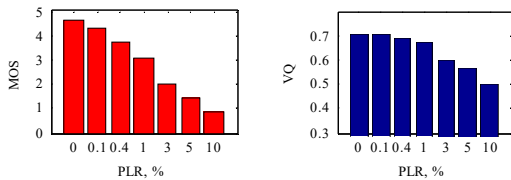
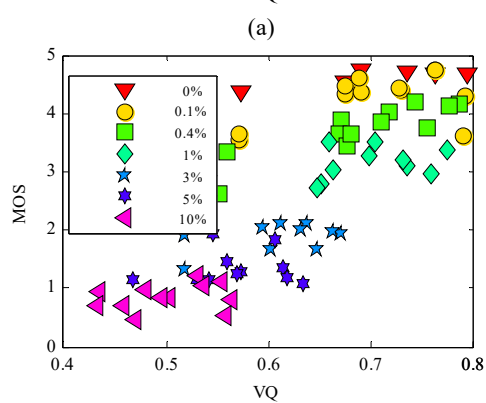
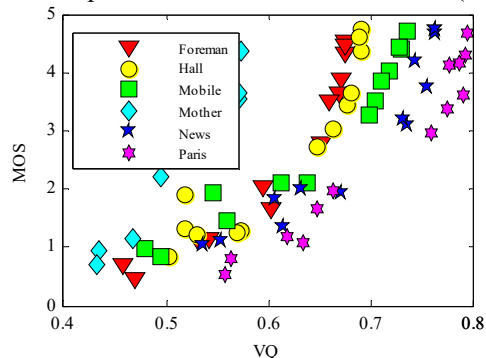


Слика 4. (а) (б) дијаграми расипања субјективних и Frame SSIM објективних скорова квалитета на EPFL-PoliMi CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака

Са слика 3, 4 и 5 се уочава значајно расипање скорова квалитета. Расипање је највеће код Frame PSNR мере, код које се скорови квалитета налазе између скорова квалитета секвенци са најмањом (Mother) и највећом битском брзином (Mobile). Такође, уочава се да објективне мере имају правилно рангирање тест секвенци које потичу од исте изворне секвенце, што се може рећи и за рангирање тест секвенци (система) са истим степеном пакетских губитака.

Степен слагања субјективних и објективних скорова квалитета дат је и кроз квантитативне мере –

коэффициент линейной корреляции (Linear Correlation Coefficient, LCC) и корреляцию рангов (Spearman Rank-Order Correlation Coefficient, SROCC). Ове две мере одређене су за подскупове секвенци које потичу од исте изворне секвенце и за комплетан сет (табела 2).



(в)

Слика 5. (а) (б) дијаграми расипања субјективних и  $VQ^{AB}$  објективних скорова квалитета на EPFL-PoliMi CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака

Табела 2. Степен слагања субјективних и објективних скорова квалитета на EPFL-PoliMi CIF бази секвенци (према изворним секвенцама и на глобалном плану)

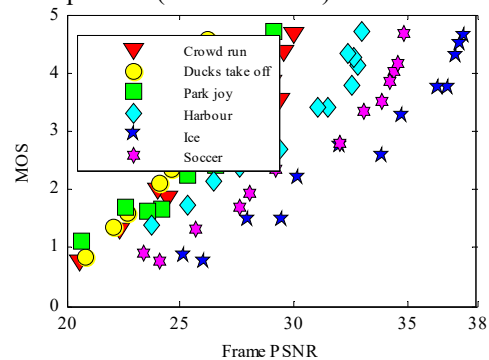
Назив секвенце	SROCC			LCC		
	Frame PSNR	Frame SSIM	$VQ^{AB}$	Frame PSNR	Frame SSIM	$VQ^{AB}$
Foreman	<b>0.989</b>	0.984	0.984	<b>0.960</b>	0.912	0.939
Hall	<b>0.934</b>	<b>0.934</b>	0.912	<b>0.933</b>	0.900	0.926
Mobile	<b>0.989</b>	0.973	0.978	<b>0.966</b>	0.931	0.962
Mother	<b>0.962</b>	0.956	<b>0.962</b>	0.935	0.931	<b>0.955</b>
News	<b>0.967</b>	0.962	0.956	<b>0.966</b>	0.911	0.939
Paris	0.984	<b>0.989</b>	0.978	<b>0.975</b>	0.932	0.969
Ср. вредн.	<b>0.971</b>	0.966	0.962	<b>0.956</b>	0.919	0.949
Цео сет	0.663	0.710	<b>0.789</b>	0.666	0.673	<b>0.778</b>

Из табеле се уочава да је степен слагања субјективних и објективних скорова квалитета на подскуповима секвенци који потичу од исте изворне секвенце веома висок. Средња вредност SROCC је већа од 0.96, док је средња вредност LCC већа од 0.91. На највећем броју подскупова највећи степен слагања са субјективним

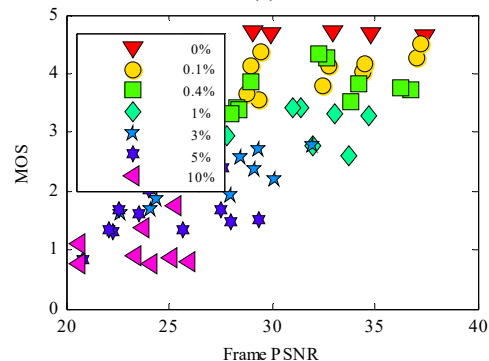
импресијама има Frame PSNR објективна мера. Међутим, она има најмањи степен слагања на глобалном плану – комплетној бази. На комплетној бази најбоље слагање са резултатима субјективних тестова има  $VQ^{AB}$  мера. Степен слагања објективних и субјективних скорова квалитета на комплетној бази је значајно мањи од степена слагања на подскуповима.

Степен слагања средњих вредности субјективних и објективних скорова квалитета на подскуповима са истим степеном пакетских губитака је такође висок. Корелација рангова је максимална (што се уочава и са слика 3, 4 и 5), док су вредности линеарних корелација:  $LCC_{PSNR}=0.98$ ,  $LCC_{SSIM}=0.93$  и  $LCC_{VQ}=0.97$ .

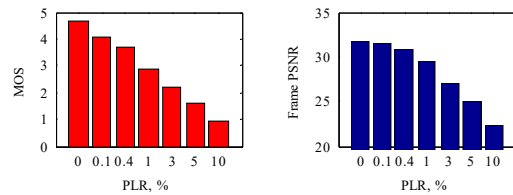
На сликама 6, 7 и 8 приказани су дијаграми расипања субјективних и објективних скорова квалитета на EPFL-PoliMi 4CIF бази секвенци. Са слика се уочава расипање скорова квалитета, која је нешто мање него код базе са секвенцама CIF просторне резолуције. Расипање је највеће код Frame SSIM мере. Скорови квалитета Frame PSNR мере се налазе између скорова квалитета секвенци са најмањом (Ice) и највећом битском брзином (Ducks take off).



(а)

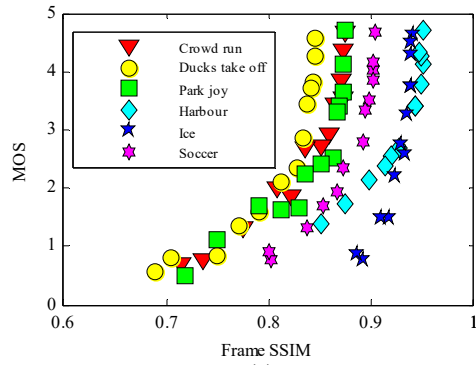


(б)

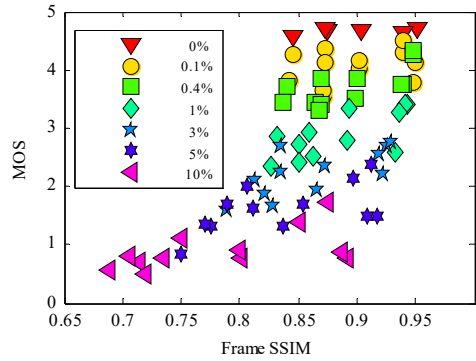


(в)

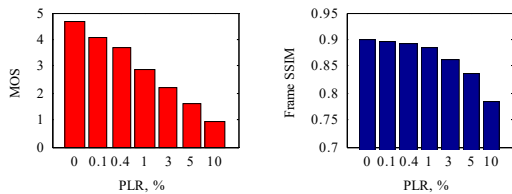
Слика 6. (а) (б) дијаграми расипања субјективних и Frame PSNR објективних скорова квалитета на EPFL-PoliMi 4CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака



(a)



(b)



(b)

Слика 7. (а) (б) дијаграми расипања субјективних и Frame SSIM објективних скорова квалитета на EPFL-PoliMi 4CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака

Са слика 6, 7 и 8 уочава се да објективне мере имају правилно рангирање тест секвенци које потичу од исте изворне секвенце, што се може рећи и за рангирање тест секвенци (система) са истим степеном пакетских губитака. У табели 3 дате су вредности корелација субјективних и објективних скорова квалитета.

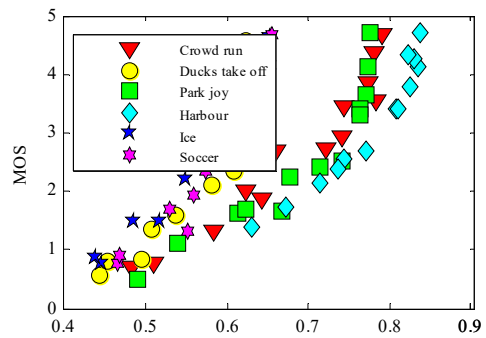
Табела 3. Степен слагања субјективних и објективних скорова квалитета на EPFL-PoliMi 4CIF бази секвенци (према изворним секвенцама и на глобалном плану)

Назив секвенце	SROCC			LCC		
	Frame PSNR	Frame SSIM	$VQ^{AB}$	Frame PSNR	Frame SSIM	$VQ^{AB}$
Crowd run	0.989	0.989	0.978	0.976	0.931	0.959
Ducks	1	1	0.995	0.950	0.899	0.916
Park joy	0.984	0.984	0.995	0.942	0.878	0.918
Harbour	0.956	0.956	0.962	0.973	0.926	0.956
Ice	0.984	0.984	0.984	0.977	0.920	0.963
Soccer	0.994	0.995	0.989	0.980	0.931	0.946
Ср. вредн.	0.994	0.984	0.984	0.966	0.914	0.943
Цео сет	0.774	0.634	0.731	0.770	0.670	0.736

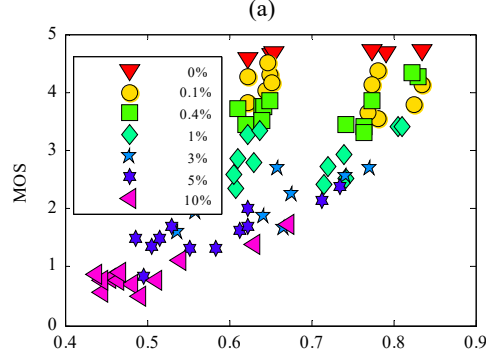
Из табеле 3 се уочава да је степен слагања субјективних и објективних скорова квалитета на подскуповима секвенци који потичу од исте изворне секвенце веома висок. Средња вредност SROCC је већа

од 0.98, док је средња вредност LCC већа од 0.91. На највећем броју подскупова највећи степен слагања са субјективним импресијама има Frame PSNR објективна мера, а која је најуспешнија и на глобалном плану. Степен слагања субјективних и објективних скорова квалитета на комплетној бази је значајно мањи од степена слагања на подскуповима.

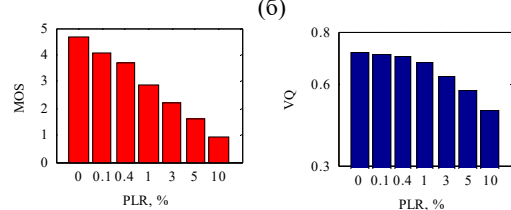
Степен слагања средњих вредности субјективних и објективних скорова квалитета на подскуповима са истим степеном пакетских губитака је такође висок. Корелација рангова је максимална (што се уочава и са слика 6, 7 и 8), док су вредности линеарних корелација:  $LCC_{PSNR}=0.97$ ,  $LCC_{SSIM}=0.92$  и  $LCC_{VQ}=0.95$ .



(a)



(b)

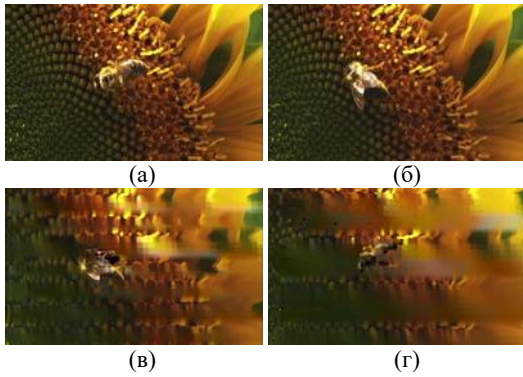


(b)

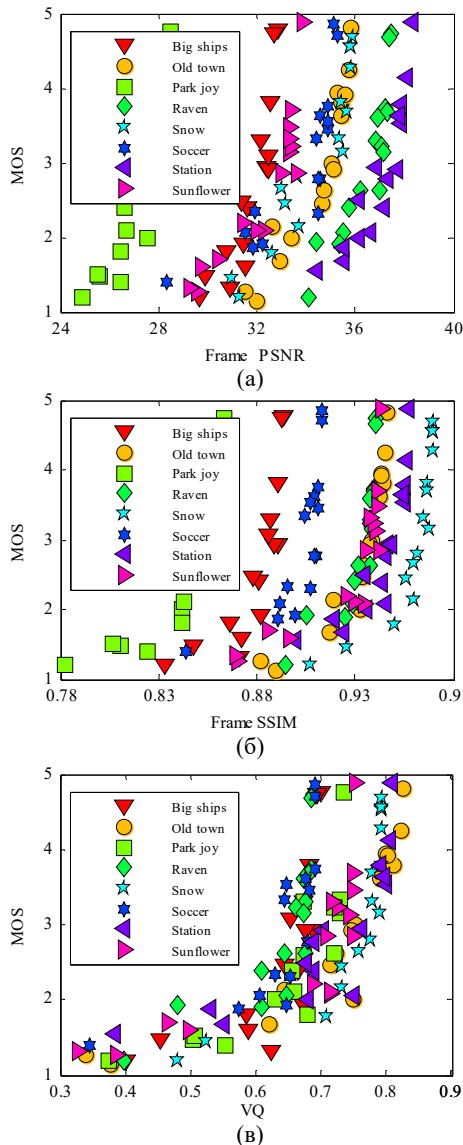
Слика 8. (а) (б) дијаграми расипања субјективних и  $VQ^{AB}$  објективних скорова квалитета на EPFL-PoliMi 4CIF бази секвенци и (в) средње вредности субјективних и објективних скорова према степену пакетских губитака

IT база видео секвенци [8], садржи 8 изворних секвенци, које су у 480p просторној резолуцији (720x480). Тест секвенце су добијене кодовањем са H.264/AVC енкодером (за битске брзине од 1 Mb/s до 5 Mb/s) и увођењем пакетских губитака од 0.17% до 7.9%. За сваку изворну секвенцу направљено је по 14 реализација пакетских губитака, што чини укупно 112 тест секвенци. Субјективне импресије квалитета су саставни део базе. Приказ репрезентативних кадрова из ове базе дат је на слици 9.





Слика 9. Приказ репрезентативних кадра секвенце Sunflower са различитим нивоом деградација: (а) оригинал; (б) PLR=0%, MOS=4.88; (в) PLR=3.86%, MOS=1.60; (г) PLR=7.75%, MOS=1.33



Слика 10. Дијаграми расипања субјективних и објективних скорова квалитета на IT бази секвенци

На слици 10 приказани су дијаграми расипања субјективних и објективних скорова квалитета на IT бази секвенци, са које се уочава најмање расипање код  $VQ^{AB}$  објективне мере. Квантитативни показатељи слагања субјективних и објективних скорова квалитета дати су у табели 4.

Табела 4. Степен слагања субјективних и објективних скорова квалитета на IT бази секвенци

Назив секвенце	SROCC			LCC		
	Frame PSNR	Frame SSIM	$VQ^{AB}$	Frame PSNR	Frame SSIM	$VQ^{AB}$
Big ships	0.925	<b>0.928</b>	0.889	<b>0.858</b>	0.766	0.695
Old town	0.961	<b>0.978</b>	0.946	<b>0.919</b>	0.857	0.842
Park joy	0.907	<b>0.961</b>	0.875	<b>0.862</b>	0.812	0.782
Raven	0.925	<b>0.968</b>	0.936	<b>0.883</b>	0.793	0.754
Snow	0.950	<b>0.968</b>	0.964	<b>0.936</b>	0.809	0.788
Soccer	<b>0.904</b>	0.893	0.839	<b>0.801</b>	0.688	0.652
Station	<b>0.961</b>	0.950	0.932	<b>0.891</b>	0.823	0.797
Sunflower	0.893	<b>0.907</b>	<b>0.907</b>	<b>0.883</b>	0.801	0.777
Ср. вредн.	0.928	<b>0.944</b>	0.911	<b>0.879</b>	0.794	0.761
Цео сеп	0.542	0.531	<b>0.752</b>	0.500	0.493	<b>0.728</b>

Из табеле 4 се уочава висок степен слагања субјективних и објективних скорова квалитета на подкуповима секвенци. Међутим, слагање на глобалном плану је значајно лошије, где је на нивоу комплетне базе најбоље слагање субјективних и  $VQ^{AB}$  објективних скорова квалитета.

#### 4. ЗАКЉУЧАК

У раду су анализирани перформансе три објективне мере у процени квалитета секвенци насталих компресијом и симулацијом пакетских губитака током преноса. Показано је да објективне мере имају висок степен слагања са резултатима субјективних тестова на подкуповима секвенци који потичу од исте изворне секвенце или на подкуповима са истим степеном пакетских губитака. Перформансе објективних мера су значајно лошије на комплетним базама него на подкуповима, што даје простора за унапређење објективних мера. У даљем раду спроведена анализа биће проширена са новим базама видео секвенци и са новим објективним мерама.

#### ЗАХВАЛНИЦА

Ово истраживање је део пројекта ВА-ТТ/1-17-19 подржаног од стране Министарства одбране Р. Србије.

#### ЛИТЕРАТУРА

- [1] Станојевић Д., Бонцулић Б., Павловић Б., Петровић В. „Утицај параметара квалитета сервиса на субјективну и објективну процену квалитета видео”, Зборник 61. конференције за ЕТРАН, стр. ТЕ1.5.1-6, Кладово, Србија, 05.-08. јун 2017.
- [2] Стојановић Н. „Анализа квалитета преноса покретне слике у оквиру бежичних мултимедијалних сензорских мрежа”, Мастер рад, Електротехнички факултет, Београд, 2016.
- [3] Бонцулић Б., Петровић В., Павловић Б., Крстић Н. „Објективна процена квалитета видео секвенци са малим битским брзинама”, Зборник радова XXXIII симпозијума ПосТел, стр. 275-284, Београд, Србија, 1. и 2. децембар 2015.
- [4] Wang Z., Bovik A.C. „Mean squared error: Love it or leave it? A new look at signal fidelity measures”, IEEE Signal Processing Magazine, Vol. 26, No. 1, pp. 98-117, 2009.
- [5] Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P. „Image quality assessment: From error visibility to structural similarity”, IEEE Transactions on Image Processing, Vol. 13, No. 4, pp. 600-612, 2004.
- [6] Бонцулић Б. „Процена квалитета слике и видео кроз очување информација о градијенту”, Докторска дисертација, Факултет техничких наука, Нови Сад, 2016.
- [7] De Simone F., Naccari M., Tagliasacchi M., Dufaux F., Tubaro S., Ebrahimi T. „Subjective quality assessment of H.264/AVC video streaming with packet losses”, EURASIP Journal on Image and Video Processing, Article 190431, pp. 1-12, 2011.
- [8] [http://amalia.img.lx.it.pt/%7Eetgsb/H264\\_test/](http://amalia.img.lx.it.pt/%7Eetgsb/H264_test/)



# ANALYSIS OF FINITE DIGITAL WORD LENGTH EFFECTS DURING IMPLEMENTATION OF IIR FILTERS

## ANALIZA EFEKATA KONAČNE DUŽINE DIGITALNE REČI PRI IMPLEMENTACIJI IIR FILTARA

Filip Mladenović, Boban Bondžulić, Milenko Andrić, Davorin Mikluc  
*University of Defence in Belgrade, Military academy*

**Abstract** - In this paper effects of finite digital word length were analyzed in infinite impulse response (IIR) filters implementation. Analysis was performed using codeword lengths of 12, 10 and 8 bits. The main goal is to find optimal realization structure, in order to minimize the effects of finite digital word length. Three realization structures were used: direct, cascade and parallel. Finite codeword length affects filters stability which was shown. The effects analysis is performed in licenced software MATLAB™.

