УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ЗБОРНИК РАДОВА
ФАКУЛТЕТА ТЕХНИЧКИХ НАУКА

Едиција: Техничке науке – зборници
Година: XLI
Број: 2/2026

Нови Сад

Едиција: „Техничке науке – Зборници“
Година: XLI Свеска: 2
Издавач: Факултет техничких наука Нови Сад

Главни и одговорни уредник Едиције: проф. др Борис Думнић, декан Факултета техничких наука у Новом Саду

Штампање одобрио: Савет за библиотечку и издавачку делатност ФТН, председник, проф. др Селена Самарџић Цвијановић

Штампа: ФТН – Графички центар ГРИД, Трг Доситеја Обрадовића 6, Нови Сад

CIP-Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

378.9(497.113)(082)
62

ЗБОРНИК радова Факултета техничких наука / главни и одговорни уредник
Борис Думнић. – Год. 7, бр. 9 (1974)-1990/1991, бр.21/22 ; Год. 23, бр 1 (2008)-. – Нови Сад : Факултет техничких наука, 1974-1991; 2008-. – илустр. ; 30 цм. – (Едиција: Техничке науке – зборници)

Месечно

ISSN 0350-428X

COBISS.SR-ID 58627591

ПРЕДГОВОР

Поштовани читаоци,

Пред вама је десета овогодишња свеска часописа „Зборник радова Факултета техничких наука“.

Часопис је покренут давне 1960. године, одмах по оснивању Машинског факултета у Новом Саду, као „Зборник радова Машинског факултета“, а први број је одштампан 1965. године. Након осам публикованих бројева у шест година, пратећи прерастање Машинског факултета у Факултет техничких наука, часопис мења назив у „Зборник радова Факултета техничких наука“ и 1974. године излази као број 9 (VII година). У том периоду у часопису се објављују научни и стручни радови, резултати истраживања професора, сарадника и студената ФТН-а, али и аутора ван ФТН-а, тако да часопис постаје значајно место презентације најновијих научних резултата и достигнућа. Од броја 17 (1986. год.), часопис почиње да излази искључиво на енглеском језику и добија поднаслов *Publications of the School of Engineering*.

Наставно-научно веће ФТН-а је одлучило да од новембра 2008. год. у облику пилот пројекта, а од фебруара 2009. год. као сталну активност, уведе презентацију најважнијих резултата свих мастер радова студената ФТН-а у облику кратког рада у „Зборнику радова Факултета техничких наука“.

Поред студената мастер студија, часопис је отворен и за студенте докторских студија, као и за прилоге аутора са ФТН или ван ФТН-а.

Зборник излази у два облика – електронском на веб-страници Факултета техничких наука (www.ftn.uns.ac.rs) и штампаном, који је пред вама. Обе верзије публикују се сваки месец, у оквиру промоције дипломираних мастера.

Известан број кандидата објавили су радове на некој од домаћих научних конференција или у неком од часописа. Њихови радови нису штампани у Зборнику радова ФТН-а.

У свесци са редним бројем 2 објављени су радови из области електротехничког и рачунарског инжењерства.

Континуираним радом и унапређењем квалитета часописа, план је да часопис постане препознатљив међу ауторима, чиме ће значајно допринети да се оствари мото Факултета техничких наука:

„Високо место у друштву најбољих“

Уредништво

Садржај

Електротехничко и рачунарско инжењерство

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.4
DOI: https://doi.org/10.24867/34BE02Popovic

PAMETNA BROJILA I NAPREDNI MERNI SISTEMI (AMI) KAO TEMELJ ZA RAZVOJ PAMETNIH MREŽA (SMART GRID)

SMART METERS AND ADVANCED MEASUREMENT SYSTEMS (AMI) AS A FOUNDATION FOR THE DEVELOPMENT OF SMART GRIDS

Stefan Popović, *Fakultet tehničkih nauka, Novi Sad*

Oblast - Primenjeno softversko inženjerstvo

Kratak sadržaj - *Rad obrađuje značaj pametnih brojila i naprednih mernih sistema (AMI) kao osnove za razvoj pametnih mreža (Smart Grid). Prikazane su njihove ključne funkcije, uloga u digitalizaciji elektroenergetskog sistema i primeri iz prakse.*

Ključne reči: *SmartGrid, Pametno brojilo, AMI, DLMS, COSEM*

Abstract - *The paper examines the importance of smart meters and Advanced Metering Infrastructure (AMI) as the foundation for the development of Smart Grids. Their key functions, role in the digitalization of the power system, and practical examples are presented.*

Keywords: *SmartGrid, Smart meter, AMI, DLMS, COSEM*

1. TRADICIONALNI ELEKTROENERGETSKI SISTEMI

Tradicionalni elektroenergetski sistemi godinama su se oslanjali na mehanička i elektromehanička brojila koja su evidentirala samo zbirnu potrošnju. Očitavanje je vršeno ručno, što je unosilo greške, kašnjenja i rizik od manipulacija. Njihov glavni nedostatak bila je statičnost - nisu pružali podatke o vremenskoj dinamici potrošnje, vršnim opterećenjima niti mogućnost komunikacije sa distributivnim centrom. Zbog toga nisu mogli da podrže detaljnu analizu, napredne tarife ni planiranje u uslovima rasta potrošnje, decentralizovane proizvodnje i razvoja elektromobilnosti, te su postali prepreka daljem razvoju sistema.

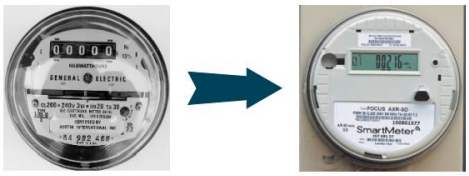
2. PRELAZAK NA PAMETNE MREŽE

Kako bi se odgovorilo na nove izazove u energetici, razvijen je koncept pametnih mreža (Smart Grid). Za razliku od tradicionalnih mreža, koje su se zasnivale na jednosmernom toku energije i centralizovanom upravljanju, SmartGrid integriše informaciono-komunikacione tehnologije u sve segmente sistema.

Pametna mreža omogućava dvosmernu komunikaciju, daljinsko upravljanje, automatizaciju i prikupljanje podataka u realnom vremenu.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio Doc. dr Aleksandar Bošković.

Posebno značajan je decentralizovani pristup, gde potrošači postaju i proizvođači energije („prosumers“), što povećava fleksibilnost i otpornost mreže.



Slika 1. *Tranzicija iz analognih u pametna digitalna brojila*

3. PAMETNA BROJILA

Pametna brojila (***smart meters***) predstavljaju savremene elektronske uređaje koji omogućavaju precizno, kontinuirano i daljinsko praćenje potrošnje električne energije. Za razliku od tradicionalnih mehaničkih brojila, koja registruju samo ukupnu potrošnju i zahtevaju fizičko očitavanje, pametna brojila omogućavaju automatsko očitavanje, dvosmernu komunikaciju i detaljnu analizu potrošnje u realnom vremenu. Kao ključna komponenta naprednog mernog sistema (AMI - Advanced Metering Infrastructure), pametna brojila predstavljaju interfejs između krajnjeg korisnika i distributivne mreže, čime se obezbeđuje pouzdana razmena informacija i efikasnije upravljanje sistemom.

3.1. Funkcionalnosti pametnih brojila

Pametna brojila predstavljaju novu generaciju mernih uređaja koja omogućavaju automatsko i daljinsko očitavanje, čime se postiže veća tačnost i smanjuju troškovi. Zahvaljujući dvosmernoj komunikaciji, ona ne samo da prenose podatke o potrošnji, već i primaju komande distributera - od promene tarifa do uključivanja i isključivanja potrošača.

Visoka vremenska rezolucija (na primer, na 15 minuta) omogućava detaljnu analizu potrošnje i bolje planiranje mreže. Brojila detektuju kvarove, prekide napajanja i pokušaje neovlašćene potrošnje, šaljući upozorenja u realnom vremenu, čime se povećava sigurnost sistema.

Dodatno, podrška za dinamičko tarifiranje i dostupnost podataka korisnicima kroz aplikacije podstiču racionalnije korišćenje energije. Integrisana sa pametnim domovima,

solarnim panelima i baterijama, pametna brojila postaju ključni deo AMI (Advanced Metering Infrastructure) i temelj razvoja Smart Grid sistema - efikasnijeg, pouzdanijeg i održivijeg elektroenergetskog okruženja.

3.2. Komunikacione tehnologije u ami sistemima

Rad AMI (Advanced Metering Infrastructure) sistema zasniva se na pouzdanoj dvosmernoj komunikaciji između brojila, koncentratora i centralnog sistema. U praksi se koriste različite tehnologije, u zavisnosti od okruženja i potreba:

- **PLC (Power Line Communication):** koristi postojeće elektroenergetske vodove, jeftino rešenje za gradske sredine, ali ograničeno u dometu i podložno smetnjama.
- **RF mreže:** bežična komunikacija u ***mesh*** (mrežna struktura u kojoj je svaki čvor povezan sa jednim ili više drugih čvorova i podaci mogu da putuju različitim rutama bez centralnog rutera) topologiji, fleksibilna i pogodna za urbana područja, ali osetljiva na interferencije.
- **Mobilne mreže (GPRS/3G/4G/LTE):** omogućavaju široku pokrivenost i direktnu vezu brojilo-server, idealne za ruralne oblasti, ali skuplje i zavisne od kvaliteta signala.
- **Optička vlakna/Ethernet:** nude veliku brzinu i pouzdanost, ali imaju visoke troškove pa se koriste u industrijskim i kritičnim objektima.
- **NB-IoT i LTE-M:** nove IoT tehnologije, energetski efikasne i pogodne za masovno povezivanje uređaja, ali još uvek neravnomerno dostupne.

U praksi se najčešće primenjuje **hibridni pristup**, koji kombinuje više tehnologija radi veće pouzdanosti i potpunog pokrivanja mreže.

Tehnologija	Cena implementacije	Zastupljenost	Domet i brzina
PLC (Power Line Communi)	Niska	Visoka (u gradovima)	Kratak, srednja brzina
RF (Radio Frequency)	Srednja	Veoma visoka	Kratak–srednji, umerena
Optička vlakna / Ethernet	Visoka	Niska–srednja	Dug, veoma visoka
GPRS / 3G / 4G / LTE	Srednja–visoka	Veoma visoka	Dug, srednja brana
NB-IoT / LTE-M	Niska–srednja	Rastuća	Dug, niska brzina

Slika 2. *Pregled komunikacionih tehnologija u AMI sistemima*

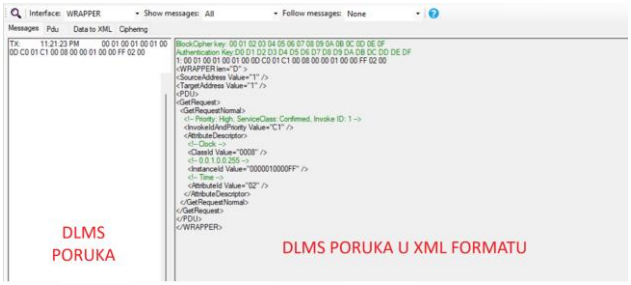
3.2. Komunikacioni protokoli u AMI sistemima

Komunikacioni protokoli u AMI sistemima predstavljaju skup pravila i standarda koji omogućavaju razmenu podataka između pametnih brojila, korisnika i distributivnih centara. Oni obezbeđuju pouzdanu, sigurnu i efikasnu komunikaciju, a izbor protokola zavisi od vrste energije, okruženja i zahteva sistema.

Najčešće se koristi DLMS/COSEM (IEC 62056), univerzalni i bezbedan standard za električna brojila, nezavisan od medijuma prenosa. M-Bus i Wireless M-Bus (EN 13757) namenjeni su vodi, gasu i toploti, jednostavni i energetski efikasni za masovno očitavanje. U industriji je prisutan Modbus, praktičan za PLC/SCADA sisteme, ali bez napredne bezbednosti. Za kućne mreže koristi se ZigBee Smart Energy, pogodan za pametne uređaje i HEMS (Home Energy Management System), sa niskom potrošnjom i mesh topologijom. IEC 60870-5-102 primenjuje se u SCADA okruženjima za telemetriju i merenje, dok je DLT645 kineski standard za brojila, široko rasprostranjen lokalno, ali sa slabijom međunarodnom interoperabilnošću.

3.3. DLMS/COSEM

DLMS/COSEM *(Device Language Message Specification /Companion Specification for Energy Metering)*, standardizovan kroz IEC 62056, predstavlja globalni okvir i de facto standard za komunikaciju sa pametnim brojilima. COSEM definiše semantiku podataka kroz objekte i OBIS (*Object Identification System*) kodove, dok DLMS određuje pravila razmene i pristupa, čime se obezbeđuje interoperabilnost uređaja različitih proizvođača. Zahvaljujući medijskoj neutralnosti, ovaj model funkcioniše preko PLC, RF, mobilnih i IP mreža, uz podršku „pull“ i „push“ komunikacije. Sistem uključuje višeslojnu bezbednost sa autentifikacijom, enkripcijom i digitalnim sertifikatima, što ga čini pogodnim za kritičnu infrastrukturu. Iako je implementacija kompleksna, DLMS/COSEM omogućava dugoročnu kompatibilnost, fleksibilno širenje i visoku pouzdanost, zbog čega predstavlja osnovu savremenih AMI sistema.