**Sadržaj** – U ovom radu efekti konačne dužine digitalne reči su analizirani na filterima beskonačnog impulsnog odziva (infinite impulse response) IIR filterima. Analiza je sprovedena korišćenjem dužine kodne reči od 12, 10 i 8 bita. Cilj rada je u pronalaženju optimalne realizacione strukture filtra kako bi se minimizovao efekat konačne dužine digitalne reči. Korišćene su tri realizacione strukture: direktna, kaskadna i paralelna. Prikazan je uticaj konačne dužine kodne reči na stabilnost filtra. Analiza je sprovedena u licenciranom softveru MATLAB™.

### 1. INTRODUCTION

During digital signal processing (DSP) the main criteria are processing rate, especially if it is required real-time work and low rate of possible errors at system output.

Implementation of digital filters can be software or hardware. In both cases the coefficients and multiplication constants can only be implemented with finite codeword length. This is the reason for occurrence of finite word length effects. The effects can degrade designed filter characteristics and system performance. These effects can be reduced by selecting appropriate realization structure of filter [1].

Filter of finite impulse response (FIR) or infinite impulse response (IIR) can be used in DSP, regarding system requirements. By using IIR filters, required amplitude characteristic is realized with low filter order. In other case, FIR filters are used if system requires linear phase characteristic and to avoid feedback. Same filter specifications can be achieved with much lower IIR filter order than the FIR, regarding complexity of its realization.

Some errors of presenting numbers may occur during implementation of digital processing algorithms. These

errors are products of finite digital word length. Possible sources of errors are:

- quantization of the input signal;
- filter coefficient quantization;
- quantization of multiplication results;
- overflow during summing;
- limit cycles [2].

The main goal of this paper is representation of finite word length effects to IIR filters implementation. The effects analysis is performed in licenced software MATLAB™ [3, 4].

### 2. REALIZATION STRUCTURES OF IIR FILTERS

IIR filter transfer function is defined as the quotient of two polynomials:

$$H(z) = \frac{Y(z)}{X(z)} = \frac{\sum_{k=0}^N a_k z^{-k}}{1 + \sum_{k=1}^M b_k z^{-k}} = \frac{A(z^{-1})}{B(z^{-1})} \quad (1)$$

where  $H(z)$  is transfer function,  $a_k$  and  $b_k$  are coefficients,  $z$  is complex variable,  $N$  and  $M$  are constants, where  $M \geq N$ .

IIR filter can be also described by the difference equation:

$$y(n) + \sum_{k=1}^M b_k y(n-k) = \sum_{k=0}^N a_k x(n-k), \quad (2)$$

where  $x(n)$  is input sequence and  $y(n)$  is output sequence. Further, it is used  $M = N$ .

Transfer function can be implemented in different ways. Basic realization structures are analyzed in this section. They are: direct, cascade and parallel realization structures. The main criteria for realization structure selection are: the effects of finite-length digital words and real time work [5,6].

The structure, which has the same multiplication constants as coefficients in transfer function, is called a direct realization structure. According to equation (1), direct realization form is given in Figure 1.

In practice transposed direct realization structure is more often used. Transposed realization structure is given in Figure 2. As can be seen, transposed structure has less delay blocks than direct and therefore output signal has less delay relative to the input. Also it requires less

memory than ordinary direct form. However, the impact of the digital word length remains the same as for regular direct structure.

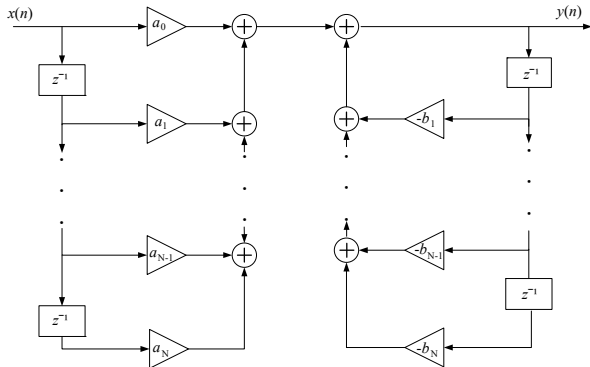


Figure 1. Direct realization structure

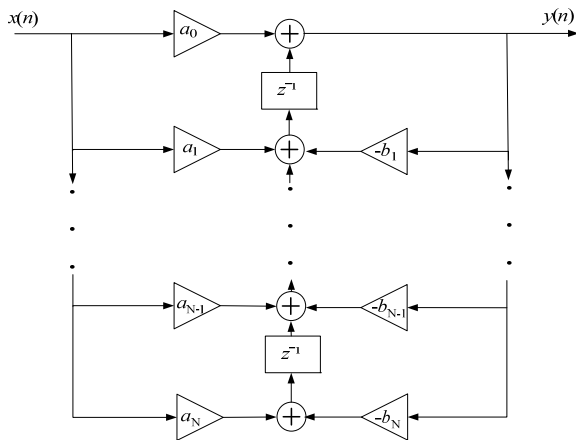


Figure 2. Transposed direct realization structure

Practice has proved that the effects of finite word length are less by using cascade or parallel realization structures that consist of a section of the first and second order [6]. Figures 3 and 4 show a section of the first and second order, respectively.

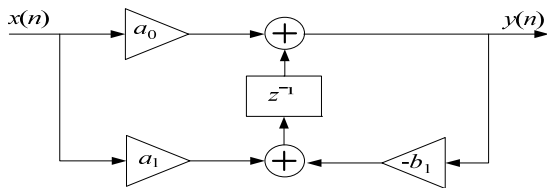


Figure 3. Direct transposed form of first order section

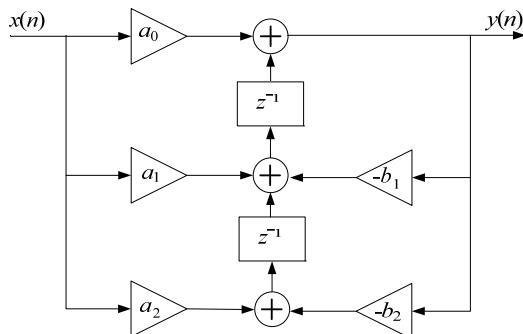


Figure 4. Direct transposed form of second order section

Cascade realization structure is obtained by presenting transfer function as a multiplication of a lower order transfer functions:

$$H(z) = \prod_{i=1}^K H_i(z) = C \frac{1 + a_r z^{-1}}{1 + b_r z^{-1}} \prod_{i=1}^{\frac{N-1}{2}} \frac{1 + a_{1i} z^{-1} + a_{2i} z^{-2}}{1 + b_{1i} z^{-1} + b_{2i} z^{-2}} \quad (3)$$

where  $K$  is number of sections,  $N$  is odd filter order,  $C$  is a constant,  $a_r$  and  $b_r$  are coefficients of first order section, and  $a_{1i}$ ,  $a_{2i}$ ,  $b_{1i}$ ,  $b_{2i}$  are coefficients of second order sections.

For even filter order  $N$  transfer function is:

$$H(z) = \prod_{i=1}^K H_i(z) = C \prod_{i=1}^{\frac{N}{2}} \frac{1 + a_{1i} z^{-1} + a_{2i} z^{-2}}{1 + b_{1i} z^{-1} + b_{2i} z^{-2}} \quad (4)$$

Figure 5 shows block diagram of cascade realization structure.

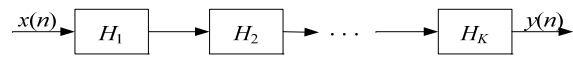


Figure 5. Block diagram of cascade realization structure

To ensure less movement of poles and zeros during quantization, it is necessary to reduce their mutual influence. This is achieved by grouping the poles and zeros.

First of all, determine which pair of conjugate complex poles is closest to the unit circle. Then determine the nearest zero to this pair of poles, and group them. This results in a second-order section. This procedure is repeated for the rest complex conjugate poles and their matched zeros. Then it continues with the grouping real poles with one their nearest zero thereby forming a section of the first order. By this method, all the sections are determined. However, to ensure a minimal effect of finite length codeword, it is necessary to select an optimum order of these sections. A cascade realization structure in practice has shown good results in designing the filters with zeros on the unit cycle [1].

Parallel realization structure is obtained by decomposing transfer function in partial fractions:

$$H(z) = H_0 + \sum_{i=1}^K H_i(z) \quad (5)$$

where for first order section:

$$H_i(z) = \frac{a_{0i}}{1 + b_{1i} z^{-1}}, \quad (6)$$

and for the second order section:

$$H_i(z) = \frac{a_{0i} + a_{1i} z^{-1}}{1 + b_{1i} z^{-1} + b_{2i} z^{-2}}. \quad (7)$$

Figure 6 shows the block diagram of parallel realization structure which is also used to minimize the effects of finite-length digital word as it is in cascade.

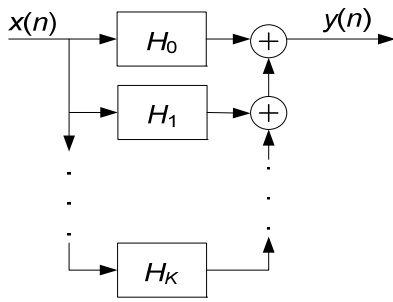


Figure 6. Block diagram of the parallel realization structure

### 3. RESULTS

#### Example 1. Effects of finite codeword length on attenuation characteristics of different realization structures

Elliptic band pass filter specifications that is analyzed are:

- filter order:  $N = 6$ ;
- bandwidth:  $\omega_p = (0.3 \div 0.6)\pi$ ;
- maximal ripple in the pass-band:  $a_p = 0.5\text{dB}$ ;
- minimal required attenuation in stop-bands:  $a_a = 40\text{dB}$ .

Analysis of the finite digital word effects are performed using  $L=12, 10$  and  $8$  bits, on previously mentioned realization structures. Their coefficients are limited by the method of rounding. According to filter order, three sections of second order were used in parallel and cascade structures. For further analysis was used attenuation characteristic, which is defined as:

$$a(\omega) = -20 \log |H(e^{j\omega})|, \quad (8)$$

where  $H(e^{j\omega})$  is filter frequency response.

Figures 7, 8, and 9 show zoomed pass-band of attenuation characteristic of direct, cascade and parallel realization structure, respectively.

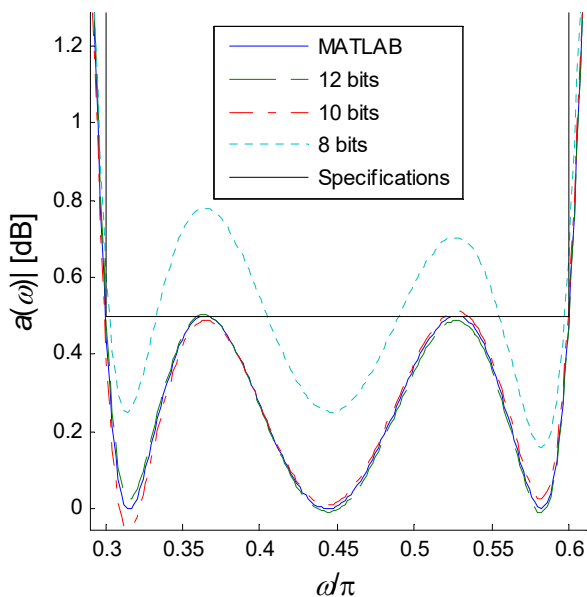


Figure 7. Direct realization – attenuation (pass-band)

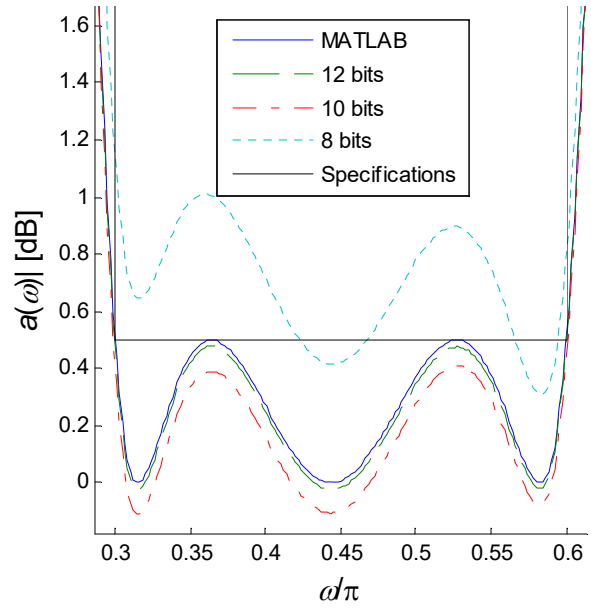


Figure 8. Cascade realization – attenuation (pass-band)

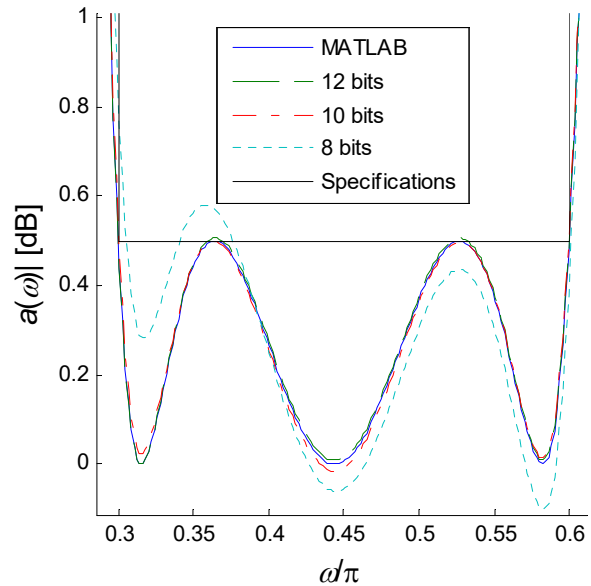


Figure 9. Parallel realization – attenuation (pass-band)

From Figures 7, 8 and 9 can be concluded that the attenuation characteristic gets worse with reduced codeword length.

Figures 10, 11 and 12 show attenuation characteristics of different types of realization with codeword lengths  $L=12, 10, 8$ , respectively.

As it can be seen on Figure 10, optimal realization structure of minimal fluctuation aspect in band-pass is cascade, and for minimal attenuation in stop band is parallel.

From Figure 11a it can be noticed that direct form does not fulfill specification of maximal attenuation in band-pass, as well as stop-bands specification. Figure 11b shows that cascade form is the nearest to satisfy specification in stop-bands.

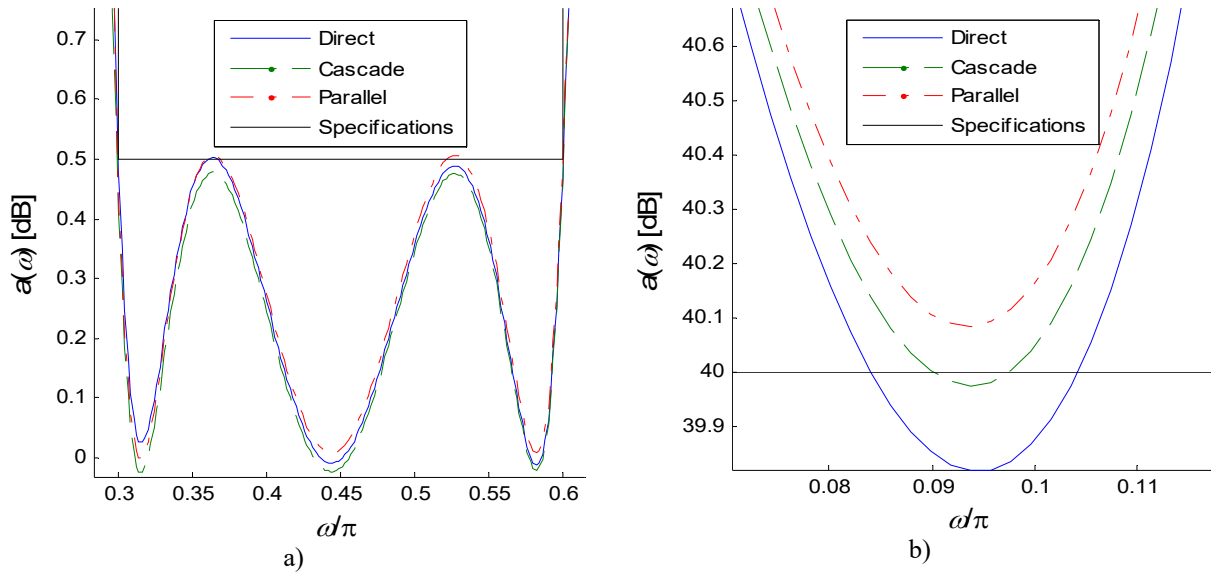


Figure 10. Comparison of realization structures for  $L=12$  bits: a) zoomed pass-band, b) zoomed LF stop-band

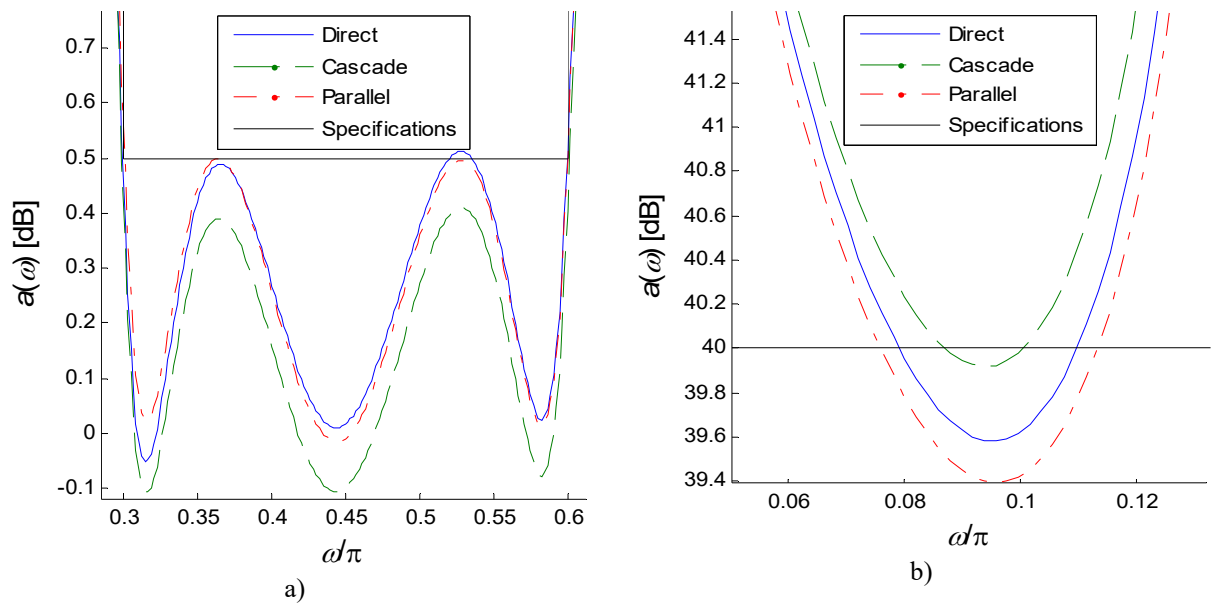


Figure 11. Comparison of realization structures for  $L=10$  bits: a) zoomed pass-band, b) zoomed LF stop-band

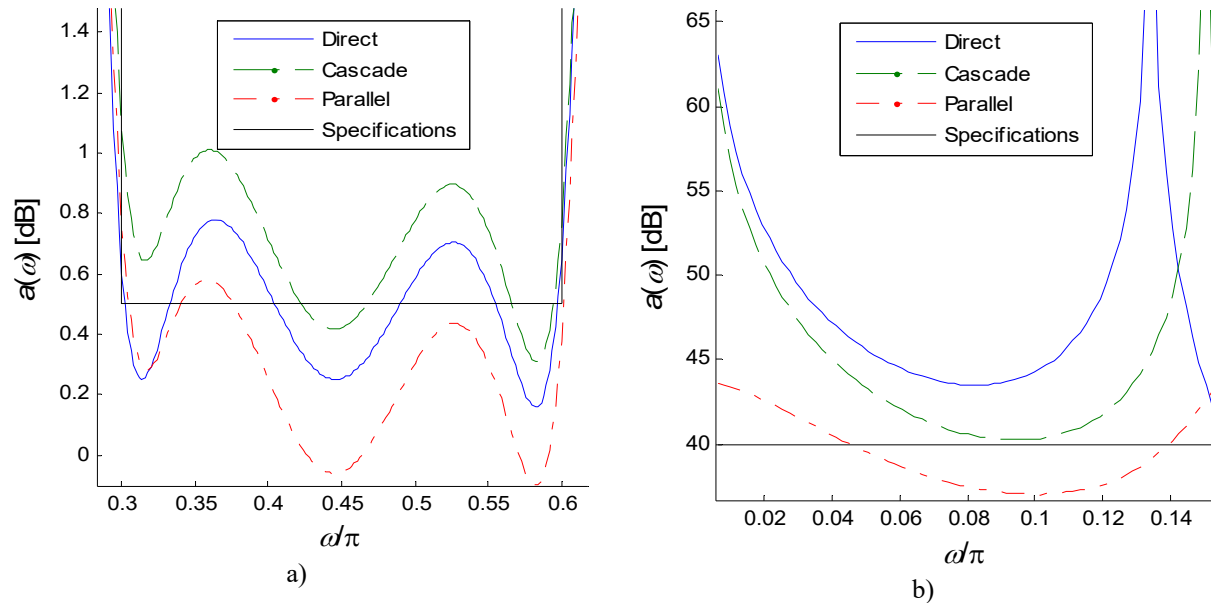


Figure 12. Comparison of realization structures for  $L=8$  bits: a) zoomed pass-band, b) zoomed LF stop-band

From Figure 12a can be seen that the best resistance of characteristic in pass band with reduced codeword length shows parallel realization structure. Direct realization form has the best characteristic in stop band as it can be seen on Figure 12b.

According to theory, the results confirmed that cascade form is optimal realization structure for this filter (with zeros on unit cycle) as it can be seen from Figures 10 and 11.

Depending on in which band filter characteristics does not fulfill specifications, it can be used following procedure to optimize it:

- If filter characteristic in band pass is better than specified, it needs to modify filter specifications. Maximal allowed variation of attenuation in pass-band for new filter needs to increase. This will increase attenuation in stop-band too.

- If characteristic in stop-band is better than specified, and variation of attenuation in band-pass is higher then allowed, it needs to decrease attenuation in pass band.
- Last and the worst case is that filter characteristic does not satisfy specifications in both bands (stop and pass). In that case it needs to get higher filter order [1].

**Example 2. Finite codeword length effects on filter stability**

This effect is tested on Chebyshev Type II low pass filter, which specifications are:

- filter order:  $N = 4$ ;
- bandwidth:  $\omega_p = 0.0625\pi$ ;
- maximal ripple in the pass-band:  $a_p = 1\text{dB}$ ;
- minimal required attenuation in stop-band:  $a_s = 40\text{dB}$ .

Coefficients of this filter are quantized with codeword length  $L = 8$ . Figure 13 shows position of zeros and poles in z-plane with and without quantization.

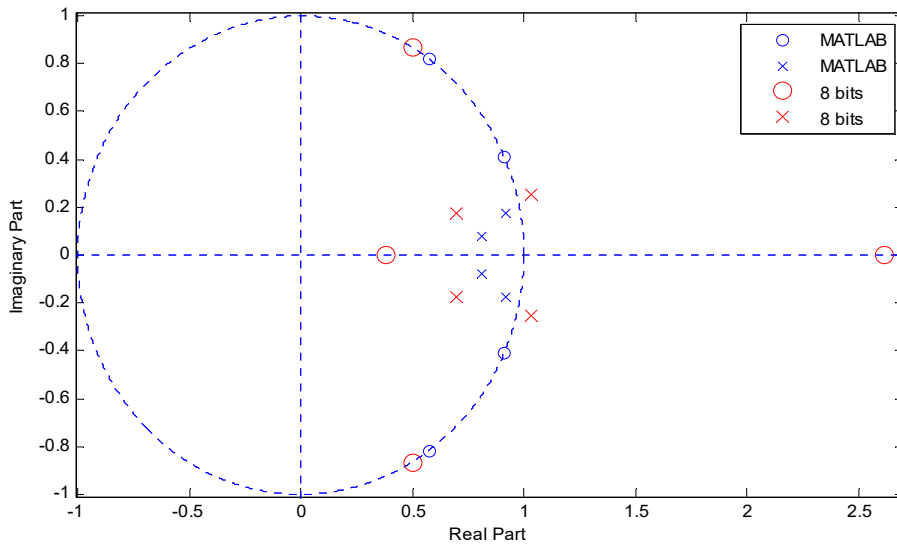


Figure 13. Zeros and poles positions of Chebyshev filter with and without quantization

As it can be seen on Figure 13, this filter became unstable after quantization, since one pair of poles went out of unit cycle (x marks - colored red).

Figure 14 shows input signal (Delta pulse),

$$\delta(n) = \begin{cases} 1, & n = 0 \\ 0, & n > 0 \end{cases} \quad (9)$$

and impulse response of this filter, which coefficients are quantized.

From Figure 14b it can be seen that impulse response diverges, which also means that this filter is unstable.

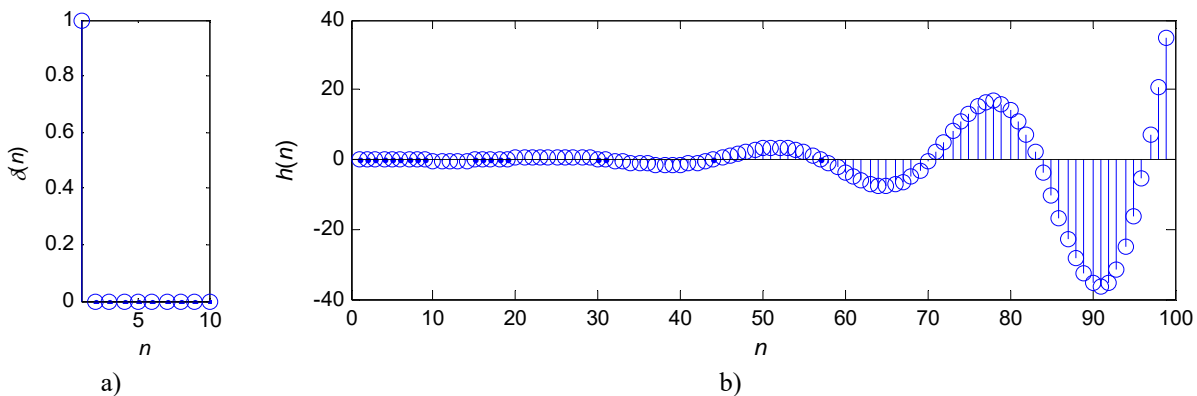


Figure 14. a) Delta pulse and b) filter impulse response



#### 4. CONCLUSION

In this paper effects of finite digital word length were analyzed in IIR filters implementation. Analysis was performed using codeword lengths of 12, 10 and 8 bits. Results show that lowering codeword length provides deviation of desirable filter characteristic. Based on band where attenuation did not accomplish given specifications, several suggestions have been given to minimize undesirable effects.

Selection of realization structure affects level of exception from given specifications of the designed filter. First example showed that optimal realization structure for filters with zeros distributed on unit cycle is cascade. The most robust on lowering the codeword length is parallel structure, regarding pass band, while it showed poorly in suppressed band. Direct realization structure has proved as the worst and it is rarely used in practice.

Lowering the codeword length affect distribution of zeros and poles can cause filter instability. If filter goes unstable, another realization structure has to be performed, in order to minimize its effect on poles distribution. If this can not be provided, new filter design has to be considered which will ensure poles closer to origin.

Future work will stand upon projecting and analysis of combined different realization structures to minimize these effects as much as it is possible. Additionally, digital filtering will be implemented on signal processors or FPGA.

#### BIBLIOGRAPHY

- [1] Milić, Lj. and Dobrosavljević, Z. "Introduction to Digital Signal Processing", *Academic Mind*, Belgrade 2009, pp. 291-330. ISBN 978-86-7466-367-7 (in Serbian)
- [2] Čertić, J. "Efficient implementation of algorithms for digital filtering and spectral analysis on signal processors", Magister thesis, School of Electrical Engineering (in Serbian), 2007.
- [3] Blanchet, G. and Charbit, M. "Digital Signal and Image Processing Using MATLAB", *ISTE Ltd.*, London 2006, ISBN 13: 978-1-905209-13-2
- [4] Taylor, F. "Digital Filters Principles and Applications with MATLAB", *John Wiley & Sons*, New Jersey, 2012 ISBN 978-0-470-77039-9
- [5] Stojić, M. "Digital control systems", *Science*, Belgrade 1990, pp. 109-119. ISBN 86-7621-017-9 (in Serbian)
- [6] Mladenović, F. "Analysis of finite digital word length effects on filter characteristics", Graduate thesis, Military academy, 2014.

# UTICAJ WRED MEHANIZMA NA KVALITET SERVISA U PAKETSKIM MREŽAMA

## THE EFFECT OF WRED MECHANISM ON QUALITY OF SERVICE IN PACKET DEFINED NETWORKS

Katarina Manojlović, Boban Pavlović  
Vojna akademija, Univerzitet Odbrane u Beogradu

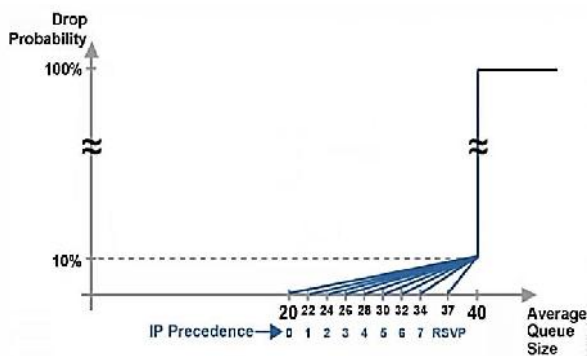
**Sadržaj** – U ovom radu su potvrđene pretpostavke o uticaju WRED mehanizma na parametre kvaliteta servisa (procenat izgubljenih paketa, jednosmerno kašnjenje, vrednost popusnog opsega, MOS parametar i izgubljeni fejmovi video-stream-a), a u cilju izbegavanja zagušenja na mreži uz očuvanje konekcije sa prioritetom.

**Abstract** – This paper confirms the assumptions about the influence of the WRED mechanism on the QoS parameters (the percentage of lost packets, one-way delay, bandwidth, MOS parameter and lost frames of video streams) in order to avoid network congestion while preserving the priority connection.

### 1. UVOD

**RED** – Random Early Detection je mehanizam za izbegavanje zagušenja na mreži selektivno odbacujući pakete pre nego što dođe do punjenja bafera i signalizira individualnim konekcijama da spuste brzinu slanja paketa [1].

**WRED** – Weighted RED mehanizam jeste Cisco-ova implementacija prethodno definisanog mehanizma uz razliku upotrebe takozvanih težinskih koeficijenata ili atributa koji se koriste za donošenje odluke o odbacivanju paketa. Atributi mogu biti zadati na osnovu IP precedence ili DiffService Code Point (DSCP) vednosti. Karakteristike verovatnoće odbacivanja paketa prikazane su na slici 1 i pokazuju kako se minimalne vrednosti praga menjaju sa promenom težinskih atributa. Ovim je omogućeno selektivno odbacivanje paketa nižeg prioriteta.

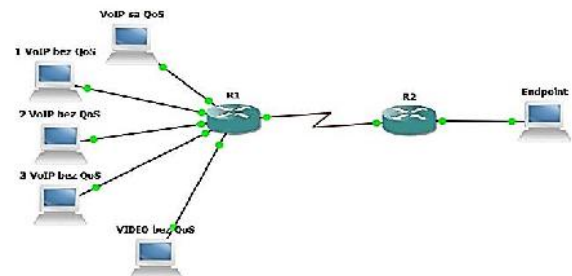


Slika 1. Krive verovatnoća odbacivanja paketa uz primenu WRED mehanizma

Pored WRED mehanizma, postoje i drugi mehanizmi koji pomažu pri ostvarivanju kvaliteta servisa i izbegavanju zagušenja na mreži, među kojima se izdvajaju primena politike redova čekanja (Queueing) i primena politike limitiranja saobraćaja (Policing).

### 2. PRIKAZ SIMULIRANOG LINKA

Praktična analiza uticaja mehanizama za izbegavanje zagušenja na mreži prikazana je na slici 2. Mreža se sastoji iz dva Cisco rutera međusobno povezanim linkom kapaciteta ograničenim na 1Mb/s. Na jednoj strani se nalazi pet izvora saobraćaja i to tri izvora VoIP saobraćaja koji nemaju prioritet, jedan izvor VoIP saobraćaja sa prioritetom i jedan izvor video saobraćaja, dok na drugoj strani je samo jedna krajnja radna tačka. Kompleksnost mreže je uprošćena upotrebom simulatora IxChariot pomoću kog je na konzolnoj strani svih pet izvora svedeno na jedan računar na kom su vršena merenja i odakle je simuliran sav neophodan saobraćaj.



Slika 2. Prikaz mrežne konfiguracije za simulaciju

Parametri koji će se upoređivati u izvedbi sa aktiviranim mehanizmom WRED i bez istog jesu: gubitak paketa izražen u procentima, jednostrano kašnjenje, propusna moć, MOS parametar i gubitak frejmova video saobraćaja.

### 3. KOD ZA PRIMENU WRED MEHANIZMA

Niže navedenim kodom je definisana klasna mapa naziva DSCP\_EF u koju se smešta sav saobraćaj koji ima dscp atribut jednak ef (atribut ef ima VoIP saobraćaj sa prioritetom) i definisana je klasna mapa naziva DSCP\_AF11\_AF23 u koju se smešta saobraćaj dscp atributa af11 (VoIP saobraćaj bez prioriteta) i atributa af23 (video saobraćaj) [2,3,4].

Nakon definisanja klasnih mapa, pristupa se definisanju polisne mape naziva WRED u okviru koje se klasnoj mapi DSCP\_EF garantuje propusni opseg koji je jednak osam procenata ukupne propusne moći, zatim se klasnoj mapi DSCP\_AF11\_AF23 dodeljuje osamdesetsedam procenata propusnog opsega i pet procenata je preostalo za sav ostali saobraćaj koji ne pripada ovim dvema klasnim mapama. U klasnoj mapi DSCP\_AF11\_AF23 u okviru polisne mape se još definišu minimalna i maksimalna vrednost praga za svaku od navedenih vrsta saobraćaja, kao i verovatnoća odbacivanja (1/10) paketa. Po završetku definisanja

polisne mape, preostaje samo da se ista primeni na konkretni izlazni interfejs rutera [5].

```

Router1> enable
Router1# conf t
Router1(config)# class-map DSCP_EF
Router1(config-cmap)# match dscp ef
Router1(config-cmap)# exit
Router1(config)# class-map DSCP_AF11_AF23
Router1(config-cmap)# match dscp af11 af23
Router1(config)# policy-map WRED
Router1(config-pmap)# class DSCP_EF
Router1(config-pmap-c)# bandwidth percent 8
Router1(config-pmap-c)# exit
Router1(config-pmap)# class DSCP_AF11_AF23
Router1(config-pmap-c)# bandwidth percent 87
Router1(config-pmap-c)# random-detect dscp-based
Router1(config-pmap-c)# random-detect dscp 10 33 40 10
Router1(config-pmap-c)# random-detect dscp 22 24 40 10
Router1(config-pmap-c)# exit
Router1(config-pmap)# class class-default
Router1(config-pmap-c)# bandwidth percent 5
Router1(config-pmap-c)# end
Router1# conf t
Router1(config)# int s1/0
Router1(config-int)# service-policy output WRED
Router1(config-int)# end

```

#### 4. REZULTATI SIMULACIJE

Tabelarni prikaz osnovnih podešavanja krajnjih tačaka i definisanih parametara za konkretne parove kojima je „zatrpan“ link između dva rutera dat je na slici 3. Prva tri para su definisana kao *VoIP* saobraćaj bez prioriteta, peti par-konekcija je video saobraćaj bez prioriteta, dok je četvrta konekcija *VoIP* saobraćaj sa prioriteto, što se može videti i definisanim servisnim kvalitetom u petoj koloni tabele.

Group/ Pair	Endpoint 1	Endpoint 2	Network Protocol	Service Quality	Script/Stream Name
All Pairs					
Pair 1	10.10.10.10	20.20.20.20	RTP	DHCP-AF11	G.711u
Pair 2	10.10.10.10	20.20.20.20	RTP	DHCP-AF11	G.711u
Pair 3	10.10.10.10	20.20.20.20	RTP	DHCP-AF11	G.711u
Pair 4	10.10.10.10	20.20.20.20	RTP	DHCP-EF	G.711u
Pair 5	10.10.10.10	20.20.20.20	RTP	DSCP AF23	MPEG3 codec

Slika 3. Tabelarni prikaz parametara

Uporednim prikazom tabela na slici 4. i 5. možemo zaključiti da je ista količina podataka izražena u bajtovima prosledena od konzolnog računara do računara koji simulira krajnju tačku, ali da se količina izgubljenih bajtova menja sa aktivacijom *WRED* mehanizma (slika 5).

Group/ Pair	Bytes Sent by E1	Bytes Received E2 (Streaming)	Bytes Lost from E1 to E2	Percent Bytes Lost E1 to E2
All Pairs	37.762.400	33.765.416	3.996.984	10,585
Pair 1	2.400.000	2.572.800	27.200	1,133
Pair 2	2.400.000	2.159.520	240.480	10,020
Pair 3	2.400.000	2.160.000	240.000	10,000
Pair 4	2.400.000	1.771.680	628.320	26,180
Pair 5	28.162.400	25.301.416	2.860.984	10,159
Totals:	37.762.400	33.765.416	3.996.984	10,585

Slika 4. Količina izgubljenih bajtova bez aktiviranog *WRED* mehanizma

Group/ Pair	Bytes Sent by E1	Bytes Received E2 (Streaming)	Bytes Lost from E1 to E2	Percent Bytes Lost E1 to E2
All Pairs	37.762.400	33.621.572	4.140.728	10,965
Pair 1	2.400.000	2.113.920	286.080	11,920
Pair 2	2.400.000	2.200.960	199.040	8,283
Pair 3	2.400.000	2.110.720	289.280	12,055
Pair 4	2.400.000	2.400.000	0	0,000
Pair 5	28.162.400	24.796.072	3.366.328	11,953
Totals:	37.762.400	33.621.572	4.140.728	10,965

Slika 5. Količina izgubljenih bajtova sa aktiviranim *WRED* mehanizmom

U slučaju kada nije aktiviran mehanizam, najmanji procenat izgubljenih podataka ima prva konekcija (1,133%), dok u drugom slučaju sa aktiviranim mehanizmom vrednost gubitaka značajno raste (11,92%) za prvu konekciju, ali opada za konekciju sa prioriteto i to sa 26,18% na nulu. Može se zaključiti da je samo došlo do preraspodele gubitaka, jer je prosečan procenat izgubljenih bajtova za sve konekcije ostala približno jednaka 10,585% bez, odnosno 10,965% sa aktivnim mehanizmom.