Slika 3. *Primer sirove DLMS poruke prevedene u XML COSEM format*

3.4. AMI (Advanced Metering Infrastructure)

Napredni merni sistemi (AMI) predstavljaju tehnološki okvir koji povezuje pametna brojila, komunikacione mreže i centralne sisteme za upravljanje podacima. Za razliku od osnovnih AMR rešenja, AMI omogućava dvosmernu komunikaciju, dinamičko tarifiranje, detekciju kvarova i aktivno učešće potrošača, čime postaje ključni stub razvoja pametnih mreža. Njegova arhitektura obuhvata brojila, komunikacione kanale, koncentratore, HES i MDMS platforme koje obezbeđuju prikupljanje, obradu i distribuciju podataka. Zahvaljujući naprednoj analitici i mogućnosti integracije sa drugim sistemima, AMI doprinosi efikasnijem upravljanju mrežom, većoj pouzdanosti i energetskoj održivosti.

3.5. SmartGrid

Pametne elektroenergetske mreže (Smart Grid) predstavljaju evoluciju tradicionalnih sistema kroz primenu informacionih i komunikacionih tehnologija koje omogućavaju dvosmernu razmenu energije i podataka,

automatizaciju i integraciju obnovljivih izvora. Njihove ključne osobine su realno-vremensko praćenje, decentralizovano upravljanje, fleksibilna potrošnja i aktivna uloga korisnika-prosumera. Arhitektura Smart Grid-a obuhvata merni sloj sa pametnim brojilima i senzorima, komunikacione mreže, SCADA/DMS/EMS sisteme, analitičke alate zasnovane na AI i Big Data tehnologijama, kao i interakciju sa korisnicima kroz pametne domove, EV punjače i mikro-mreže.

U ovom okviru, AMI sistemi i pametna brojila čine temelj digitalizacije, omogućavajući prikupljanje podataka, detekciju kvarova, dinamičko tarifiranje i povezivanje distribuiranih izvora. Iako Smart Grid donosi bezbednosne i tehničke izazove - poput cyber napada, skalabilnosti i obrade ogromnih količina podataka - njegovi benefiti su dalekosežni: veća efikasnost, smanjene emisije, podrška elektromobilnosti i razvoj novih tržišnih modela. Budući trendovi uključuju primenu veštačke inteligencije, blockchain tehnologije i kvantno otporne bezbednosti, što će mrežu učiniti prediktivnom, fleksibilnom i otpornom na buduće izazove.

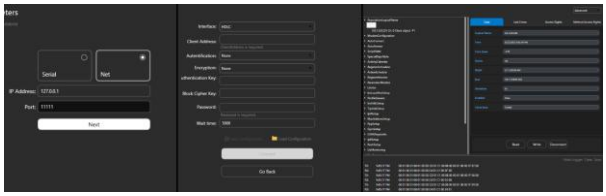
4. Primer DLMS desktop aplikacije za radnike elektrodistribucije

DLMS desktop aplikacija razvijena je u **WPF okruženju**, C# (.NET) programskog jezika, uz primenu **MVVM (Model–View–ViewModel)** arhitektonskog obrasca, što obezbeđuje jasnu separaciju logike, prezentacije i podataka, lakše održavanje koda i jednostavnije proširivanje funkcionalnosti. Namenjena je radnicima elektrodistribucije na terenu i u centrali, kao alat za dijagnostiku, konfiguraciju i otklanjanje kvarova na pametnim brojilima.

Komunikacija sa uređajima uspostavlja se preko serijske ili TCP konekcije, korišćenjem **DLMS poruka** definisanih prema **COSEM standardu (IEC 62056)**. Nakon odabira komunikacionog medijuma, korisnik definiše parametre povezivanja: u slučaju serijske komunikacije bira odgovarajući COM port (USB port na računaru na koji je povezan optički kabl ili RS485), dok se u slučaju mrežne (TCP/IP) komunikacije unose IP adresa i broj porta preko kojih se ostvaruje veza.

Slika 4. *Optički port na DLMS brojilu*

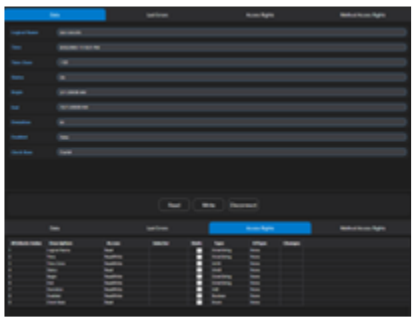
Nakon odabira komunikacionog medijuma definišu se odgovarajući konekcioni parametri uređaja, čime se stvaraju uslovi za uspostavljanje komunikacione veze. Nakon razmene poruka za uspostavljanje konekcije i uspostavljene konekcije, aktivira se mehanizam održavanja veze (***heartbeat***), koji obezbeđuje kontinuiranu razmenu podataka sve do eksplicitnog prekida sesije (održava se konekcija da ne bi doslo do connection timeout).



Slika 5. *Korisnički interfejs aplikacije*

Prvi korak interakcije sa brojilom nakon uspostavljanja konekcije podrazumeva čitanje **asocijacije** - kompletnog skupa konfiguracionih podataka koji obuhvata registre i funkcije uređaja. Proces se realizuje ***Read*** operacijom nad standardizovanim **OBIS kodovima**, pri čemu se dobijeni DLMS podaci transformišu u **XML objekte**, usklađene sa COSEM modelom. XML objekti se zatim parsiraju u okviru aplikacije i organizuju prema atributu **ObjectType**, čime se COSEM objekti grupišu u funkcionalne kategorije. Objekti istog tipa poseduju (po COSEM) identične metode i atribute, što omogućava standardizovan i pregledan rad. U korisničkom interfejsu podaci su vizualizovani kroz **Tree strukturu**, koja omogućava intuitivnu navigaciju kroz registre, pregled i izmenu atributa, kao i izvršavanje ***read/write*** operacija. Dodatno, aplikacija sadrži tab sa kompletnim pregledom registara i podešavanjima, gde se mogu videti sva polja registra i metode. Na dnu interfejsa nalazi se **log prozor**, gde se u realnom vremenu prikazuju sve razmenjene DLMS poruka prilikom isčitavanja datog registra.

Jedna od osnovnih funkcionalnosti pametnih brojila jeste ***Clock registar***, koji prema COSEM standardu sadrži vreme, vremensku zonu, status, podešavanja letnjeg računanja vremena i ***clock base***. Važno je da ovaj registar bude sinhronizovan, jer svako brojilo funkcioniše kao eksterni servis i tačni vremenski podaci su ključni za određivanje trenutka alarma, očitavanja i drugih događaja. Kako kristalni oscilatori imaju odstupanje od nekoliko sekundi mesečno, periodična sinhronizacija sata obezbeđuje preciznost i pouzdanost sistema.



Slika 6. *Clock registar*

Kako je pametno brojilo mrežni uređaj, ono uobičajeno poseduje GPRS modul sa SIM karticom, dok se parametri mreže, poput APN-a, definišu u GPRS Setup registru. U IPv4 i IPv6 registrima prikazuju se mrežni parametri

uređaja, kao što su IP adresa, maska podmreže i drugi relevantni podaci.