Group/ Pair	One-Way Delay Average (ms)	One-Way Delay Minimum (ms)	One-Way Delay Maximum (ms)
All Pairs	116	96	139
Pair 1	124	96	132
Pair 2	116	100	135
Pair 3	116	100	134
Pair 4	116	101	133
Pair 5	120	104	139
Totals:	116	96	139

Slika 6. Vrednost jednosmernog kašnjenja bez aktivacije mehanizma

Kada posmatramo vrednosti jednosmernog kašnjenja sa i bez aktiviranog *WRED* mehanizma (slika 6. i 7.) možemo primetiti da u slučaju sa aktivnim mehanizmom vrednosti kašnjenja za sve konekcije, osim četvrte, rastu za oko 39%. U prvom slučaju vrednost kašnjenja konekcije koja ima prioritet je bila 116 ms (133 ms max – 101 ms min), a nakon aktiviranja mehanizma ona iznosi 19 ms (26 ms max – 4 ms min).

Group/ Pair	One-Way Delay Average (ms)	One-Way Delay Minimum (ms)	One-Way Delay Maximum (ms)
All Pairs	162	4	219
Pair 1	157	156	219
Pair 2	156	152	216
Pair 3	157	163	219
Pair 4	19	4	76
Pair 5	207	80	218
Totals:	162	4	219

Slika 7. Vrednost jednosmernog kašnjenja sa aktiviranim *WRED* mehanizmom

Vrednosti propusne moći iskazane u Mb/s su prikazane na slici 8. u slučaju da mehanizam nije aktiviran, odnosno na slici 9. kada je WRED aktivan. Vrednosti u oba tabelarna prikaza su relativno jednake, ali pažnju zahteva četvrti par kod kog se ne javljaju oscilacije u propusnoj moći (minimum i maksimum su jednaki) aktiviranjem WRED mehanizma, a sve to očigledno na uštrb ostalih konekcija koje prenose VoIP saobraćaj. Naime, WRED mehanizmom je definisan minimalni propusni opseg od 8% za ovu konekciju od ukupno raspoloživog saobraćaja što je i ostvareno.

Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)
All Pairs	0,899	0,041	0,700
Pair 1	0,063	0,055	0,065
Pair 2	0,058	0,051	0,062
Pair 3	0,058	0,053	0,063
Pair 4	0,047	0,041	0,054
Pair 5	0,674	0,655	0,700
Totals:	0,899	0,041	0,700

Slika 8. Vrednosti propusnog opsega bez aktiviranog WRED mehanizma

Group/ Pair	Average (Mbps)	Minimum (Mbps)	Maximum (Mbps)
All Pairs	0,895	0,050	0,940
Pair 1	0,056	0,050	0,062
Pair 2	0,059	0,056	0,062
Pair 3	0,056	0,052	0,062
Pair 4	0,064	0,064	0,064
Pair 5	0,660	0,638	0,940
Totals:	0,895	0,050	0,940

Slika 9. Vrednosti propusnog opsega sa aktiviranim WRED mehanizmom

MOS – Mean Opinion Score vrednost predstavlja subjektivnu ocenu lica, učesnika u razgovoru, o kvalitetu servisa VoIP konekcije. Na slici 10. možemo videti da je konkretni parametar za sve konekcije oko 1 (što predstavlja izuzetno loš rezultat), izuzev prvog para gde u proseku iznosi oko 3,38. Ovi rezultati su dobijeni bez primene WRED mehanizma, koji se koristi za izbegavanje zagušenja i koji za krajnji rezultat ima obezbeđivanje prioriteta za pojedine konekcije (četvrti par - konekcija) garantujući im minimalni propusni opseg. Minimalni propusni opseg za VoIP konekciju putem Ethernet interfejsa prema Cisco-vom standardu iznosi 87,2 kb/s. Međutim, nije samo minimalni opseg definisan Cisco-vim standardom, već i sama vrednost MOS parametra, koji uz primenu kodeka G.711u mora iznositi 4,1 i više. Aktiviranjem WRED mehanizma, vrednost MOS parametra prelazi 4,1 (4,36 u proseku) za konekciju sa prioriteto, dok je za ostale ta vrednost oko 1,09.

Group/ Pair	MOS Average	MOS Minimum	MOS Maximum
All Pairs	1,63	1,00	4,32
Pair 1	3,38	1,00	4,32
Pair 2	1,04	1,00	2,23
Pair 3	1,08	1,00	2,08
Pair 4	1,00	1,00	1,00
Pair 5	n/a	n/a	n/a
Totals:	1,63	1,00	4,32

Slika 10. Vrednosti MOS parametra bez WRED mehanizma

Group/ Pair	MOS Average	MOS Minimum	MOS Maximum
All Pairs	1,90	1,00	4,37
Pair 1	1,07	1,00	3,93
Pair 2	1,09	1,00	3,47
Pair 3	1,09	1,00	4,10
Pair 4	4,36	4,36	4,37
Pair 5	n/a	n/a	n/a
Totals:	1,90	1,00	4,37

Slika 11. Vrednosti MOS parametra sa aktiviranim WRED mehanizmom

Što se tiče video konferencije, pored prethodno analiziranih parametara u scenarijima sa i bez aktiviranim WRED mehanizma, možemo posmatrati i vrednosti izgubljenih frejmova. Slika 12 nosi informaciju o količini izgubljenih frejmova videa u jedinici vremena. Može se primetiti da, u slučaju kada nije aktiviran mehanizam, prosek izgubljenih frejmova iznosi oko 50 med.frame/s (60 med.frame/s max – 18 med.frame/s min).

Group/ Pair	Maximum MDI Maximum DF : Maximum MLR	Average MLR (media frames/s)	Minimum MLR (media frames/s)	Maximum MLR (media frames/s)
All Pairs	171 : 60,006	50,508	18,828	60,005
Pair 1	n/a	n/a	n/a	n/a
Pair 2	n/a	n/a	n/a	n/a
Pair 3	n/a	n/a	n/a	n/a
Pair 4	n/a	n/a	n/a	n/a
Pair 5	171 : 60,006	50,508	18,828	60,005
Totals:	171 : 60,006	50,508	18,828	60,005

Slika 12. Izgubljeni frejmovi pete konekcije bez primenjenog WRED mehanizma

Group/ Pair	Maximum MDI Maximum DF : Maximum MLR	Average MLR (media frames/s)	Minimum MLR (media frames/s)	Maximum MLR (media frames/s)
All Pairs	366 : 375,000	63,006	12,299	375,000
Pair 1	n/a	n/a	n/a	n/a
Pair 2	n/a	n/a	n/a	n/a
Pair 3	n/a	n/a	n/a	n/a
Pair 4	n/a	n/a	n/a	n/a
Pair 5	366 : 375,000	63,006	12,299	375,000
Totals:	366 : 375,000	63,006	12,299	375,000

Slika 13. Izgubljeni frejmovi pete konekcije sa primenjenim WRED mehanizmom

Slika 13. prikazuje vrednosti izgubljenih frejmova video konekcije u jedinici vremena kada aktiviramo WRED mehanizam kako bismo očuvali konekciju VoIP sa prioriteto. Prosečna vrednost izgubljenih frejmova iznosi 63 med.frame/s (375 med.frame/s max – 12,3 med.frame/s min). Blagi porast u prosečnoj vrednosti izgubljenih frejmova jeste posledica primenjenog WRED mehanizma, odnosno činjenice da je četvrti konekcija sa prioriteto i kao takva mora se očuvati sa što manjim gubicima, a to direktno utiče na preostale četiri konekcije na testu.

## 5. ZAKLJUČAK

*TCP* protokol deli celokupni tok podataka u veći broj odvojenih tokova unutar kojih se mogu naći podaci više različitih izvora. Kontrola toka omogućena je ovom protokolu upotrebom mehanizma takozvanog klizajućeg prozora uz primenu različitih tajmera. Ukoliko podaci ne stignu na destinaciju ili stignu oštećeni, neophodno je izvršiti retransmisiju tih podataka, a na koju direktno utiču razne politike *TCP* protokola.

Problem koji se javlja kod *TCP* protokola jeste nemogućnost detekcije odnosno kontrole zagušenja, a koja utiče i na kontrolu toka. Jedan od načina za izbegavanje zagušenja na mreži jeste primena *Jacobson*-ovog mehanizma za ranu detekciju greške – *RED (Random Early Detection)* mehanizam. Ovaj mehanizam, kao i sve njegove varijacije, zasniva se na tome da kada vrednosti bafera premaše neke definisane granice (*threshold*), a da pri tome nije u potpunosti ispunjen, mehanizam signalizira predajnom entitetu da smanji brzinu prenosa i da će otpočeti sa nasumičnim odbacivanjem paketa prema nekom pravilu o odabiru izvora. Takodje, neka vrsta izbegavanja zagušenja na mreži se primenjuje manipulacijom softverski definisanih redova čekanja, ali i oblikovanjem saobraćaja na mreži primenom opcija *policing* i *shaping*.

Teorijske pretpostavke su potvrđene u praktičnoj implementaciji koja je prikazana u radu, odnosno parametri kvaliteta servisa su se menjali u slučaju aktivnog *WRED* mehanizma i u odnosu na scenario kad nije bio aktivan. Procenat izgubljenih paketa je u proseku isti u oba scenarija za sve konekcije osim za konekciju sa prioritetom, gde u slučaju aktivnog mehanizma ta vrednost je jednaka nuli. Vrednosti kašnjenja u jednom smeru za sve konekcije su porasle za 39% osim za četvrtu konekciju gde je ta vrednost opala drastično čime je obezbeđena brža dostava paketa. Propusna moć u periodu merenja je oscilirala od minimalnih do maksimalnih vrednosti za sve konekcije, a nakon aktiviranog *WRED* mehanizma ponašanje konekcija ostaje isto sem četvrtog para gde ta vrednost ostaje konstantna u periodu merenja. Uzimajući u obzir vrste konekcija, izdvojili smo karakteristične parametre koje smo posmatrali u ova dva scenarija.

Prvi je parametar *MOS* za *VoIP* konekcije koji je u prvom scenariju u rangju 1,0-3,8, a u scenariju sa aktivnim mehanizmom *WRED* *MOS* parametar za prioritetnu konekciju iznosi 4,36, odnosno 1,7-1,9 za preostale *VoIP* konekcije.

Za video par, analiziran je parametar koji je koji predstavlja količinu izgubljenih video frejmova u jedinici vremena. Analogno ponašanju konekcija koje nisu sa prioritetom, par koji prenosi video-stream se ponaša isto – u scenariju sa aktivnim mehanizmom vrednost izgubljenih frejmova je porasla. Ovo doprinosi činjenici da je *WRED* mehanizam zaista izvršio svoju funkciju i zaštitio konekciju koju smo odredili prioritetnom, a na uštrb ostalih konekcija koje su se uspostavljale zajedničkim linkom, odnosno zagušenje je izbegnuto jer su najpre realizovane prioritetne komunikacije, a nakon njih preostale.

## ZAHVALNICA

Ovaj rad je nastao kao deo istraživanja u okviru projekta br. VA-TT/1-17-19 finansiran od strane Ministarstva odbrane Republike Srbije.

## LITERATURA

- [1] W. Stallings, „Integrated and Differentiated Services“, in Book *High-Speed Networks and Internets: Performance and Quality of Service*, ch. 17, pp. 469-506, New Jersey, USA: Prentice Hall, 2002.
- [2] *Recommendations on Queue Management and Congestion Avoidance in the Internet*, RFC 2309 (International), IETF, 1998.
- [3] Blake, S., Black, D., Davies, E., Wang, Z., and Weiss, W., *An Architecture for Differentiated Services*, RFC 2475 (International), IETF, 1998.
- [4] Davie, B., et al. *An Expedited Forwarding PHB (Per-Hop Behavior)*, RFC 3246, Internet Engineering Task Force, March 2002.
- [5] *Cisco IOS Quality of Service Solutions Configuration Guide, release 12.2 SR*



# PRISTUP SPECIFIKACIJI ZAHTEVA ZA RAZVOJ SISTEMA “FAKTURISANA REALIZACIJA U ZDRAVSTVENOJ ZAŠTITI” APPROACH TO SPECIFICATION REQUIREMENTS FOR DEVELOPMENT OF “FACTURED REALIZATION IN HEALTH CARE ”

Rajko Terzić<sup>1</sup>, Milosav Majstorović<sup>2</sup>

Gradski zavod za javno zdravlje<sup>1</sup>

Visoka škola strukovnih studija za informacione tehnologije, Beograd<sup>2</sup>

**Sadržaj** – Neprecizna i neformalna specifikacija zahteva dovodi do teškoća u kasnijim fazama razvoja softverskih sistema. Štaviše, ovakva specifikacija zahteva može dovesti do potpunog neuspeha projekta. Jedna od najtežih, i kritičnih aktivnosti u procesu specifikacije zahteva je identifikacija funkcionalnih zahteva. Popularan pristup za identifikaciju i opis funkcionalnih zahteva je korišćenje UML modela slučajeva korišćenja. U ovom radu je izložen pristup koji omogućuje korišćenje rezultata modelovanja poslovnih procesa, koje se sprovodi u fazi analize sistema, u kasnijoj konstrukciji modela slučajeva korišćenja. Ovaj pristup omogućuje da zahtevi koje treba da ispuni softverski sistem budu poravnati sa poslovnim potrebama, kako sa aspekta poslovnih procesa, tako i sa aspekta informacionih entiteta kojima se ovi procesi bave. Pristup je primenjen u razvoju sistema „Fakturisana realizacija u zdravstvenoj zaštiti“ u Gradskom zavodu za javno zdravlje u Beogradu. Radi ilustracije pristupa, u radu su prikazani elementi modela softverskih zahteva koji su kreirani u taku razvoja ovog sistema.

**Abstract** - Improper and informal specification of the requirements leads to difficulties in later phases of software development. Moreover, such requirements specification may lead to complete failure of the project. One of the most difficult and critical activities in the specification process requires identification of functional requirements. The most popular approach for identifying and describing functional requirements is the use of UML use cases models. This paper presents an approach that allows the use of business process modelling results, which is implemented in the system analysis phase, in the later design of the of use cases model. This approach allows alignment the software requirements and business needs, both from the aspect of business processes and from the aspect of the information entities involved in these processes. Approach has been implemented in the development of the "Factured Realization in Health Care" system at the Belgrade Institute for Public Health. To illustrate the approach, the paper presents the modalities of the software requirements created in the development of this system.

## 1. UVOD

Globalizacija tržišta i kontinuirano povećanje konkurentnosti između kompanija zahteva konstantne promene u organizacijama, sa ciljem prilagođavanja novim okolnostima, kao i implementaciju novih strategija poslovanja. Dakle, savremeno poslovanje karakterišu krupne i česte promene, koje iziskuju promenu i

poslovnih procesa (PP) kojima se poslovanje realizuje. Ovim, fleksibilnost i efikasno upravljanje poslovnim procesima (UPP) postaje od esencijalne važnosti za organizacije [1]. Da bi se upravljalo poslovnim procesima neophodno ih je precizno modelovati. Između postojećih jezika za modelovanje PP u ovom radu se koristi BPMN (*Business Process Model and Notation*) jezik [2], koji je postao svetski standard za modelovanje poslovnih procesa i koji je prihvaćen od strane korisnika širom sveta i podržan od strane velikih proizvođača softvera.

Tako, sa jedne strane, modelovanje PP i UPP sve više dobija na važnosti, a sa druge strane, timovi za razvoj softvera, još uvek imaju ozbiljne poteškoće pri definisanju softverskih (aplikacionih) zahteva [3]. Softverski sistemi se implementiraju kako bi se zadovoljile potrebe korisnika. Loša analiza i specifikacija zahteva je još uvek glavni razlog neuspeha velikog broja IT projekata. Put za rešenje ovog problema je specifikacija sistema u skladu s poslovnim procesima koje treba da podrži, i u kontekstu njegove upotrebe. Imajući na umu ova dva važna aspekta specifikacije zahteva, pristup izložen u ovom radu polazi od modelovanja PP i specifikaciji konteksta upotrebe softverskog sistema pomoću modela slučajeva korišćenja, koji se tradicionalno koristi za ovu namenu [4].

U [5] je prepoznat problem modelovanja PP u početku specifikacije zahteva i dat metod za generisanje slučajeva korišćenja iz modela PP. Međutim, rad se ne bavi problemom kreiranja i ostalih modela, potrebnih kako u fazi specifikacije zahteva, tako i kasnijim fazama razvoja sistema. U [4] je dat model softverskih zahteva za velike sistema, ali taj model ne uključuje eksplicitno modele PP. Objektivno orijentisane metodologije, kao što je npr. [6] koriste UML jezik i modele za specifikaciju sistema, ali naglasak nije na korišćenju modela PP u samom početku specifikacije zahteva, i direktnom izvođenju modela slučajeva korišćenja iz njega.

U ovom radu se zagovara pristup specifikaciji zahteva zasnovan na modelu softverskih zahteva, za koji je dat i proces izrade specifikacije zahteva u [7]. Pristup omogućuje korišćenje rezultata modelovanja PP, koje se sprovodi u početku faze analize sistema (korišćenjem BPMN jezika), u kasnijoj konstrukciji modela slučajeva korišćenja. Pri ovome, kreiranje modela slučajeva korišćenja se zasniva na modelu PP, u skladu sa [5]. U radu je naglašena primena poslovnih pravila i njihova komplementarnost sa modelima PP, koja u principu dovodi do manje kompleksnih BPMN dijagrama. Pristup je verifikovan kroz razvoj jednog netrivialnog softverskog sistema. U radu su prikazani elementi modela

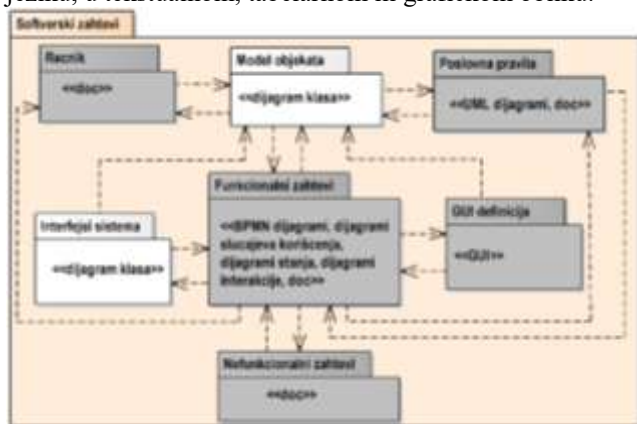
softverskih zahteva (tretirani su samo funkcionalni zahtevi) koji su kreirani u taku razvoja ovog sistema.

U sledećem poglavlju je ukratko opisan model softverskih zahteva na kojem se zasniva pristup korišćen u radu. Treće poglavlje se bavi problemom identifikacije funkcionalnih zahteva i poslovnih pravila. U četvrtom poglavlju se prikazuje modelovanje PP. Metodološki postupak kreiranja modala PP ilustrovan je na primeru PP koji uključuje više institucija zdravstvenog sistema Republike Srbije. U petom poglavlju je pokazano kako se može koristiti model PP u razvoju modela slučajeva korišćenja. Šesto poglavlje se bavi kreiranjem modela poslovnih objekata (konceptualnog modela). Pri ovome, naglašena je uloga analize logičkih odnosa među podacima ulazne strukture u kreiranju konceptualnog dijagrama klasa. U zaključku su navedeni osnovni rezultati i doprinosi rada, kao i teškoće koje su autori imali u primeni pristupa. Na kraju su izneti planovi za dalji rad.

## 2. MODEL SOFTVERSKIH ZAHTEVA

U [7] je dat model softverskih zahteva (zahtevi koje treba da ispuni softverski sistem) koji predstavlja strukturu zahteva kroz međusobno povezane komponente (slika 1.). Globalni model softverskih zahteva (predstavljen najvećim paketom) sadrži druge artefakte koji su modelovani kao manji paketi. Komponente modela softverskih zahteva su na slici predstavljene kao graf manjih paketa povezanih vezama zavisnosti. Centralni deo modela zahteva je model funkcionalnih zahteva koji opisuje željeno ponašanje sistema. On opisuje jasno i detaljno svaki servis koji programski sistem treba da obezbedi.