Slika 7. *IPv4 registar*

Sve merenje sa senzora (npr. trenutni napon, jačina struje, potrošnja) u skladu sa COSEM standardom čuva se u registrima tipa **Register**. Pored numeričke vrednosti, **Register** sadrži polja **Unit** i **Scaler**, pri čemu se realna vrednost dobija primenom faktora 10^{scaler} i dodeljivanjem jedinice. Jednostavno čitanje podrazumeva slanje READ zahteva na odgovarajući **OBIS kod** (adresa registra) i atribut, a zatim parsiranje DLMS odgovora u objekat Register (vrednost + scaler + unit → odgovarajući C# tip).

Slika 8. *Register frekvencije struje i trenutnog napona*

S obzirom na to da svaki atribut u COSEM standardu ima definisan svoj tip, aplikacija vrši mapiranje tih tipova u odgovarajuće C# tipove radi pravilne interpretacije i obrade podataka.

Tabela 1. *Mapa mapiranja COSEM tipova u C# tipove*

COSEM tip	.NET/C# tip
Int8 / Int16 / Int32 / Int64	sbyte / short / int / long
Float32 / Float64	float / double
OctetString	byte[]
Array	List ili List

Proces čitanja registara prikazan je na Slici 9, gde se najpre uspostavlja konekcija sa uređajem, a zatim poziva metoda read za odgovarajući OBIS kod, atribut i tip podatka. Na osnovu prosleđenog tipa unapred je poznato koji podatak treba da bude vraćen (na osnovu prethodno pomenutog mapiranja u C# tipove), dok se nakon izvršenog čitanja dobija povratna vrednost atributa datog registra.

```
public async Task<Result<T, ResponseError>> Read<T>(DlmsReader
reader, AssociationDto association)
{
   var openResult = reader.Open();
   if (openResult.IsFailure)
      return openResult.Error;

var returnItem = reader.Read(association.ObisCode,
(ObjectType)association.ObjectType,(DataType)association.DataType,
association.AttributeNo
);

   if (returnItem.IsFailure)        return returnItem.Error;

   return ret.Value;
}
```

Slika 9. *Metoda za čitanje registra*

Pored navedenih, brojilo podržava i čitav niz dodatnih registara, od kojih svaki ima svoju specifičnu ulogu u okviru kompletnog sistema.

5. ZAKLJUČAK

Savremeni elektroenergetski sistem prolazi kroz duboku transformaciju pod uticajem digitalizacije, održivosti i rastuće uloge krajnjih korisnika. U tom okviru, pametna brojila i napredni merni sistemi (AMI) čine osnovu nove energetske paradigme - omogućavajući dvosmernu komunikaciju, precizno merenje i aktivno upravljanje potrošnjom. Kao čvorišta pametnih mreža, brojila prevazilaze ulogu pasivnih uređaja i postaju ključni elementi u integraciji obnovljivih izvora i fleksibilnih tarifa. AMI obezbeđuje infrastrukturu za prenos i obradu podataka, dok Smart Grid objedinjuje sve komponente u celinu koja omogućava otporniji, efikasniji i održiv energetski sistem budućnosti.

6. LITERATURA

[1] EC 62056 - DLMS/COSEM suite: Electricity metering data exchange. International Electrotechnical Commission.

[2] DLMS User Association, Blue Book, Edition 17. Geneva, 2025.

[3] DLMS User Association, Green Book, Edition 12. Geneva, 2025.

[4] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. National Institute of Standards and Technology, 2021.

Kratka biografija:

Stefan Popović rođen je u Šapcu 2000. godine. Osnovne studije Primenjenog softverskog inženjerstva završio je na Fakultetu tehničkih nauka.kontakt: stefan.popowic00@gmail.com

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/34BE04Gligorov

ARHITEKTURA BEZBEDNOG DIGITALNOG NOVČANIKA SA VIŠESTRUKIM POTPISIMA

ARCHITECTURE OF A SECURE MULTI-SIGNATURE WALLET

Nevena Gligorov, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu će biti analizirana arhitektura bezbednih digitalnih novčanika, sa glavnim naglaskom na novčanike sa višestrukim potpisima. Rad uključuje i predlog arhitekture digitalnog novčanika sa višestrukim potpisima u sistemima elektronskog plaćanja.*

Ključne reči: *digitalni novčanik, e-novčanik, digitalni novčanik sa višestrukim potpisom, arhitektura, bezbednost*

Abstract – *This paper will present an analysis of the architecture of secure digital wallets, with the main focus on multisignature digital wallets. The paper also includes a proposal for an architecture of a secure multisignature digital wallet that could be used in electornic payment systems.*

Keywords: *digital wallet, e-wallet, multi-signature digital wallet, architecture, security*

1. UVOD

Trgovina je evoluirala od razmene materijalnih dobara i zlatnika do savremenih digitalnih sistema plaćanja. *Fintech* revolucija sa sobom je donela mobilno bankarstvo koje omogućava brz i jednostavan uvid u stanje računa i izvršavanje transakcija putem mobilnog telefona. Uz to, sve veću popularnost počeli su da dobijaju sistemi elektronskog plaćanja i korišćenje kriptovaluta. Glavni zahtev ovih sistema jeste očuvanje bezbednosti visokog nivoa. U te svrhe, nastali su digitalni novčanici sa višestrukim potpisima, čija bezbednost se temelji na korišćenju podeljene odgovornosti nad sredstvima. Tehnologija se kontinuirano razvija, a sa njom i sistemi plaćanja koji zajedno sa digitalnim novčanicima tek treba da dostignu svoj vrhunac upotrebe [1, 2].

2. TEORIJSKE OSNOVE I KORIŠĆENE TEHNOLOGIJE

2.1. Platni instrument

Platni instrument predstavlja skup informacija koje opisuju neku ekonomsku vrednost, a koji je potreban odgovarajućem protokolu radi izvršavanja transakcije elektornskog plaćanja.

2.2. Elektronski novac

Elektronski novac je novac koji može (npr. evro), ali i ne mora (npr. kriptovalute) imati svoju fizičku reprezentaciju, a čija je osnovna namena korišćenje u sistemima elektronskog plaćanja, u okviru kog i omogućava sam proces plaćanja.

Kirptovaluta je ime dato sistemu koji koristi kriptografiju kako bi se proces slanja podataka izvršio na siguran način. Pored toga, sistem takođe koristi kriptografiju radi distribucije digitalnih tokena u raštrkanom maniru [3].

Kako bi mogao da se koristi u sistemima elektronskog plaćanja, elektronski novac mora biti: univerzalno prihvaćen, transferabilan, deljiv, takav da ga je nemoguće falsifikovati ili ukloniti bez odgovarajuće autorizacije, privatan (niko sem korisnika koji učestvuje u transakciji nema uvid u njenu vrednost), anoniman (korisnik koji vrši plaćanje se ne može identifikovati) i takav da se valuta može koristiti i kada sistem nema pristup *Internet* mreži, odnosno, da ne zahteva *online* verifikaciju [4].

2.3. *Blokčejn*

Blokčejn predstavlja javni zapisnik (engl. *public ledger*) svih izvršenih transakcija. Sastoji se iz blokova, gde svaki blok iz mreže referencira na heš vrednost svog bloka prethodnika (roditeljskog bloka). Blok se sastoji od tela, u okviru kojeg se nalaze transakcije i njihov brojač, ali i zaglavlja koje sadrži: verziju bloka, heš vrednost roditeljskog bloka, heš vrednost korena Merkleovog stabla, vreme, *nBits* i *Nonce*.

Osnovna karakteristika *Blokčejn* mreže jeste da je ona decentralizovana, perzistentna, anonimna i da ima mogućnost revizije. Razlog zbog kojeg se mreža pokazala dobro u okviru decentralizovanih sistema je zato što koristi heš funkciju za enkriptovanje, digitalni potpis zasnovan na asimetričnoj kriptografiji, kojim se vrši potvrda identiteta i konzenus protokol.

Blokčejn mreže omogućavaju realizaciju elektronskog plaćanja bez potrebe za postojanjem posrednika, poput banaka kod kartičnog plaćanja, čime se povećava efikasnost i smanjuje cena izvršavanja čitavog procesa plaćanja [5].

2.4. Sistemi elektronskog plaćanja

Sistem elektronskog plaćanja obuhvata sve transakcije, odnosno, plaćanja izvršena elektronskim putem. Danas, jedan od veoma popularnih načina kupovine jeste *online*

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, vanr. prof.

kupovina, koja je realizovana upravo upotrebom ovog sistema, a uz pomoć koje krajnji korisnik uživa u pogodnostima kupovine iz svog doma.

Svaki sistem elektornskog plaćanja koji nudi različite opcije za izvršavanje procesa kupovine, mora ispunjavati stroge kriterijume upotrebljivostio, prihvaljivosti, skalabilnosti, interoperabilnosti, dostupnosti i bezbednosti.

Kao jedno od večito aktuelnih tema, pitanju bezbednosti se i kod tradicionalnih i kod elektronskih sistema plaćanja mora pristupiti veoma ozbiljno. Bezbednost se može posmatrati kao niz zahteva koje je potrebno ispuniti, poput: prevencije od prevare, poverljivosti i otpornosti na greške. Krajnji korisnik, odnosno, njegove lične informacije i sredstva u novčaniku u svakom momentu moraju biti zaštićeni, tako da ne postoji nijedan način kojim bi se napadači mogli koristiti da se tih istih sredstava, odnosno, informacija dokopaju. Takođe, ukoliko dođe do iznenadnog pada sistema, to ni na koji način ne sme uticati na korisnika. Kako su sve transakcije koje se izvršavaju atomične, u ovom slučaju bi to značilo prosto poništavanje svi do tada izvršenih koraka, čime se rezervisani deo korisnikovih sredstava ne gubi [6].

Postoji jako puno različitih tehnologija i načina koji se mogu koristiti za implementaciju jednog digitalnog novčanika. U ovom radu, iako je glavni fokus na digitalnim novčanicima sa višestrukim potpisima, ukratko će biti i opisana ideja integracije standardnog digitalnog novčanika u okviru mobilnog telefona, čiji rad se zasniva na upotrebi *NFC* i *NDEF* tehnologija u okviru *Android* operativnog sistema, kao što je opisano u radu [4]. S druge strane, moguće je kreirati interoperabilni digitalni novčanik opisan u [7] koji se zasniva na korišćenju *IFPS*, *SHA256* i *blokčejn* tehnologija.

Poput *Electrum* digitalnog novčanika [8] moguće je koristiti *Python*, P*yQt6*, *Kivy*, *libsecp256k1* i *QML* kako bi se realizovao novčanik koji podržava i jednostruke i višestruke potpise. Pored njega, sličnu podršku daju i *Sparrow Wallet* [9], koji za svoju implementaciju koristi *PSBT, Java (JDK 17+), JavaFX, HWI*, *Drongo, OpenPNP, Hummingbird, Lark, DuckDB secp256k1* i *ZBar*, i *Safe Smart Account* [10] koji se bazira na korišćenju *TypeScript*, *Solidity*, *Python* i pametnih ugovora.

U [11] se predlaže implementacija digitalnog novčanika sa višestrukim potpisima kojim se upotrebom *Bloom* filtera, *T-ECDSA* algoritma i *Multi-praty ECDSA* postiže viši nivo bezbednost, uz očuvanje performansi standardnih digitalnih novčanika.

3. ANALIZA BEZBEDNOG DIGITALNOG NOVČANIKA SA VIŠESTRUKIM POTPISIMA

Digitalni novčanik predstavlja servis namenjen elektronskom plaćanju koji izdaje izdavalac (engl. *issuer*) koji je nezavisan od bilo koje transakcije. Sadrži podatke o platnom instrumentu, kao i sva sredstva neophodna za izvršavanje online transakcija. Bez obzira da li je reč o digitalnim novčanicima sa jednim ili više potpisa, kako bi se ostvarila brza i efikasna transakciona komunikacija, novčanik mora biti: proširiv, simetričan, ne čisto *web* namenjen, klijentski orijentisan i pre svega, bezbedan. Arhitektura većine gotovih rešenja koja se danas koriste ne podržava svaku od prethodno navedenih stavki, jer bi takva implementacija bila veoma zahteva, zbog čega se često pravi kompromis u implementiranim i neimplementiranim delovima [3].

3.1. Digitalni novčanik sa jednim potpisom

Digitalni novčanik sa jednim potpisom je najčešće korišćeni tip digitalnih novčanika. Kontrola nad sredstvima u celosti zavisi samo od jednog korisnika, zbog čega je omogućena direktna i jednostavna kontrola nad digitalnom imovinom.

3.1.1. Digitalni novčanik integrisan u mobilni telefon

[4] predlaže kreiranje mobilne aplikacije koja bi predstavlja sistem elektrosnkog plaćanja u kom bi digitalni novčanik bio njegov sastavni deo. Korišćenjem *NFC* tehnologije moguće je izvršiti transfer novca iz jednog u drugi novčanik. Komunikacija, koja se još i naziva procesom zračenja, vrši se razmenom poruka uz pomoć *NDEF* tehnologije. Svaka poruka se sastoji od: količine novca koji se šalje, sertifikata valute (koristi se kao mehanizam bezbednosti uz pomoć kog se proverava validnost novca koji se transferuje, a u okviru ovog pristupa se smatra da svaka valuta ima svoj digitalni sertifikat), korisnika koji transferuje sredstva, korisnika koji prima sredstva i datum izvršavanja plaćanja.