Na slici 1. komponente čiji modeli se mogu izraziti sa UML su predstavljeni svetlo (moguće ih je predstaviti relativno formalno). Sive komponente se mogu samo delimično predstaviti korišćenjem UML-a. Za njihov opis mogu se koristiti dokumenti zasnovani na prirodnom jeziku, u tekstualnom, tabelarnom ili grafičkom obliku.



Slika 1. Model softverskih zahteva – glavne komponente

Centralni deo modela zahteva je model funkcionalnih zahteva koji opisuje željeno ponašanje sistema. On opisuje jasno i detaljno svaki servis koji programski sistem treba da obezbedi. Osnovni dijagrami kojima se u

ovoj komponenti opisuje ponašanje su BPMN dijagrami (kojima se definiše model poslovnih procesa koji programski sistem treba da podrži) i dijagram slučajeva korišćenja (kojima se daje prikaz funkcija sistema, tj. slučajeva korišćenja sistema, kao i aktera/učesnika koji te funkcionalnosti koriste).

## 3. IDENTIFIKACIJA FUNKCIONALNIH ZAHTEVA I POSLOVNIH PRAVILA

Prva aktivnost u procesu izrade specifikacije zahteva, u pristupu koji se zagovara u ovom radu, je inicijalna analiza poslovnog sistema, odnosno njegovog dela koji je predmet konkretne specifikacije. Ova aktivnost (faza) je kritični deo procesa jer treba razumeti dotičan poslovni problem, tj. poslovni proces, koji je najčešće na početku slabo definisan (npr. ne postoje precizno definisane poslovne procedure za njegovo obavljanje), a korisnik ga teško može precizno izraziti. Pored posmatranja odvijanja PP, intervju sa izvršiocima odgovornim za njegovu realizaciju, neophodno je proučiti i relevantna dokumenta koja se bave dotičnim PP.

Pri analizi PP „Analiza izvršenja rada zdravstvene ustanove (ZU) i formiranje plana rada za iduću godinu“, korišćeni su dokumenti [8] i [9]. Ovaj poslovni proces je deo sistema za obradu fakturne realizacije zdravstvene zaštite u kojem učestvuju Republički fond za zdravstveno osiguranje (RFZO), Institut za javno zdravlje Srbije „Dr Milan Jovanović Batut“ (IZJZS), Gradski zavod za javno zdravlje (GZJZ) i zdravstvene ustanove (ZU). Rezultati ove aktivnosti mogu biti funkcionalni zahtevi i poslovna pravila izražena kroz strukturirani tekst na prirodnom jeziku. Inicijalni funkcionalni zahtevi i poslovna pravila za spomenuti PP dati su u tabelama 1 i 2, respektivno. U ovoj fazi, funkcionalni zahtevi i poslovna pravila se daju okvirno i uopšteno (ali svakako trebaju biti verifikovana od naručioca), a u sledećim fazama se oni mogu detaljisati i formalno prikazivati.

U procesu pribavljanja funkcionalnih zahteva od svih relevantnih učesnika moguće je da se pojave različite, u nekom stepenu konfliktne ideje, koje treba razrešiti. Mogući način razrešenja konfliktnih i konkurentnih zahteva je dodela prioriteta zahtevima. Ovaj način zahteva od korisnika da definiše koje zahtevane funkcionalnosti su najvažnije. Manje strog pristup prioritetima može podeliti zahteve u tri kategorije [7]:

1. Zahtevi obavezno moraju biti ispunjeni (**E**sencijalni)
2. Zahtevi su veoma poželjni, ali nisu obavezni (**P**oželjni)
3. Zahtevi su mogući, ali nisu obavezni (**O**pcionalni)

Oznaka funkcionalnog zahteva se formira po šablonu: FR – funkcionalni zahtev (Engl. **F**unctional **R**equirement), oznaka procesa (u primeru ARFP – **A**naliza **R**ada i **F**ormiranje **P**lana), redni broj zahteva. Kada je reč o poslovnim pravilima, njihova oznaka počinje sa R – pravilo (Engl. **R**ule)

Oznaka funk. zahteva	Opis zahteva	Prioritet
FR_ARFP_1	Prijem podataka od IZJZS i njihova analiza	E
FR_ARFP_2	Slanje poruke prema IZJZS o lošem formatu ulaznih podataka	O
FR_ARFP_3	Konsolidacija ulaznih fajlova	E
FR_ARFP_4	Import podataka u SQL bazu	E
FR_ARFP_5	Obrada podataka i generisanje tabela o izvršenju rada	E
FR_ARFP_6	Po potrebi, korekcija ulaznih podataka i slanje na novu obradu	O
FR_ARFP_7	Prosleđivanje izveštajnih podataka (izveštajnih tabela) ZU	E
FR_ARFP_8	Prijem planova rada od ZU	P
FR_ARFP_9	Formiranje mišljenja o planovima rada ZU i prosleđivanje mišljenja prema	P

Tabela 1. Primer funkcionalnih zahteva za PP „Analiza izvršenja rada zdravstvene ustanove (ZU) i formiranje plana rada za iduću godinu“

Oznaka pravila	Opis pravila
R_ARFP_1	Ako podaci za obradu nisu u zadovoljavajućem formatu, slanje poruke o lošem formatu
R_ARFP_2	Ako faktorni izveštaj stiže u nekoliko fajlova mora se uraditi sabiranje po svakoj usluzi, za svaku zdr. ustanovu pojedinačno kao i druge operacije aktivnosti koje nazivamo konsolidacija podataka
R_ARFP_3	Ako obrada podataka nije zadovoljavajuća, potrebno je uraditi korekcije nad ulaznim podacima i sprovesti novu obradu
R_ARFP_4	Ako je obrada zadovoljavajuća, distribuirati izveštajne tabele ZU kako bi one napravile svoje planove rada
R_ARFP_5	Ako su planovi rada stigli iz ustanova početi aktivnosti izrade mišljenja na planove rada

Tabela 2. Primer poslovnih pravila za za PP „Analiza izvršenja rada zdravstvene ustanove (ZU) i formiranje plana rada za iduću godinu“

#### 4. MODELOVANJE POSLOVNIH PROCESA

Specifikacija softverskih zahteva i modela često nije u saglasnosti sa poslovnim procesima koje sistem treba da podrži, odnosno pomoću kojeg poslovni procesi treba da se realizuju. Zato, zasnivanje pribavljanja i analize korisničkih zahteva na modelima poslovnih procesa, može osigurati poravnanje poslovnih procesa i softverskih modela. Zbog toga, modelovanje poslovnih procesa prirodno spada u početne faze razvoja softvera kao što su analiza sistema i specifikacija zahteva [7].

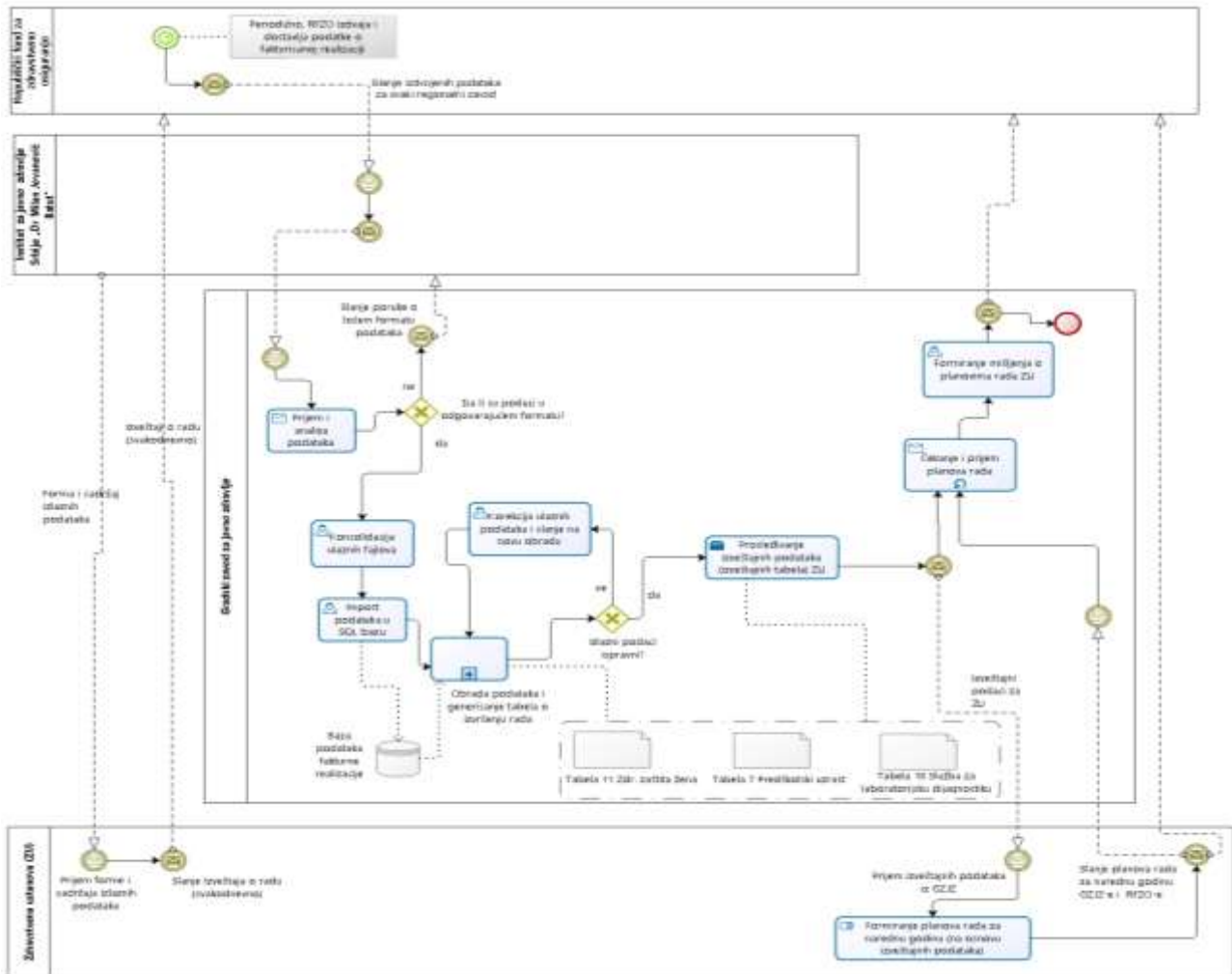
Pri kreiranju modela PP koriste se rezultati inicijalne analize sistema, čiji su fragmenti prikazani u prethodnoj sekciji. Svaki funkcionalni zahtev može predstavljati aktivnost ili podproces na BPMN dijagramu. Poslovna pravila igraju sve važniju ulogu u agilnim poslovnim scenarijima, utičući na to kako se poslovnim objektima upravlja u PP i kako učesnici u njemu ostvaruju interakciju [10]. U našem pristupu, poslovna pravila su iskazana deklarativno (tabela 2), i na BPMN modelu (koji ima proceduralni karakter) se procesiraju u kapijama (raskrscicama). Na ovaj način, zadržava se jednostavnost BPMN dijagrama, eliminisanjem određenih puteva u modelu procesa i upravljanjem različitim situacijama pomoću pravila. Na slici 2. je prikazan model PP „Analiza izvršenja rada zdravstvene ustanove (ZU) i formiranje plana rada za iduću godinu“ pomoću BPMN dijagrama. Aktivnosti ovih učesnika su prikazane u tri bazena (koji odgovaraju dotičnim učesnicima). Kolaoboracija učesnika je ilustrovana kroz razmenu

poruka. Na primer, IZJZS propisuje formu i sadržaj podataka koje ZU svakodnevno pripremaju i dostavljaju RFZO.

Softverski sistem, čiji zahtevi su predmet ovog rada, treba da podrži poslovne procese u GZJZ, pa su u ovom bazenu i prikazane aktivnosti dijagrama orkestracije PP „Analiza izvršenja rada zdravstvene ustanove (ZU) i formiranje plana rada za iduću godinu“. U nastavku se okvirno opisuje ovaj PP koji u GZJZ počinje prijemom izdvojenih podataka ZU čije podatke GZJZ evidentira i obrađuje (podatke u polustrukturiranom formatu dostavlja IZJZS). GZJZ vrši analizu primljenih podataka. U slučaju da primljeni podaci nisu u formatu pogodnom za import u bazu podataka GZJZ, šalje se obaveštenje IZJZS o neusklađenosti. Ako su podaci u dogovorenom formatu pristupa se konsolidaciji ulaznih fajlova. U slučaju da je format podataka neodgovarajući GZJZ kroz odgovarajuću poruku o tome obaveštava IZJZS. Posle konsolidacije ulaznih fajlova podaci se importuju u SQL bazu podataka (baza podataka fakturane realizacije).

Podaci u bazi podataka se obrađuju i pri tome se generišu tabele o izvršenim uslugama ZU (primeri naziva takvih tabela su prikazani su na slici 2.). Ako su izlazni podaci ispravni oni se prosleđuju ZU koje na osnovu njih formiraju planove rada za narednu godinu. U slučaju da to nije slučaj, ulazni podaci se koriguju i šalju na novu obradu. ZU planove rada dostavljaju GZJZ i RFZO. GZJZ po prijemu planova rada vrši njihovu analizu i formira

mišljenje o njima, koje dostavlja RFZO. Ovim se jedna instanca ovog PP u GZJZ završava.



Slika 2. BPMN dijagram PP „Analiza izvršenja rada ZU i formiranje plana rada za iduću godinu“

## 5. DIJAGRAM SLUČAJEVA KORIŠĆENJA

Modeli slučajeva korišćenja se tradicionalno koriste za opisivanje ponašanja sistema sa gledišta korisnika, i to u početnoj fazi specifikacije softverskog sistema [6]. Ranije je naglašeno da softver koji podržava poslovanje mora biti poravnat sa poslovnim procesima. Zato je prirodno nastojanje približavanja modelovanja PP i modelovanja softvera. Viša autora je predložilo pristupe koji se zasnivaju na izvođenju slučajeva korišćenja iz modela PP. Analiza ovih pristupa je van opsega ovog rada. U našem pristupu se koristi rešenje predloženo u [5]. U skladu s ovim, u pojednostavljenoj formi, učesnici sa BPMN dijagrama (predstavljeni bazenima i stazama) postaju akteri, a aktivnosti slučajevi korišćenja, na dijagramu slučajeva korišćenja. Akter koji predstavlja bazen (ili stazu) je povezan sa svim slučajevima korišćenja koji odgovaraju aktivnostima koje pripadaju dotičnom bazenu

(ili stazi). Akter koji predstavlja učesnika koji šalje (ili prima) poruku u aktivnost, je povezan sa slučajem korišćenja koji reprezentuje tu aktivnost. Korišćenjem ovog pristupa dobijen je dijagram slučajeva korišćenja na osnovu ranije prikazanog BPMN dijagrama (slika 3.). Radi jednostavnosti prikaza, svi slučajevi korišćenja povezani sa GZJZ kao akterom su grupisani i uokvireni pravougaonik, i tako kao celina povezani sa ovim akterom. Ovi slučajevi korišćenja upravo pripadaju softverskom sistemu za analizu izvršenja rada ZU i formiranje plana rada za iduću godinu.

U [5] je dat i šablon za generisanje opisa slučaja korišćenja iz modela PP. U tabeli 3 je dat primera opisa jednog slučaja korišćenja formiran na osnovu ovog šablona.

<b>Use Case name</b>	Konsolidacija ulaznih fajlova.
<b>Actors</b>	Gradski zavod za javno zdravlje
<b>Pre-condition</b>	Podaci su u formatu pogodnim za import u bazu podataka.
<b>Scenario</b>	Izvršava se skup aktivnosti nad agregiranim podacima u cilju usklađivanja za import u bazu podataka.

Tabela 3. Konsolidacija ulaznih fajlova - opis slučaja korišćenja



Slika 3. Dijagram slučajeva korišćenja „Analiza izvršenja rada ZU i formiranje plana rada za iduću godinu“

## 6. KREIRANJE MODELA POSLOVNIH OBJEKATA (KONCEPTUALNOG MODELA)

U procesu prikupljanja zahteva i njihove analize identifikuju se i osnovni poslovni objekti (kao i veze između njih) koji učestvuju u određenom poslovnom procesu. Struktura ovih objekata, u fazi analize zahteva se tradicionalno naziva model domena, odnosno konceptualni model i uobičajeno predstavlja pomoću UML dijagrama klasa [6]. U istraživačkim i industrijskim krugovima ne postoji saglasnost oko redosleda kreiranja modela slučajeva korišćenja i konceptualnog modela [11]. U radu su korišćeni poslovni dokumenti ([12], [13]), opisi slučajeva korišćenja, kao i analiza ulaznih podataka (fragment ovih podataka prikazan je na slici 4.) u procesu kreiranja konceptualnog modela (slika 5.).

Ulazni podaci u sistem stužu kao excel fajlovi i predstavljaju određene relacije podataka poslovnog sistema. Fragment takve relacije prikazan je na slici 5., i očigledna je velika redundansa podataka u njoj. Na osnovu iskustva autora, kao i uhodanog načina rada i razmene podataka između učesnika ovog PP, došlo se do zaključka da kolone: filijala, naziv ustanove, naziv službe,

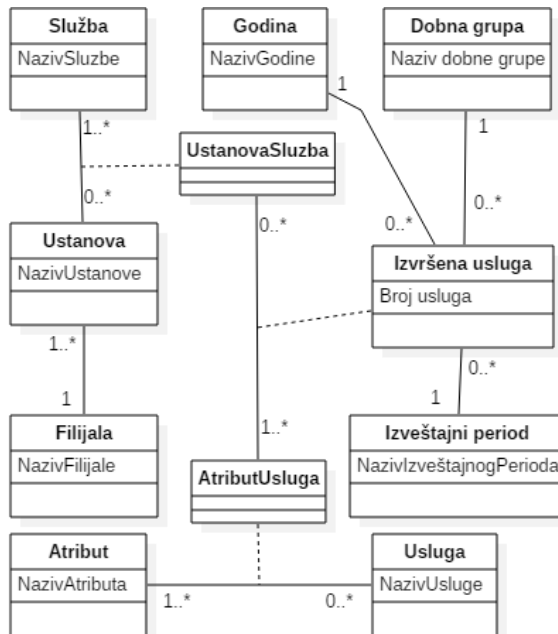
naziv usluge, šifra usluge, atribut i dobne grupe predstavljaju klase domena, dok ostale kolone predstavljaju podatke koje su nastali transakcionim obradama (npr. broj izvršenih usluga). Analizom logičkih veza (veza zavisnosti) koje postoje između atributa relacije došlo se do sledeće semantike sistema: Jedna filijala ima više ZU, dok ZU pripada samo jednoj filijali. ZU ima više službi, i obrnuto služba se može nalaziti u više ZU. Usluga ima više atributa po kojima se evidentira njeno izvršenje i atribut može karakterisati više usluga. Služba određene ustanove pruža više usluga u kontekstu nekog atributa i usluga u kontekstu nekog atributa može biti pružena u više službi ustanova. Broj izvršenih usluga u kontekstu određenog atributa se evidentira sumarno po dobnim grupama. Osim spomenutih, nije poznato postojanje drugih zavisnosti atributa ove relacije.

Na osnovu korišćenih izvora, spomenutih u ovoj sekciji, kao i izvedene semantike sistema, formiran je konceptualni model, prikazan na slici 5. Ovakav model bio je ishodište za kreiranje strukture SQL baze podataka, koja omogućuje evidentiranje svih ulaza i generisanje zahtevanih izlaza, bez anomalija ažuriranja i izveštavanja.



Filijala	Naziv ustanove	Sluzba	Usluga	Sifra	Atribut	od 7-14 godin	od 15-19 godin	od 20-34 godin
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Stomatologija	Amalgamski ispuni na 1 površini	2400190	Podrazumevana vrednost atributa	0	8	18
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Stomatologija	Amalgamski ispuni na 2 površine	2400216	Podrazumevana vrednost atributa	0	8	19
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Stomatologija	Amalgamski ispuni na 3 površine	2400232	Podrazumevana vrednost atributa	0	1	0
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Fizikalna medicina i rehabilitacija	Dijadnamske struje	1800143	Izbitna medicinska pomoc	0	0	0
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Fizikalna medicina i rehabilitacija	Elektroforeza	1800127	Podrazumevana vrednost atributa	40	84	314
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Fizikalna medicina i rehabilitacija	Elektromagnetna terapija	1800085	Izbitna medicinska pomoc	0	0	2
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Ginekologija i akušerstvo	Diagnostički test za ispitivanje oboljenja reproduktivnog sistema	1300094	Izbitna medicinska pomoc	0	0	0
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Ginekologija i akušerstvo	Diagnostički test za ispitivanje oboljenja reproduktivnog sistema	1300094	Podrazumevana vrednost atributa	0	0	546
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Ginekologija i akušerstvo	Elektrofiziološko snimanje u ginekologiji i akušerstvu	1300086	Podrazumevana vrednost atributa	0	0	34
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Laboratorijska dijagnostika	Aktivirano parcijalno trombotoplastinsko vreme (aPTT)	L014332	Podrazumevana vrednost atributa	13	15	350
Filijala Beograd	Dom zdravlja - Stari Grad Beograd	Laboratorijska dijagnostika	Alanin aminotransferaza (ALT) u serumu - spektrofotometrijski	L001057	Podrazumevana vrednost atributa	343	575	1773
Filijala Beograd	Dom zdravlja "Dr Milutin Mirović", Pal	Stomatologija	Amalgamski ispuni na 1 površini	2400190	Izbitna medicinska pomoc	1	1	0
Filijala Beograd	Dom zdravlja "Dr Milutin Mirović", Pal	Stomatologija	Amalgamski ispuni na 2 površine	2400216	Izbitna medicinska pomoc	1	3	0

Slika 4. Fragment izvora podataka



Slika 5. Konceptualni dijagram klasa sistema

## 7. ZAKLJUČAK

Analiza poslovnog sistema, razvoj i uvođenje softverskog sistema „Fakturisana realizacija u zdravstvenoj zaštiti“ vođeni su zahtevima koji su dobijeni korišćenjem pristupa izloženog u ovom radu. Softversko rešenje je realizovano u centru za analizu, planiranje i organizaciju zdravstvene zaštite GZJZ u Beogradu. Pri ovome, od ključne važnosti se pokazalo modelovanje PP u prvoj fazi razvoja sistema, što je kasnije omogućilo da zahtevi koje treba da ispuni softverski sistem budu poravnati sa poslovnim potrebama. Teškoće koje su se pokazale u primeni pristupa proistekle su pre svega zbog korišćenja različitih alata za modelovanje pri kreiranju različitih artifakta, pogotovo kod uspostavljanja veza između elemenata ovih artifakta nastalih u različitim alatima i fazama razvoja sistema.

U daljem radu se planira dogradnja pristupa izložen u ovom radu u skladu sa razvojem disciplina softverskog inženjerstva i primena u razvoju sopstvenih softverskih rešenja kao i nabavci gotovih rešenja na tržištu. Pri ovome, posebno se razmatra korišćenje softverskih alata za automatizaciju transformacije modela PP u model slučajeva korišćenja i automatsko izvođenje drugih UML modela u sledećim metodološkim fazama razvoja sistema.

## LITERATURA

- [1] Majstorović M., Regodić D., Majstorović G., Krstajić D., Cvetković R., "Sinergija arhitekture organizacije i upravljanja poslovnim procesima", YUINFO 2016, Društvo za informacione sisteme i računarske mreže, Beograd, pp. 58 - 63, Feb, 2016.
- [2] OMG 2011, "Business Process Model and Notation (BPMN)", Version 2.0, January 2011.
- [3] Jalote P., A concise Introduction to Software Engineering, Springer, 2008.
- [4] Johnson R., Roussos G., Tagliati L.V., Requirements analysis for large scale systems, *Journal of Object Technology*, November-December 2008. Vol. 7, No. 8, pp 119-137.
- [5] Estrela F. C., Ricardo J. M., Maribel Y. S., From Business Process Models to Use Case Models: A systematic approach, *Advances in Enterprise Engineering VIII*, Volume 174 of the series Lecture Notes in Business Information Processing, pp 167-181, 2014.
- [6] Jacobson I., Booch B., Jim Rumbaugh J., Unified Software Development Process, Addison-Wesley, 1999.
- [7] Majstorović M., Terzić R., "Pristup izradi specifikacije zahteva u procesu nabavke softverskog sistema", *INFOTEH '2017*, Arandelovac, 2017.
- [8] Živković Šulović M., Dukić D., Ljubičić M., Ločkić N., Pavlović B., Banković Lazarević D., Kilibarda B., "Uputstvo za izradu planova rada zdravstvenih ustanova primarne zdravstvene zaštite finansiranih sredstvima RFZO-a u 2017. godini", Beograd: Institut za javno zdravlje Srbije „Dr Milan Jovanović Batut“, 2017.
- [9] Pravilnik o bližim uslovima za obavljanje zdravstvene delatnosti u zdravstvenim ustanovama i drugim oblicima zdravstvene službe („Sl. glasnik RS” br. 43/06, 112/09, 50/10, 79/11, 10/12, 119/12 i 22/13)
- [10] Koehler J., The Process-Rule Continuum —How can the BPMN and SBVR Standards interplay? Lucerne University of Applied Sciences and Arts, Switzerland, 2011.
- [11] Shoval P., Yampolsky A., Last M., "Class Diagrams and Use Cases - Experimental Examination of the Preferred Order of Modeling", EMMSAD'06 Luxembourg 5-6 June, 2006.

[12] Pravilnik o Nomenklaturi zdravstvenih usluga na primarnom nivou zdravstvene zaštite. br. 17/13 i 32/15 - dopuna Pravilnika, 43/16). Pravilnik. Beograd: JP "Službeni glasnik".

[13] Pravilnik o Nomenklaturi laboratorijskih zdravstvenih usluga na primarnom, sekundarnom i tercijarnom nivou zdravstvene zaštite. br. 59/12, 24/17. Pravilnik. Beograd: JP "Službeni glasnik".

# INFORMACIONI SISTEM USTAVNOG SUDA SRBIJE

## INFORMATION SYSTEM OF THE CONSTITUTIONAL COURT OF SERBIA

Đuro Klipa<sup>1</sup> M.sc. , Radovan Bezbradica<sup>1</sup> , mr Rade Dragović<sup>2</sup>

<sup>1</sup> *Ustavni sud Srbije,*

<sup>2</sup> *Institut za standarde i tehnologije, Beograd*

**Sažetak:** Ustavni sud Srbije ustanovljen je Ustavom Socijalističke Republike Srbije od 9. aprila 1963. godine, kao samostalni organ Republike, koji obezbeđuje zaštitu ustavnosti i zakonitosti na osnovu Ustava u okviru svojih Ustavom utvrđenih prava i dužnosti. Složeni proces postupanja i odlučivanja po ustavnosudskim predmetima odvijao se u Ustavnom sudu, sve do 2011. godine, na tradicionalan način, u tzv. papirnoj formi, da bi avgusta te godine njegov rad bio modernizovan uvođenjem poslovanja u elektronskoj formi kroz Informacioni sistem Ustavnog suda (u daljem tekstu: ISUS). Glavni cilj uvođenja jednog takvog Document management system-a bila je podrška evidentiranju i obradi ustavnosudskih predmeta u elektronskom obliku, uz potpunu eliminaciju pomenute papirne forme, kao i podizanje efikasnosti i funkcionalnosti rada Ustavnog suda na znatno viši nivo. Postignuta je potpuna transparentnost u radu, kako unutar sistema, tako i za građane i privredne subjekte koji mogu pratiti status svog predmeta u Sudu. Ovaj rad ima za cilj da prikaže tehnološke i organizacione smernice za primenu koncepta korišćenja sistema za podršku odlučivanju u postupcima donošenja odluka u Ustavnom sudu.

### **Abstract:**

*The Constitutional Court of Serbia was established by the Constitution of the Socialist Republic of Serbia on April 9, 1963, as an independent body of the Republic, which ensures the protection of constitutionality and legality under the Constitution within the framework of its constitutionally established rights and obligations. A complex process of handling and deciding on constitutional court cases took place in the Constitutional Court, until 2011, in a traditional way, in the so-called "in paper form, that in August of that year his work was modernized by the introduction of business in electronic form through the Information System of the Constitutional Court (hereinafter: ISUS). The main goal of introducing such a Document Management System was to support the recording and processing of constitutional court cases in electronic form, with the complete elimination of the mentioned paper form, as well as raising the efficiency and functionality of the work of the Constitutional Court at a significantly higher level. Full transparency has been achieved in the work, both within the system, as well as for citizens and businesses that can monitor the status of their case in the Court. This paper aims to present technological and organizational guidelines for implementing the concept of using decision support systems in decision-making procedures in the Constitutional Court.*

### **1. UVOD - POSLOVNI PROCES**

Upravljanje poslovnim sistemom Ustavnog suda predstavlja složeni proces zasnovan na pravno proceduralnim, organizacionim i tehnološkim parametrima koji u svom sadejstvu trebaju da obezbede efikasno i racionalno funkcionisanje ove značajne državne institucije. Odluke i odlučivanje jesu svakodnevne ljudske delatnosti. Odluke se donose neprekidno u toku izvršavanja poslova vezanih za upravljanje aktivnostima i sistemima. Savremene informacione tehnologije omogućavaju prikupljanje, obradu i skladištenje podataka koje u fokus stavljaju upotrebljive podatke za analize i donošenje odluka na osnovu tih analiza [3].

Poslovni proces u elektronskoj formi u Ustavnom sudu odvija se počev od trenutka prijema podnesaka u Sud, njihovog evidentiranja, obrade, distribuiranja između radnih tela i obrađivača, pripreme sednice Suda, pripreme sednica radnih tela i na kraju u održavanju elektronske sednice kao finalnog dela u postupanju po ustavnosudskim predmetima, nakon čega se odluke ekspeduju učesnicima u postupku i šalju, u slučajevima predviđenim zakonom, na objavljivanje u odgovarajuće službeno glasilo. Ustavni sud na godišnjem nivou formira oko 11.000 predmeta, uglavnom po ustavnim žalbama, odnosno oko 1.000.000 raznih dokumenata.

ISUS pruža pomoć na svim nivoima postupanja i odlučivanja (radna tela, mala i velika veća, sednica Suda), sa posebnim značajem za podršku odlučivanju kroz vertikalne informacione tokove, a time i integraciju informacija koje se koriste na različitim organizacionim i upravljačkim nivoima.

Uspostavljanje efikasnog produkcionog okruženja za rad Ustavnog suda nosi sa sobom rizike u domenu mogućeg pristupa struktuiranim podacima neovlašćenih lica. U cilju sprečavanja ovakvog scenarija primenjene su tehničke mere koje obezbeđuju sigurnost i bezbednost ISUS-a uz potpuno uvažavanje pozitivnih propisa u ovoj oblasti, ali i sagledavanja tog sistema u realnom tehničko-tehnološkom okruženju. Ovakvim merama štiti se fizički integritet celokupnog informacionog sistema onemogućavanjem VPN pristupa, kao i implementacija neophodnih mera bezbednosti u samom ISUS-u kroz: a) autentifikaciju korisnika, b) autorizaciju korisnika, c) obezbeđenje integriteta podataka kroz proveru privilegija nad podacima [5].

### **Faze poslovnog procesa**

- Prijem podnesaka u pisarnici
- Klasifikacija i trijaža
- Formiranje predmeta (elektronski unos podataka o predmetu, elektronsko određivanje sudije izvestioca i

- dr.)
- Prethodna kontrola
- Prosleđivanje predmeta sudiji izvestiocu i obrađivaču i stručna obrada
- Odobranje predloga odluke/rešenja od strane sudije izvestioca
- Prijavlivanje i prosleđivanje predmeta na sednicu odbora, odnosno veća i sednice Suda
- Kreiranje dnevnog reda od strane sekretara odbora
- Priprema i održavanje sednice odbora
- Završna obrada predmeta od strane obrađivača nakon sednice odbora
- Odobranje sadržaja predmeta za sednicu veća, odnosno Suda od strane sudije izvestioca
- Prijavlivanje i prosleđivanje predmeta na sednicu veća ili Suda
- Kreiranje dnevnog reda sednice suda od strane sekretara/zamenika sekretara Suda
- Verifikacija predloženog dnevnog reda od strane predsednika Suda
- Održavanje sednice veća/Suda
- Završna obrada predmeta nakon sednice veća, odnosno Suda
- Rad Redakcione komisije
- Okončanje rada na predmetu

## 2. ARHITEKTURA SISTEMA

### 2.1 Moduli

- Podsystem za pisarnicu, pripremu elektronskih sednica i praćenje realizacije
- Podsystem e-sednica, za upravljanje tokom sednica
- Podsystem za razmenu podataka sa JP „Službeni glasnik RS,„
- Podsystem za elektronsku razmenu podataka između informacionog sistema US i web sajta Ustavnog suda
- Podsystem za izradu plana rada Ustavnog suda po kvartalima
- Podsystem za statističko izveštavanje o radu Ustavnog suda (sudije, obrađivači, vrste donetih odluka po načinu odlučivanja i ishodima i dr.)

### 2.2 Softverske komponente sistema RDMBS

- **RDBMS** (Relational Database Management System) je sistem za upravljanje relacionim bazama podataka
- **MS SQL Server** je server baze podataka koji je zadužen za skladištenje svih podataka modela koji nisu sam sadržaj dokumenta (atributi predmeta i dokumenta, procesi, zadaci i dr).

### 2.3 Softverske komponente sistema Content Server

**EMC Documentum Content Server** je centralna komponenta sistema, zadužena za upravljanje sadržajima repozitorijuma i opsluživanje zahteva klijenata.

**EMC Documentum Java Method Server** je aplikativni server ugrađen u Content Server zadužen za izvršavanje specifičnih zadataka, kao što su transfer sadržaja i aktivnosti procesa.

**EMC Documentum DFS** (Documentum Foundation Services) Server je aplikativni server na kome se nalaze i izvršavaju Documentum web servisi koji

omogućavaju integraciju trećih aplikacija ili klijentskih modula u drugoj tehnologiji (poput modula ESednice na .NET platformi).

### 2.4 Softverske komponente sistema Index Server

**EMC Documentum Index Server** je komponenta na posebnom serveru, zadužena za indeksiranje svih tekstualnih sadržaja i pretragu po tom sadržaju. **Index Agent** je zadužen za preuzimanje zadataka za indeksiranje i prosleđivanje indeksnom serveru, kao i za vraćanje rezultata pretrage po indeksu.

### 2.5 Softverske komponente sistema Application Server

**Apache Tomcat 6** je aplikativni server koji hostuje aplikaciju za pisarnicu, pripremu sednica i praćenje realizacije.

**EMC Documentum WDK** (Web Development Kit) je radni okvir (eng. framework) za razvoj web aplikacija na EMC Documentum platformi. Zasnovan je na JSP tehnologiji. Na njemu je razvijena i web aplikacija **WebTop**, koja predstavlja osnovu podsistema za pisarnicu, upravljanje predmetima i pripremu sednice. **EMC Documentum WebTop** je web aplikacija, koja sadrži sve suštinske funkcije ECM (Enterprise Content Management) sistema, i kao takva predstavlja osnovu podsistema za pisarnicu, upravljanje predmetima i pripremu sednice.

**EMC Documentum Administrator** je web aplikacija za centralizovanu administraciju celokupnog EMC Documentum sistema – administraciju korisnika, uloga, grupa, konfiguracije repozitorijuma, izvršavanje zakazanih poslova, administraciju listi kontrola pristupa i dr.

**Comtrade SpinnTop web aplikacija** je osnovni interfejs za rad sa sistemom korisnika pisarnice, obrade predmeta i pripreme sednica. Sastoji se od modula pisarnice, obrade predmeta i pripreme sednice koji su integrisani u jedinstvenu aplikaciju. Predstavlja prilagođenje WebTop aplikacije specifičnim potrebama Ustavnog suda.

**ESednice** je modul zadužen za implementaciju korisničkog interfejsa samog toka elektronske sednice Ustavnog suda.

**ESednice Servis** (ESession Service) je pozadinska komponenta modula za implementaciju toka sednice Ustavnog suda, zadužen za međusobnu komunikaciju i sinhronizaciju svih elemenata modula.

**Statistika Servis** je servis zadužen za slanje podataka koji se koriste za statistiku.

**Razmena Servis** je skup web servisa zaduženih za razmenu dokumenata između državnih organa.

**IMIS Scan ++** je klijentska windows desktop aplikacija zadužena za skeniranje i OCR (Optical Character Recognition) svih ulaznih dokumenata. Instancira se iz SpinnTop aplikacije, modula pisarnice, korišćenjem ActiveX tehnologije.

### 2.6 Korišćene tehnologije

Osnova ISUS-a je EMC Documentum platforma, koja se sastoji od više internih komponenti, razvijenih u Java i C++ okruženjima.

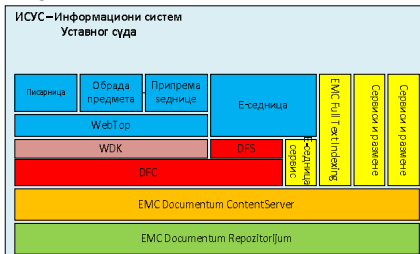
Moduli za pisarnicu, obradu predmeta i pripremu sednice su deo ISUS/SpinnTop aplikacije. Kao osnova ISUS/SpinnTop aplikacije iskorišćena je EMC Documentum WebTop aplikacija, koja je razvijena na WDK radnom okviru, baziranom na JAVA JSP tehnologiji.

Moduli ESednice, Esednice servis, Razmena Servis i Statistika Servis predstavljaju .NET module.

### 2.6.1 Logička arhitektura

Pod logičkom arhitekturom podrazumeva se poslovno-tehnološki pogled na sistem, sa prikazanim komponentama sistema i njihovim odnosom.

Slika br.1 Logička arhitektura sistema



#### Logička arhitektura-repozitorijum

Na najnižem nivou arhitekture, nalazi se EMC Documentum repozitorijum, kao skladište svih predmeta i dokumenata. Svi atributi poslovnih entiteta, poput dokumenata, predmeta, procesa, nalaze se u relacionoj bazi podataka (SQL Server), dok se sadržaji dokumenata nalaze na fajl storu, tj. definisanom prostoru na storage uređaju. To su osnovne komponente EMC Documentum repozitorijuma.

#### Logička arhitektura-upravljanje sadržajima

Za upravljanje sadržajima zadužen je EMC Documentum Content Server, kao servis koji prima zahtev za operaciju nad repozitorijumom, izvršava operaciju i vraća odgovor klijentu koji je poslao zahtev. Ni jednom objektu repozitorijuma nije moguće pristupiti bez Content Servera. Klijenti mu pristupaju korišćenjem API-ja, kao što su DFC (Documentum Foundation Classes) i DFS (Documentum Foundation Services). DFC je prirodni Java API, skup biblioteka koje implementiraju funkcionalnosti platforme, tj. Content Servera. DFS je web service API, koji predstavlja DFC izložen u vidu skupa web servisa, za integraciju sa drugim tehnologijama ili spoljnim sistemima.

#### Logička arhitektura-pretraga sadržaja

EMC Documentum Full Text Indexing predstavlja posebnu komponentu sistema, zaduženu za automatsko indeksiranje po tekstualnom sadržaju, tako da su objekti pretraživi po delu svog sadržaja. Prilikom kreiranja novog dokumenta u sistemu, ukoliko je on tekstualnog sadržaja, tj. moguć za indeksiranje, on se automatski smešta u red za indeksiranje, koji se u zadatim vremenskim intervalima proverava od strane EMC Documentum Index Agent-a, servisa koji čini integralni deo indeksnog servera. Indeksni agent šalje

sadržaj na indeksiranje, posle čega je dokument raspoloživ i za pretragu po sadržaju.