Prednosti ovog pristupa su što, ukoliko primenjeno na veliki broj korisnika, ne postoji potreba za nošenjem fizičkog novčanika uz mobilni telefon, jer će se u okviru prenosnog uređaja nalaziti sve što je jednom korisniku potrebno. S druge strane, to je i jedna od glavnih mana, jer u slučaju gubitka mobilnog telefona, to efektivno znači i gubitak svih sredstava digitalnog novčanika.

3.1.2. Digitalni novčanik zasnovan na blokčejn tehnologiji

Moguće je kreirati standardni digitalni novčanik koji se zasniva na korišćenju *blokčejn* tehnologije, kao što je opisano u [7]. Arhitektura ovog pristupa se zasniva na korišćenju *miner* komponenti za svaku od banaka sistema, prilikom čega one predstavljaju računarski server vrhunskih performansi. Ideja je da svaka banka svojim klijentima izda digitalni novčanik, poput kartica koje se danas koriste, prilikom čega bi taj novčanik sadržao adrese svih *miner* komponenti sistema, ali i svoj privatni i javni ključ koji su mu potrebni za potpisivanje, odnosno, validaciju digitalnih potpisa. Banke sistema veruju jedna drugoj i koriste *POS* konsenzus protokol radi dogovaranja oko jedne verzije istine.

Prilikom plaćanja, kreira se transakcija koja sadrži količinu sredstava potrebnu za plaćanje, kao i digitalni potpis korisnika koji izvršava datu akciju, a koji je kreiran njegovim privatnim ključem. *Miner* komponente prihvataju tu transakciju, beleže je i nakon toga prebacuju novac iz bankovnog računa korisnika u njegov digitalni novčanik, prilikom čega se vrši provera da li korisnik uopšte ima dovoljno sredstava za izvršavanje transakcije. Ukoliko ima, *miner* komponente kreiraju još jednu transakciju koja simbolizuje prebacivanje sredstava, a koju sve ostale *miner* komponente beleže. Vrši se transfer sredstava iz jednog u drugi novčanik, gde je poslednji korak prebacivanje tih sredstava iz novčanika na račun primaoca.

Osnovna mana ovih novčanika jeste što imaju jednu glavnu kritičnu tačku, a to je korišćenje jednog privatnog ključa. U slučaju njegovog gubitka ili krađe od strane hakera, sva sredstva koja se nalaze u digitalnom novčaniku se nepovratno gube.

3.2. Digitalni novčanik sa višestrukim potpisima

Digitalni novčanici sa višestrukim potpisima nude rešenje problema bezbednosti, u okviru kog se realizuje deljena odgovornost nad sredstvima novčanika, odnosno, vrši se generisanje više različitih parova privatni/javni ključ koji se dodeljuju svakom od korisnika koji su vlasnici novčanika. Ovim putem se rešava slabost jedne kritične tačke standardnih digitalnih novčanika. Veoma je teško doći do jednog privatnog ključa, što postaje eksponencijalno teže sa porastom njihovog broja. Međutim, najveća mana ovog pristupa je što većina postojećih rešenja zahteva izmene u protokolima koji se koriste, ili čak i upotrebu pametnih ugovora, što utiče na performanse čitavog sistema [11].

3.3. Postojeća rešenja

3.3.1. *Electrum*

Electrum je manje zahtevna (engl. *lightweight*) verzija *Bitcoin* digitalnog novčanika, koju je 2011. godine kreirala i objavila kompanija *Electrum Technologies GmbH* [12]. Podržava kreiranje i korišćenje standardnih digitalnih novčanika, ali i novčanika sa višestrukim potpisima.

Kreira i održava desetak konekcija ka serverima, od kojih se samo jedan koristi kao glavni, dok ostali služe za dobijanje informacija vezanih za transakcione naknade. Glavni server se koristi za praćenje aktivnosti vezanih za deljene novčanike, kao i uvrštavanje transakcije u *blokčejn* mrežu.

Svaki od korisnika dobija svoj par privatnog i javnog ključa, prilikom čega se privatni ključ generiše na osnovu slučajno generisane fraze. Da bi transakcija bila odobreno, prilikom kreiranja novčanika definiše se *n* korisnika koji će deliti sredstva, od kojih je samo *m* potrebno da digitalno potpiše transakciju kako bi se ona smatra odobrenom [8].

Arhitekturu ovog novčanika je moguće ugrubo podeliti na pet modula: prezentacioni, aplikacioni, biznis logiku, mrežni i *Bitcoin* mrežni modul. Prezentacioni modul sadrži sva podešavanja neophodna za korišćenje desktop aplikacije kojom se novčanik reprezentuje, dok se u aplikacionom modulu nalazi glavna logika. Mrežni modul je namenjen održavanju konekcije sa *Electrum* serverima, dok se *Bitcoin* mrežni modul koristi za komunikaciju *Electrum* novčanika sa *bitcoin* mrežom [13].

3.3.2. *Sparrow wallet*

Sparrow wallet je desktop aplikacija koja predstavlja *Bitcoin* novčanik koji je podržan na većini hardverskih novčanika. Bazira se na korišćenju popularnih standarda poput *PBST*, pri čemu je akcenat stavljen na transparentnosti i upotrebljivosti novčanika [14].

Podržava dva režima rada: sa i bez pristupa mreži, kao i konekciju na tri različita tipa servera: javni server, *Bitcoin Core* čvor i privatni *Electrum* server. Ovi server nude različite nivoe bezbednosti i kompleksnosti, pa su iz tog razloga i namenjeni različitim tipovima korisnika.

Podržava kreiranje digitalnih novčanika sa višestrukim potpisima, prilikom čega se svakom od *n* korisnika kreira novčanik sa privatnim i javnim ključem, a za odobravanje transakcije potrebno i dovoljno je usaglašavanje samo *m* korisnika [9].

Na osnovu otvorenog koda ovog digitalnog novčanika [14] moguće je definisati njegovu arhitekturu, koja se sastoji iz: prezentacionog i aplikacionog sloja, sloja *Drongo* biblioteke, skladišta, mrežnog sloja, hardverskog sloja i niza eksternih zavisnosti, potrebnih za funkcioniasnje čitavog sistema.

Upravljanje novčanicima, transakcijama i svim događajima vrši aplikacioni sloj, a za potrebe enkapsulacije logike *Bitcoin* protokola se koristi *Drongo* biblioteka [15].

3.3.3. Digitalni novčanik sa višestrukim potpisima i *Bloom* filterom

Potrebno je dizajnirati digitalni novčanik sa višestrukim potpisima koji unapređuje aspekt bezbednosti standardnih digitalnih novčanika, ali ne na račun performansi, kao što to obično biva kog novčanika sa višestrukim potpisima. U te svrhe, predložen je novčanik [11] koji vrši rekonstrukciju višestrukih potpisa, tako da se od njih kreira jedan digitalni potpis koji *blokčejn* mreža može brzo proveriti. Na ovakav način se višestrukim digitalnim potpisima postiže očuvanje povećane bezbednosti koju imaju digitalni novčanici višestrukih potpisa, ali se njihovom rekonstrukcijom obezbeđuje očuvanje performansi sistema.

Rekonstrukcija digitalnih potpisa se postiže korišćenjem algoritma digitalnih potpisa zasnovanim na korišćenju praga eliptične krive *T-ECDSA*. Provera validnosti dobijenog potpisa omogućena je upotrebom *Bloom* filtera koji se šalje u okviru transakcije umesto svih javnih ključeva korisnika. Osim što zauzima manje prostora nego javni ključevi, ovaj filter eliminiše nepotrebno slanje personalnih informacija putem javnog ključa. Uz pomoć *Bloom* filtera moguće je i dobiti uvid u učesnike prilikom potpisivanje transakcije.

Arhitektura ovog sistema se može podeliti na klijentsku i serversku stranu, kod koje je serverska zadužena za razmenu javnih i enkriptovanih ključeva. U okviru njega vrši se pomenuta rekonstrukcija potpisa, kao i njegova validacija. S druge strane, klijentska strana sadrži različite module za enkripciju i dekripciju, generisanje ključeva i transakcija, kao i potpisivanje, komunikaciju i validaciju.

3.3.4. *Safe Smart Account*

Safe Smart Account je digitalni račun sa integrisanim funkcionalnostima digitalnih novčanika sa višestrukim potpisima, zbog čega se često i nazivaju digitalnim novčanicima. Predstavlja jedan od vodećih primera digitalnih novčanika *Ethereum* mreže.

Na osnovu otvorenog koda [10] izvodi se zaključak da se glavna logika u radu ovog tipa novčanika zasniva na korišćenju pametnih ugovora. Arhitekturu *Safe* novčanika moguće je podeliti u nekoliko slojeva. Klijentski sloj omogućava različite načine upravljanja digitalnim računima. Glavni sloj (engl. *Core layer*) predstavlja srž arhitekture. Dizajniran je prema *proxy pattern* principu,

čija je osnovna ideja odvajanja stanja novčanika od njegove logike. Integracioni sloj omogućava proširenja funkcionalnosti sistema dodavanjem novih, ali tako da one nikako ne utiču na osnovna ponašanja čitavog sistema. Dizajniran je po principu odvojenih odgovornosti (engl. *separation of concerns*), tako da je svaka komponenta nezavisna od ostalih i od osnovnog sistema.

Poslednji sloj je *Blokčejn* sloj koji predstavlja infrastrukturu sa kojom *Safe Smart Account* komunicira, odnosno, u okviru koje vrši emitovanje i izvršavanje transakcija i ugovora sistema.

3.4. Integracija u sistem elektronskog plaćanja

U sistem elektronskog plaćanja koji korisnicima omogućava plaćanje putem kartice banke ili *QR* koda, upotrebom *PayPal* servisa ili *Ethereum* kriptovalute, moguće je integrisati digitalni novčanik sa višesturkim potpisima uz pomoć kog bi se povećala bezbednost celokupnog sistema, ali ne na račun njegovih performansi. Uz pomoć ovog novčanika bi se izbacila potreba za postojanjem dodatnih učesnika u komunikaciji, kao što to obično biva kod kartičnog plaćanja. Po uzoru na opisane novčanike, moguće je kreirati arhitekturu digitalnog novčanika sa višestrukim potpisima koji bi se bazirao na kreiranju odvojenih računa za svaki način plaćanja, a koji bi jedan modul u kome se nalazi celokupna logika. Rekonstrukcijom višestrukih potpisa, moguće je kreirati jedan potpis, za koji je potrebno odrediti odgovarajući mehanizam validacije. Time bi se omogućila bezbednost visokog nivoa, uz izbacivanje redudantne implementacije sličnih procesa obrađivanja transakcija.

4. ZAKLJUČAK

Digitalni novčanici sa višestrukim potpisima predstavljaju rešenje koje adresira probleme bezbednosti sistema elektronskih plaćanja. Oni eliminišu slabosti standardnih rešenja i omogućavaju transparentan način upravljanja sredstvima u okviru timova i organizacija.

Trenutno opisani sistem predstavlja idejno rešenje čija je dalja razrada potrebna. Nakon definisanja tehnološkog steka i implementacije svih funkcionalnosti, potrebno je izvršiti obimno testiranje i tek nakon optimizacionih korigovanja, moguće je razmatranje implementacije digitalnog novčanika u realni sistem elektronskog plaćanja.

LITERATURA

[1] M. A. Hassan and Z. Shukur, “Review of Digital Wallet Requirements,” in *2019 International Conference on Cybersecurity (ICoCSec)*, Sept. 2019, pp. 43–48. doi: 10.1109/ICoCSec47621.2019.8970996.

[2] S. Sukaris, W. Renedi, M. A. Rizqi, and B. Pristyadi, “Usage Behavior on Digital Wallet: Perspective of the Theory of Unification of Acceptance and Use of Technology Models,” *J. Phys. Conf. Ser.*, vol. 1764, no. 1, p. 012071, Feb. 2021, doi: 10.1088/1742-6596/1764/1/012071.

[3] T. Handayani and A. Novitasari, “Digital Wallet as a Transaction Media in The Community,” *IOP Conf. Ser. Mater. Sci. Engl.*, vol. 879, no. 1, p. 012001, July 2020, doi: 10.1088/1757-899X/879/1/012001.

[4] O. Dospinescu, “E-Wallet. A New Technical Approach,” *Acta Univ. Danub. Œcon.*, vol. 8, no. 5, pp. 84–94, 2012.

[5] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.

[6] A.-R. Sadeghi and M. Schneider, “Electronic Payment Systems,” in *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, E. Becker, W. Buhse, D. Günnewig, and N. Rump, Eds., Berlin, Heidelberg: Springer, 2003, pp. 113–137. doi: 10.1007/10941270_9.

[7] K. Singh, N. Singh, and D. Singh Kushwaha, “An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain,” in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, Sept. 2018, pp. 165–169. doi: 10.1109/GUCON.2018.8674919.

[8] “Welcome to the Electrum Documentation! — Electrum 4 documentation.” Accessed: Oct. 09, 2025. [Online]. Available: https://electrum.readthedocs.io/en/latest/

[9] “Documentation,” Sparrow Wallet. Accessed: Oct. 12, 2025. [Online]. Available: https://sparrowwallet.com/docs/

[10] “safe-global/safe-smart-account at release/v1.5.0,” GitHub. Accessed: Oct. 13, 2025. [Online]. Available: https://github.com/safe-global/safe-smart-account

[11] J. Han, M. Song, H. Eom, and Y. Son, “An efficient multi-signature wallet in blockchain using bloom filter,” in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, in SAC ’21. New York, NY, USA: Association for Computing Machinery, Apr. 2021, pp. 273–281. doi: 10.1145/3412841.3441910.