#### Logička arhitektura-WEB aplikacije

WDK (Web Development Kit) je razvojno okruženje zasnovano na JSP tehnologiji, koje je namenjeno razvoju EMC Documentum web aplikacija, kao što je WebTop. U svojoj arhitekturi koristi DFC za pristup Content Server-u. Nadgradnjom aplikacije WebTop i daljim prilagođenjima razvijeni su moduli za pisarnicu, obradu predmeta i pripremu sednice, klijentske web aplikacije, prikazane kao najviši sloj u arhitekturi ISUS rešenja. Oni objedinjeno predstavljaju ISUS/SpinnTop aplikaciju za krajnje korisnike.

#### Logička arhitektura E-sednice

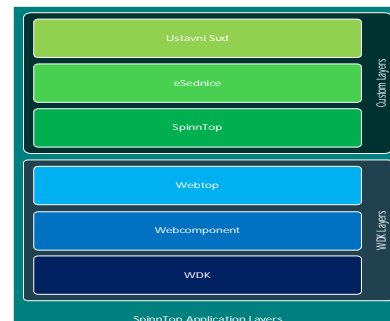
E-sednica je podsistem za upravljanje tokom sednica Ustavnog suda, a predstavlja desktop aplikaciju, u kiosk režimu, razvijenu u .NET tehnologiji. Za rad sa podacima, predmetima, dokumentima, tačkama dnevnog reda, koji su smešteni u EMC Documentum repozitorijumu, koristi DFS, kao web servis API, koji omogućuje razvoj EMC Documentum klijentskih aplikacija u tehnologijama koje nisu Java tehnologije. Modul koristi i E-sednica Servis, koji je zadužen za komunikaciju i slanje poruka između servera i klijenata, učesnika sednice.

#### Logička arhitektura-servisi

Servisi statistike su .NET komponenta zadužena za slanje statistike predmeta web servisu „Informatike“. Servisi razmene su .NET web servisi koji su namenjeni razmeni dokumenata sa JP „Službeni glasnik RS“.

#### ISUS/Spinn Top- slojevi aplikacije

Slika br.2 Slojevi aplikacije



#### Koncepti Web aplikacija – serverske komponente

Slika br.3 Serverske komponente



#### Koncepti Web aplikacija – klijentske komponente

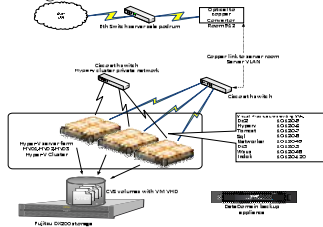


Slika br.4 Klijentske komponente



**Logički izgled infrastrukture**

Slika br.5 Logički izgled serverske arhitekture



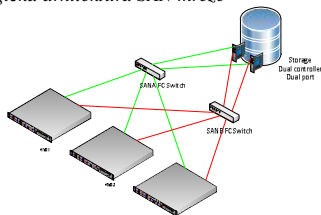
Primarni Data centar Ustavnog suda sastoji se od tri servera (Fujitsu Siemens) i Storage sistem (ETERNUS DX200 Base). Proces unapređenja serverskog dela infrastrukture sastoji se u tome da je na novim serverima (Fujitsu Primergy RX2530 M1 ) instaliran microsoft hypervisor HyperV V2. Virtualizacija je urađena na tri hosta HV1, HV2 i HV3. Kako bi se postigla veća dostupnost i veća skalabilnost sa visokim nivoom pouzdanosti ova tri hosta su stavljena u MS HyperV klaster koji ima ulogu da upravlja svim funkcijama datog klastera. Ovakva unapređena arhitektura omogućila je migraciju ISUS-a u potpuno novo virtuelno okruženje.

Slika br.6 Fizički izgled rack ormara Primarnog data centra



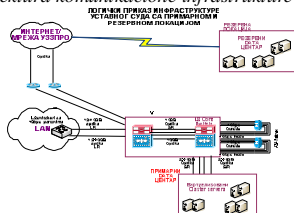
**Logička arhitektura LAN mreže**

Slika br.7 Logička arhitektura SAN mreže



SAN infrastruktura je izvedena preko dva brocade FC sviča koji čine dva nezavisna SAN ostrva radi potpune redundanse.

Slika br. 8 Arhitektura komunikacione infrastrukture



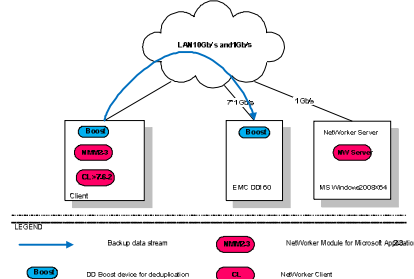
Na slici br.8 prikazana je topologija, odnosno arhitektura komunikacione infrastrukture na lokaciji Ustavnog suda. Na slici su predstavljeni spratni svičevi, centralni (backbone) svičevi koji skupljaju saobraćaj sa svih vertikalna i usmeravaju ga ka serverskoj infrastrukturi koja je na slici nazvana Server farm. Takođe, prikazana je i potrebna oprema za zaštitu sistema.

**Backup okruženje**

Backup produkcionog okruženja je zasnovan na EMC Networker proizvodu, koji je instaliran na virtualnoj mašini na produkcionom Hyper V clusteru. Networker server je verzije NetWorker 7.6.5.7.Build.1231 i instaliran je na windows server 2012. Networker klijenti su verzije 8.1.0.1.Build.199, jer omogućuju direktni backup na postojeći DataDomain 160 uređaj. Korišćenje DataDomain tehnologije radi se i deduplikacija podataka, što je značajno za uštedu prostora za Backup okruženje. Backup okruženje je projektovano tako da se sve produkcijske mašine na aplikativnom nivou štite direktno na nekoliko DataDomain device-ova. Networker server je instaliran na serveru pod imenom networker.isus.local.

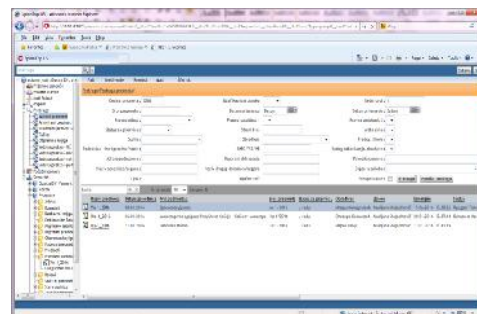
Slika br.9 predstavlja metodologiju backup-ovanja uz korišćenje Networker klijenata koji se instaliraju na svaki server koji se backup-uje.

Slika br. 9 Metodologija backup-ovanja



**3. IZGLED APLIKATIVNOG REŠENJA**

Slika br.10 Forma aplikativnog rešenja

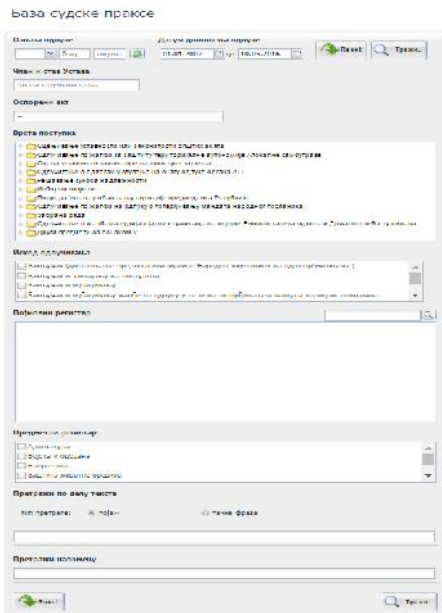


**4. BAZA SUDSKE PRAKSE**

Baza sudske prakse sadrži izabrane i klasifikovane odluke Ustavnog suda, počev od 1.januara 2007.

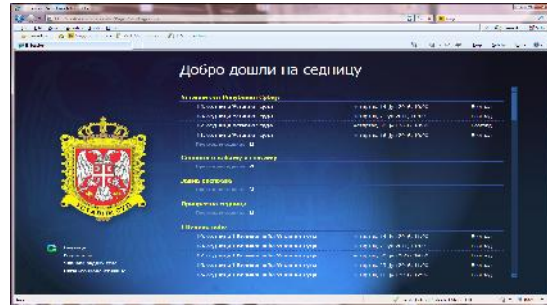
godine. Baza se redovno ažurira unošenjem odluka o kojima je Ustavni sud odlučivao u tekućoj godini. U bazi sudske prakse postoje dva „prozora“ sa različitim kriterijumima koji zavise od klasifikacionih oznaka odluka. Sadržaj formi za izbor kriterijuma pretrage zavisi od oznake odluke odnosno da li se radi o:

- odlukama donetim u postupcima po ustavnim žalbama (klasifikaciona oznaka UŽ ) ili
- odlukama iz drugih nadležnosti Ustavnog suda (IU, odlučivanje o saglasnosti opštih akata s Ustavom, zakonom, opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, IJU - ocena ustavnosti zakona koji je izglasan, a ukazom još nije proglašen, IIJU - rešavanje sukoba nadležnosti između različitih grana vlasti, IVU - odlučivanje o postojanju povre4de Ustava u obavljanju funkcije predsednika Republike, VU - odlučivanje o izbornim sporovima za koje zakonom nije određena nadležnost sudova, VIU - odlučivanje po žalbi na odluku donetu u vezi sa potvrđivanjem mandata, VIIU - odlučivanje o zabrani verske zajednice, o zabrani rada političke stranke, sindikalne organizacije ili udruženja građana, VIIIU - žalba protiv odluke o prestanku sudijske funkcije I žalba protiv odluke o prestanku funkcije javnog tužioca, IXU – odlučivanje po žalbi na pojedinačni akt ili radnju državnog organa ili organa jedinice lokalne samouprave kojim se onemogućava vršenje nadležnosti autonomne pokrajine, odnosno lokalne samouprave i XU - drugi poslovi predviđeni Ustavom I zakonom).

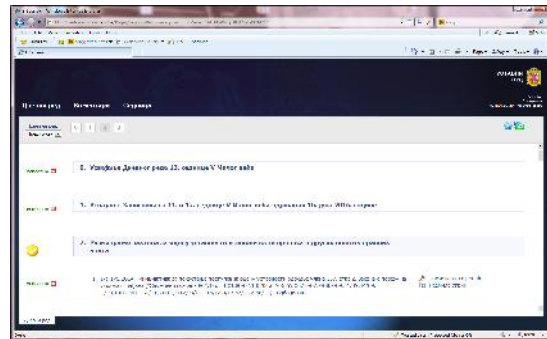


## 5. MODUL E-SEDNICE

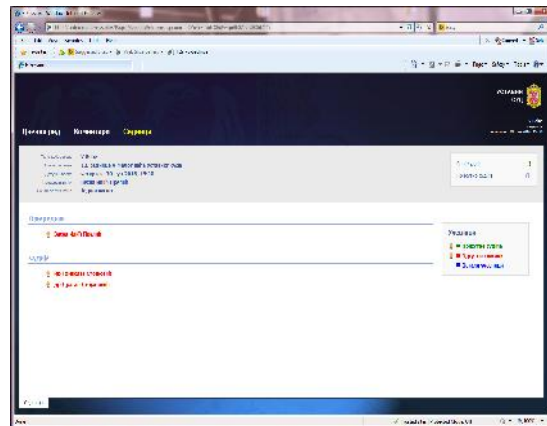
Slika br.11 Izgled forme modula E-sednice



Prikaz dnevnog reda sednice i glasanja



Prikaz sudijskog sastava odgovarajućeg veća/sednice Suda ili radnog tela



## 6. MODUL POSLOVNO IZVEŠTAVANJE

Slika br.12 Izgled forme modula poslovno izveštavanje



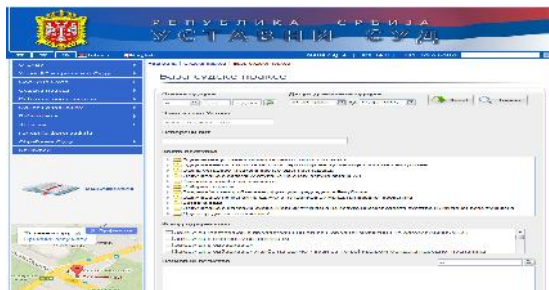
U pomentom modulu izvršavaju se svi definisani izveštaji o radu Ustavnog suda prema zadanim kriterijumima.

## 7. INTERNET SAJT USTAVNOG SUDA

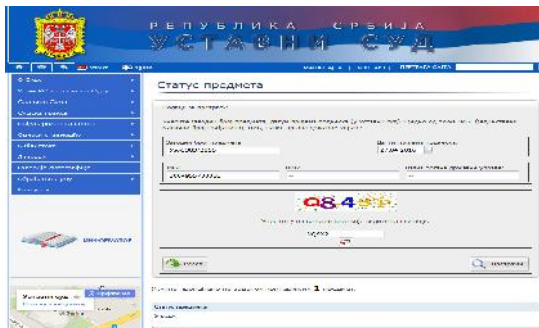
Slika br. 13 Izgled forme sajta Ustavnog suda



Baza sudske prakse



Status predmeta u sudu



## 8. ZAKLJUČAK

Primena ovakvog elektronskog sistema, za razliku od tradicionalnog, tzv. papirnog sistema, za rezultat ima brojne prednosti za državu, pravne subjekte i građane kroz sledeće globalne korisnosti [1]: smanjenje vremena rešavanja predmeta, transparentnost, povećanje učinka rada, bolje razumevanje problema koji se rešava, kvalitetnije odluke, poboljšanje kontrole odlučivanja i efikasniji timski rad [2].

Multidisciplinarnost je nezaobilazna za donošenje odluka u Ustavnom sudu. Proces odlučivanja mora uzeti u obzir i predefinisati sve potrebne parametre [4] (prava, ekonomije, sociologije, matematike,

psihologije, filozofije...) za donošenje određene odluke zasnovane na znanju.

Proces odlučivanja i donošenje odluke u nekom državnom organu, dakle i u Ustavnom sudu, mora uvažavati sve oblasti koje utiču na proces/sistem na koji se odnosi odluka. Kako pravo nije izolovana naučna celina već se odnosi na društvo sa svojim socijalnim, filozofskim i psihološkim aspektima, tako se moraju uvažavati i tehnološki aspekti informaciono komunikacionih resursa. Tehnologija doprinosi povećanju efikasnosti i produktivnosti rada Ustavnog suda, ali ne može da zameni donosioc odluka u okviru pravno uređenog organizacionog sistema.

Potreba za podrškom u odlučivanju proističe iz spoznaje najčešće finansijskih i vremenskih ograničenja u Ustavnom sudu. Za uspešan proces odlučivanja potrebno je racionalno postaviti ciljeve odlučivanja, racionalno identifikovati probleme i povoljnosti i racionalno odabirati metode i tehnike odlučivanja. Odluke treba bazirati na unapred definisanim pristupima, metodama i tehnikama suprotno od intuitivnog odlučivanja.

Ograničenja sistema za podršku odlučivanju su neke urođene ljudske veštine i talenti, kao i znanja, koji se ne mogu ugraditi u današnje sisteme za podršku odlučivanju. Tako je i ISUS ograničen na projektovane softverske mogućnosti, a broj korisnika sistema definisan unutar njega. ISUS je osmišljen za prilično usku i specifičnu oblast primene, što ga čini jedinstvenim informacionim sistemom državnih organa.

## 9. LITERATURA

- [1] Dragović R., *Funkcionalne preporuke za uspostavljanje pravosudnog informacionog sistema*, Zbornik radova ISDOS, 2010.
- [2] Dragovic R., "Data mining sistemi kao podrška istražnim radnjama", Zbornik radova YUINFO, 2011
- [3] Dragović R., Ivković M., Perović B., Klipa Đ., *Dataveillance i data mining kao tehnološka podrška procesu istražnih radnji*, Zbornik radova TELFOR, 2011
- [4] Harrision, E. F. (1987): *The Managerial Decision-Making Process*, Houghton Mifflin Company, Boston
- [5] Dragović R., Perović B., Klipa Đ., Pešić Lj., Nuhović E. *Preporuke za unapređenje bezbednosti baza podataka u pravosudnom informacionom sistemu*, Zbornik radova YUINFO, 2012

# PRIMENA GIS ALATA U KARTIRANJU RIZIKA OD POPLAVA APPLICATION OF GIS TOOLS IN FLOOD RISK MAPPING

Nevena Cvijanović<sup>1</sup>, Boris Krunic<sup>1</sup>, Vojislav Antonić<sup>1</sup>

*Institut za vodoprivredu "Jaroslav Černi"<sup>1</sup>*

**Sadržaj** – Kartiranje rizika od poplava predstavlja jednu od najvažnijih stručnih aktivnosti za efikasno upravljanje rizikom od poplava. Analiza potencijalnog rizika od poplava i njegovo kartiranje igraju važnu ulogu u okviru neinvesticionih mera zaštite od poplava. Pri izradi karata rizika od poplava danas se masovno koriste geografski informacijski sistemi (GIS) koji omogućuju efikasan način integrisanja podataka iz različitih softverskih okruženja i obavljanje svih neophodnih prostornih analiza i proračuna (hidroloških, hidrauličkih, ekonomskih i dr.). U ovom radu je prikazana primena GIS alata u kartiranju rizika od poplava na primeru doline reke Resave.

**Abstract** - Flood risk mapping is one of the most important professional activities for efficient flood risk management. Investigation of the potential flood risk and its mapping play a significant role within the non-investment measures for flood protection. Lately, the main part in production of flood risk maps have Geographic Information Systems (GIS) which provide an efficient method for integrating data from different software environments, and perform all necessary spatial analysis and calculations (hydrologic, hydraulic, economic, etc.). This paper presents the application of GIS tools in flood risk mapping in the case of the Resava River.

## 1. UVOD

Zaštita od poplava je oblast kojoj se u poslednjim decenijama poklanja velika pažnja u mnogim zemljama. Osnovni razlog za to jeste taj što poplave postaju sve učestalija pojava usled uticaja raznih prirodnih i ljudskih faktora. Štete koje nastaju plavljenjem nekog područja su neprocenjive, s obzirom na to da se od svih prirodnih katastrofa, u poplavama izgubi najveći broj ljudskih života. U skladu sa tim, razvija se potreba za naprednijom zaštitom od poplava i njenim uspešnijim upravljanjem, kako bi se štete usled poplava smanjile na najmanju moguću meru. Kao rezultat ove potrebe, nastale su karte rizika od poplava, kojima se prikazuje stepen ugroženosti od poplava nekog područja. Na ovaj način postiže se efikasan način informisanja i razvoja svesti šire javnosti o riziku od poplava i merama za njenim uspešnim upravljanjem.

## 2. METODOLOGIJA KARTIRANJA RIZIKA OD POPLAVA

Rizik od poplava predstavlja verovatnoću pojave štete na području koje je ugroženo poplavama i kvantifikuje se preko očekivane godišnje štete, u zavisnosti od verovatnoće pojave plavnog događaja [1]. Kartiranje rizika sastoji se iz nekoliko koraka: hidrološko-hidrauličke analize na osnovu koje se određuje plavno područje, proračuna potencijalne štete odnosno njene očekivane godišnje vrednosti, procene rizika i njihovog

kartiranja. Veličina plavnog područja, potencijalna šteta i rizik zavise od dubine plavljenja, trajanja poplavnog talasa, topografije terena (rečne doline) i namene zemljišta koje je ugroženo poplavama.

### 2.1. Plavne površine i dubine plavljenja

Hidrološkom analizom velikih voda na pripadajućem slivnom području dobijaju se merodavni poplavni talasi različitih povratnih perioda za potrebe hidrauličke analize. Pored podataka o merodavnim poplavnim talasima, za hidrauličku analizu potrebni su topografija sliva i podaci o Maningovom koeficijentu rapavosti glavnog korita reke i plavnih površina. Ovaj koeficijent se određuje kalibracijom kada je u pitanju glavno korito, dok se za plavne površine uglavnom procenjuje na osnovu namene zemljišta duž rečne trase [2]. Hidraulički proračun sprovodi se primenom jednodimenzionalnih ili dvodimenzionalnih modela tečenja, za poplavne talase različitih povratnih perioda. Rezultati hidrauličkog proračuna integrišu se u GIS okruženje i na taj način se dobijaju granice plavnog područja (plavne zone) i dubine plavljenja.

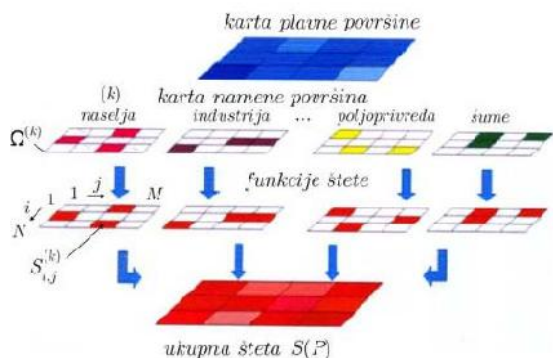
### 2.2. Definisane štete

*Specifične štete.* Veličina štete usled pojave poplave prvenstveno zavisi od veličine plavnog područja, namene zemljišta i vrednosti materijalnih dobara na tom području. Samim tim vrednost štete zavisi od verovatnoće pojave poplavnog talasa. Elementi koji su potrebni za određivanje štete jesu vrednosti pripadajuće imovine na datom zemljištu, površina zemljišta, i na kraju specifične (jedinične) štete koje se dobijaju kao odnos prethodna dva elementa za svaki tip namene zemljišta [4]. Ovako dobijene štete nisu stvarne već maksimalne štete, koje se ne mogu dostići čak ni u slučaju pojave velikih voda visokih povratnih perioda. Stvarne štete se mogu određivati jedino analizom poplava koje su se već dogodile na nekom području.

*Funkcije štete* predstavljaju zavisnosti između dubine vode na plavnim površinama i štete koju bi ta dubina vode izazvala na površini određene namene (potencijalne štete). Mogu uzimati vrednosti od 0, u slučaju da šteta ne postoji, i 1 kada se ostvaruje potpuna šteta. Funkcije štete su definisane sledećim parametrima: početnom vrednošću, odnosno prvom pojavom štete (odsečak funkcije na ordinati), maksimalnom vrednošću i oblikom funkcije. Funkcije štete se mogu zasnivati na stvarnim štetama (štete koje su registrovane nakon pojave poplave koja se desila u prošlosti) i na sintetičkim (potencijalnim) štetama koje se koriste za potrebe analiza u prognostičke svrhe [5]. Ove funkcije nisu univerzalne za sva područja, već se moraju posebno određivati u skladu sa razmatranim područjem.



Potencijalna (moguća) šteta obuhvata sve elemente područja koji podležu poplavama, a to su: ljudski životi, životinje, stambeni i industrijski objekti, infrastruktura, pokretna imovina, šume, javne i poljoprivredne površine i dr. Potencijalne štete određuju se na osnovu funkcija šteta za različite namene zemljišta i dubina plavljenja vodama različitih povratnih perioda (slika 1). U našoj praksi se zbog nedovoljnog broja potrebnih podataka uglavnom usvajaju originalni ili delimično korigovani oblici funkcija šteta, koje su formirane u razvijenijim zemljama za potrebe njihovih projekata [4].



Slika 1. Procena ukupne potencijalne štete za poplavu određenog povratnog perioda

Očekivana godišnja šteta se određuje na osnovu sračunatih mogućih šteta, usled poplava različite verovatnoće pojave. Matematički se definiše kao integral funkcije moguće štete u zavisnosti od povratnog perioda poplavnog talasa. Kao donja granica integrala usvaja se najniži povratni period poplavnog talasa pri kome dolazi do pojave štete na razmatranom području. Za gornju granicu integrala usvaja se vrednost maksimalnog povratnog perioda poplave koja se razmatra u analizi rizika. Opisani postupak može se definisati sledećim izrazom:

$$\bar{S} = \int_{P_0}^{P_{max}} S(P) dP \quad (1)$$

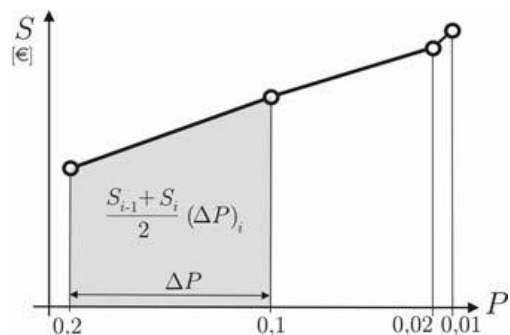
gde su:  $\bar{S}$  –srednja godišnja šteta [€god],  $S(P)$ –očekivana šteta od poplave u funkciji verovatnoće pojave poplave  $P$ ,  $P_0$  –verovatnoća pojave najmanje poplave pri kojoj dolazi do pojave materijane štete,  $P_{max}$ –verovatnoća pojave najveće razmatrane poplave.

Vrednost integrala se određuje numeričkom integracijom funkcije mogućih šteta, uglavnom trapeznim pravilom (slika 2), pod pretpostavkom da je funkcija mogućih šteta između dva intervala linearna [1].

### 2.3. Karte rizika od poplava

Karta rizika od poplava dobija se klasifikacijom specifične godišnje štete prema učestalosti poplava i visini štete koja može nastati njenom pojavom. Rizik se uglavnom deli u tri zone (klase): visok, umeren i nizak, koje se na kartama prikazuju različitim bojama. Klasifikovanje rizika još uvek nije standardizovano pa se može izvršiti na više načina. Usled postojanja velike razlike u specifičnim štetama na urbanim i neurbanim

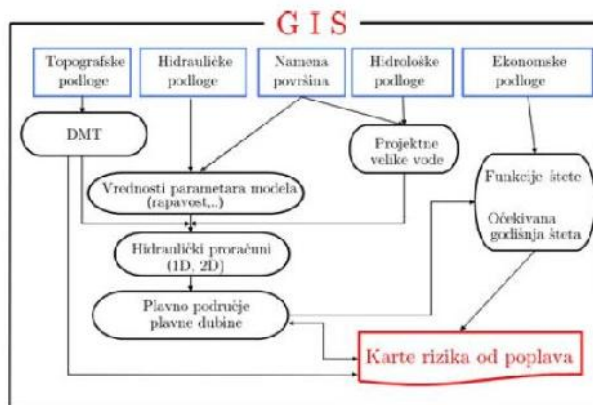
površinama, klasifikacija rizika se uglavnom definiše posebno za oba tipa područja.



Slika 2. Određivanje očekivane godišnje štete numeričkom integracijom funkcije mogućih šteta, trapeznim pravilom

### 3. PRIMENA GIS APLIKACIJA U KARTIRANJU RIZIKA

GIS tehnologije se primenjuju u raznim stručnim oblastima i imaju značajnu ulogu u analizama prostornih podataka i grafičkom predstavljanju njihovih rezultata. Primena GIS alata znatno olakšava postupak izrade karata rizika od poplava jer pored prostornih analiza omogućuje i različite proračune koristeći podatke iz drugih softverskih okruženja.



Slika 3. Shema primene GIS alata u izradi karata rizika od poplava

Prvi korak u procesu kartiranja rizika jeste izrada digitalnog modela terena, koji predstavlja kontinualnu površ formiranu na osnovu prikupljenih podataka o tačkama terena. Ovaj model se dalje koristi u hidrauličkim analizama kako bi se odredile plavne površine za poplavne talase različitih povratnih perioda i dubine vode koje se formiraju na površinama prilikom njihovog plavljenja.

Pored plavnih zona i dubina plavljenja u ovim zonama, na razmatranom području potrebno je napraviti kartu namene površina koja se dobija digitalizacijom topografskih podloga na kojima se jasno vide različite namene zemljišta. Sledeći korak je formiranje karte potencijalnih šteta koja se dobija na osnovu prikupljenih podataka o jediničnim štetama, funkcijama šteta u zavisnosti od postojećih namena površina, i dubina plavljenja na tim



površinama. Ovaj postupak izvodi se vrlo jednostavno zahvaljujući raspoloživim GIS alatima (*Spatial Analyst*) u okviru *ArcMap* aplikacije, koji omogućuju analize i kombinovanje podataka prikazanih u obliku takozvanih rastera na kojima su podaci predstavljeni mrežom piksela.

Integracijom funkcije potencijanih šteta u zavisnosti od povratnog perioda poplavnog talasa, takođe korišćenjem pomenutih GIS alata, određuje se karta očekivanih godišnjih šteta. Klasifikacijom godišnjih šteta na osnovu usvojenih pragova prema visini štete definišu se zone rizika. S obzirom na to da se štete koje mogu nastati nakon plavljenja nekog područja, znatno razlikuju na urbanim i ruralnim područjima, trebalo bi usvojiti različite pragove za klasifikaciju rizika na obe vrste područja [3]. Vrednosti ovih pragova nisu univerzalne već ih je potrebno odrediti ekonomskim analizama.

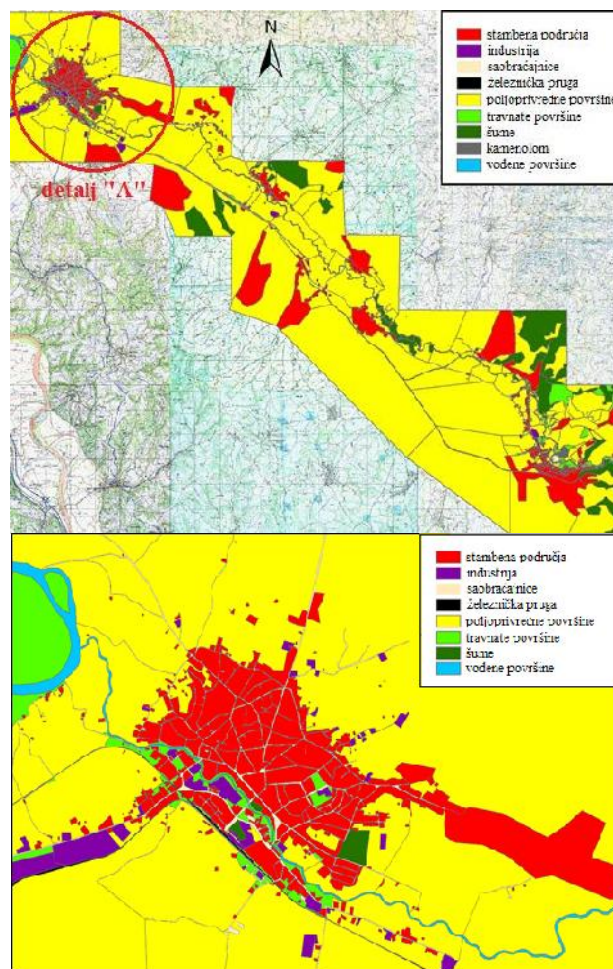
#### 4. PRIMER REKE RESAVE

Metodologija izrade karata rizika od poplava primenjena je na dolinu reke Resave koja pripada istočnom delu Srbije i najduža je desna pritoka Velike Morave. Za potrebe ovog rada analizira se deonica duga 43 kilometra, koja se prostire od Despotovca do ušća u Veliku Moravu i pripada donjem delu sliva u kome se ostvaruje mirno tečenje.

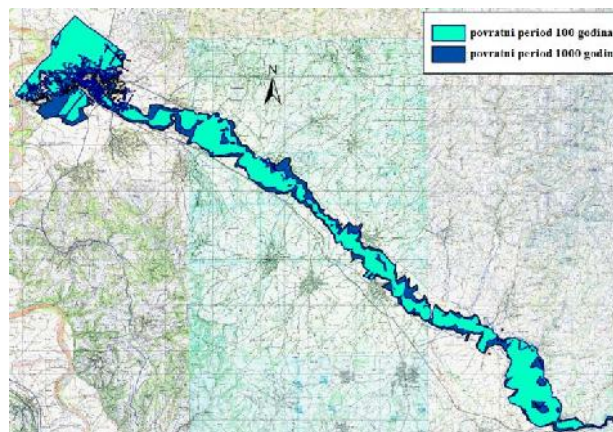
Za izradu potrebnih geodetskih podloga u ovom radu korišćeni su programi AutoCAD Civil 3D i ArcMap GIS aplikacija. Digitalni model terena formiran je na osnovu topografske karte razmere 1:25.000 i snimljenih poprečnih profila duž rečnog korita. Na osnovu digitalnog modela terena dobijena je geometrija korita i rečne doline koji su korišćeni u hidrauličkoj analizi. Namene površina na razmatranom području identifikovane su na osnovu raspoloživih ortofoto snimaka i topografske karte i digitalizovane u aplikaciji *ArcMap* (slika 4).

Karakteristične vrednosti proticaja velikih voda, koji su korišćeni u hidrauličkoj analizi odgovaraju povratnim periodima 100 i 1000 godina. Hidraulički proračun sproveden je programskom paketu HEC-RAS pod pretpostavkom linijskog, ustaljenog i nejednolikog tečenja u mirnom režimu. Rezultati proračuna integrisani su u *ArcMap* okruženje pomoću GIS alata *HEC-GeoRAS* koji omogućuje komunikaciju između ova dva programa. Na ovaj način dobijene su plavne zone (slika 5) i dubine plavljenja na razmatranoj deonici za poplavne talase povratnih perioda 100 i 1000 godina.

Usled nedovoljnog broja podataka koji su potrebni za definisanje funkcija šteta u ovom primeru usvojene su originalne funkcije potencijalnih šteta koje su korišćene u Nemačkoj za analizu rizika u dolini reke Elbe (Slika 6). Razlog za odabir baš ovih funkcija jeste taj što se u dolini razmatrane deonice reke Resave pretežno prostiru poljoprivredne površine, pa je samim tim i njihov uticaj na ukupne štete veoma značajan. Kako bi se taj uticaj adekvatno istakao u rezultatima proračuna, usvojene su



Slika 4. Namene površina duž doline reke Resave (gore), sa detaljem gradske zone (dole)

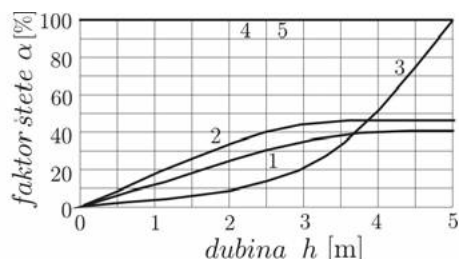


Slika 5. Plavne zone u dolini reke Resave za povratne periode 100 i 1000 godina

ove funkcije jer se u njima za poljoprivredne površine usvaja totalna šteta prilikom njihovog plavljenja. Korišćenjem podataka o dubinama plavljenja dobijenih hidrauličkom analizom i jediničnih vrednosti šteta (tabela 1), određene su specifične potencijalne štete [€/m<sup>2</sup>] za različite namene zemljišta.

Očekivane godišnje štete određene su pomoću funkcije *Raster Calculator* u okviru *Spatial Analyst* alata, korišćenjem prethodno definisanog izraza (1). S obzirom

na to da su na raspolaganju bile funkcije specifične moguće štete za dva poplavna talasa, povratnih perioda 100 i 1000 godina, korišćen je samo jedan interval verovatnoća pojave duž koga je određen integral funkcije specifičnih mogućih šteta. Ovaj postupak ponovljen je za sve tipove namena površina i na taj način dobijena je karta specifičnih godišnjih šteta na razmatranom području.

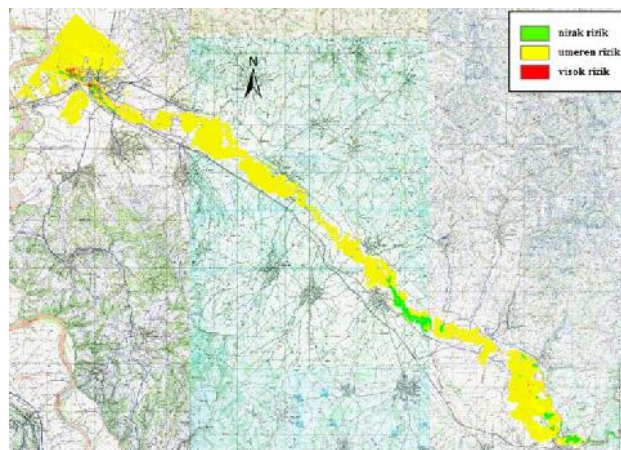


Slika 6. Funkcije šteta od poplava u dolini reke Elbe: 1 – naselja, 2 – industrija, 3 – saobraćajna infrastruktura, 4 – poljoprivreda, pašnjaci/livade, 5 – šume

Tabela 1. Usvojene vrednosti jediničnih šteta [€m<sup>2</sup>]

Namena površina	Jedinične štete [€m <sup>2</sup> ]
Stambene oblasti	333
Industrija i trgovina	400
Saobraćajne i javne površine	160
Železnička pruga	583
Poljoprivredne površine	23
Travnate površine	0.075
Šume	0.1

Klasifikacija specifičnih godišnjih šteta, prema usvojenim vrednostima pragova za različite namene zemljišta, izvršena je pomoću funkcije *Reclassify*, koja se nalazi u okviru grupe alata *Spatial Analyst*. Za prag umerenog rizika u urbanim područjima (stambene oblasti, industrija, saobraćajnice) usvojena je vrednost od 0.03 [€/m<sup>2</sup>god], a za prag visokog rizika usvojena je vrednost od 1 [€/m<sup>2</sup>god]. Ove vrednosti pragova važe uglavnom u većini evropskih zemalja. U neurbanim područjima (poljoprivreda, travnate površine i šume), kao prag umerenog rizika usvojena je vrednost od 0.012 [€/m<sup>2</sup>god], koja se koristi u Nemačkoj [4]. Kao ulazni podaci korišćeni su prethodno dobijeni rasteri specifičnih godišnjih šteta za različite namene zemljišta. Ove štete su klasifikovane u definisane zone rizika za svaku namenu zemljišta posebno pa je time dobijena karta rizika od poplava (slika 7).



Slika 7. Karta rizika od poplava u dolini reke Resave

## 5. ZAKLJUČAK

Izrada karata rizika od poplava je kompleksan posao, koji zahteva veliki broj ulaznih podataka o ugroženom području, koji nisu uvek lako dostupni, pa se mora pribegavati raznim pojednostavljenjima u analizi rizika. Zahvaljujući razvoju geografskih informacionih sistema (GIS), postupak izrade ovih karata znatno je olakšan, s obzirom na to da GIS omogućava da se većina analiza obavi baš u ovom softverskom paketu. Pored zavidnog nivoa detaljnosti obrade podataka koju pruža GIS, sama analiza u sebi nosi niz neizvesnosti i grešaka koji su posledica nedostatka i nepreciznosti ulaznih podataka koji se koriste u proračunima [4]. Uprkos tome, ove karte predstavljaju efikasan način prikazivanja stepena ugroženosti od poplava kojim se na jednostavan način može informisati i razviti svest šire javnosti o posledicama koje bi mogla izazvati ovakva prirodna katastrofa. Njihovom izradom definišu se smernice za uspešno upravljanje rizikom i unapređivanje zaštite od budućih poplava.

## LITERATURA

- [1] Jovanović, M. *Flood Risk Mapping*, Postgraduate Course in Water Resources and Environmental Management– Educate!, 2008.
- [2] Jovanović, M. *Regulacija reka-rečna hidraulika i morfologija*, Građevinski fakultet, Beograd, 2008.
- [3] Jovanović, M., Prodanović, D., Plavšić, J., Rosić, N. *Problemi pri izradi karata ugroženosti od poplava*, Vodoprivreda, Vol. 46, str. 3-13, 2014.
- [4] Jovanović, M., Todorović, A., Rodić, M. *Kartiranje rizika od poplava*, Vodoprivreda, Vol. 41, br.1-3, str. 31-45, 2009.
- [5] Kolarov, V., Babić Mladenović, M. *Podaci za izradu preliminarne procene rizika od poplava na teritoriji Republike Srbije*, Vodoprivreda, Vol. 42, br. 1-3, str. 79-86, 2010.