[12] “Electrum (software),” *Wikipedia*. Aug. 25, 2025. Accessed: Oct. 09, 2025. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Electrum_(software)&oldid=1307780521

[13] *spesmilo/electrum*. (Oct. 11, 2025). Python. spesmilo. Accessed: Oct. 11, 2025. [Online]. Available: https://github.com/spesmilo/electrum

[14] *sparrowwallet/sparrow*. (Oct. 11, 2025). Java. Sparrow Wallet. Accessed: Oct. 11, 2025. [Online]. Available: https://github.com/sparrowwallet/sparrow

[15] *sparrowwallet/drongo*. (Oct. 10, 2025). Java. Sparrow Wallet. Accessed: Oct. 13, 2025. [Online]. Available: https://github.com/sparrowwallet/drongo

Kratka biografija:

Nevena Gligorov rođena je u Kraljevu 2001. god. Diplomski rad na Fakultetu tehničkih nauka u Novom Sadu iz oblasti Elektrotehnike i računarstva – Računarstvo i automatika odbranila je 2024. god. kontakt: gligorov.nevena@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.9
ДОИ: https://doi.org/10.24867/34BE05Djuric

УПРАВЉАЊЕ ДОГАЂАЈИМА У ВЈУ.ЏЕЈ-ЕС И АНГУЛАР ФРОНТЕНД ПРОГРАМСКИМ ОКВИРИМА

EVENT HANDLING IN VUE.JS AND ANGULAR FRONTEND FRAMEWORKS

Кристина Ђурић, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У овом раду је дат опис, као и поређење управљања догађајима помоћу Ангулар и Вју.џеј-ес фронтенд програмских оквира. Догађаји у овом контексту представљају акције или промене стања у апликацији (нпр. клик мишем, унос текста, учитавање података) на које систем може да реагује. На основу истраживања како сваки од оквира управља догађајима и компарација приступа имплементацији истих функционалности у сваком од њих, изведени су закључци о предностима и манама сваке од платформи, као и о томе колико је сваки од њих погодан за коришћење.*
Кључне речи: *догађај, Вју.џеј-ес, Ангулар*

Abstract – *This paper describes and compares event management using Angular and Vue.js frontend frameworks. Based on the research of how each of the frameworks manages events and the comparison of approaches to the implementation of the same functionalities in each of them. Conclusions were drawn about the advantages and disadvantages of each of the platforms, as well as how suitable each of them is for use.*

Keywords:: *event, Vue.js, Angular*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дину Драган, ванр. проф.

1. УВОД

Основна карактеристика модерних веб апликација је њихова способност да обезбеде богат и реактиван приступ кориснику. Срж интерактивности је комплексно управљање догађајима, које подразумева како ће нека апликација реаговати на акције корисника. Ефикасност, скалабилност и једноставност развоја апликације у великој мери зависе од њеног приступа управљању догађајима [1].

С обзиром на развој и популарност савремених ЈавaСкрипт (енгл. JavaScript) фронтенд програмских оквира који су тема рада, избор одговарајуће технологије је кључан корак у планирању архитектуре апликације. Због тога је упоредна анализа њихових основних механизама, као што је управљање догађајима, од суштинског значаја за доношење праве одлуке. Иако су Вју.џеј-ес (енгл. Vue.js) и Ангулар (енгл. Angular) водећи оквири за развој динамичких корисничких интерфејса, они примењују различите механизме у управљању догађајима, што захтева детаљно истраживање.

Вју.џеј-ес је лаган и прогресиван ЈавaСкрипт фронтенд програмски оквир. Специфичности које су наглашене су једноставност, флексибилност и лакоћа усвајања. Ангулар, који је развио и одржава Гугл (енгл. Google), заснован је на ТајпСкрипту (енгл. TypeScript). Специфичности су јача типизација, модуларна архитектура, омогућава бољу организацију кода, одржавање и скалабилност апликације.

Развој веба је значајно еволуирао од класичних ЈавaСкрипт слушалаца догађаја. Данас савремени фронтенд програмски оквири нуде нове механизме који поједностављују управљање догађајима, укључујући директиве, модификаторе и обрасце комуникације између компоненти. Иако ови системи повећавају продуктивност, они уносе нове слојеве комплексности. Како у перформансама, тако и у архитектонском дизајну и искуству програмера. Постојећи извори обично пореде ове оквире уопштено, као што су перформансе, скалабилност или крива учења. Међутим, техничка анализа конкретно усмерена на механизме управљања догађајима не постоји. Овај рад има за циљ да попуни ту празнину анализом принципа и техника који постоје за управљања догађајима у фронтенд програмским оквирима Вју.џеј-ес и Ангулар.

Рад је организован на следећи начин. У другом поглављу дат је кратак осврт на појам догађаја и њихов значај у савременим фронтенд оквирима, уз објашњење основних термина. У трећем поглављу је описано на које све начине је могуће управљање догађајима у Вју.џеј-есу. У четвртом поглављу је описано на које све начине је могуће управљати догађајима у Ангулару. Пето поглавље доноси компаративну анализу ова два фронтенд програмска оквира са практичним примерима, уз сажетак предности, мана и сложености. Шесто поглавље је закључак рада.

2. УПРАВЉАЊЕ ДОГАЂАЈИМА

Догађај у веб апликацијама представља било коју интеракцију са HTML елементом – клик на дугме или линк, унос текста у поље, притисак тастера на тастатури, као и имплицитне радње попут завршетка

учитавања странице или промене величине прозора прегледача. Ови догађаји чине основу динамике и интерактивности, јер покрећу извршавање одређених функција путем обрађивача догађаја (енгл. event handler). Начин на који се управља догађајима варира у зависности од технологије која се користи. Најнижи ниво представља ЈавaСкрипт, који дефинише основне механизме рада са DOM-ом и омогућава регистровање и обраду догађаја. Зато ЈавaСкрипт чини основу на којој су изграђени фронтенд оквири Ангулар и Вју.џеј-ес. DOM је стандардизован од стране W3C/WHATWG и описује структуру HTML документа као стабло објеката. Сам DOM није део самог језика, него API који веб прегледач приказује. Фронтенд оквири додају апстракцију и лакшу синтаксу. Сама логика обраде догађаја се заснива на ЈавaСкрипту и DOM API-ју, што значи да се ниједан фронтенд оквир не удаљава потпуно од основног модела, већ практично га прилагођава својој парадигми.

2.1. Кључни појмови за лакше разумевање управљања догађајима у Вју.џеј-есу и Ангулару

ЈавaСкрипт је скрипт програмски језик који служи за изградњу динамичких и функционалних веб решења заједно са HTML-ом и CSS-ом. Пошто је реч о клијент-скрипт језику, то значи да се овај програмски језик извршава, тачније интерпретира, са стране самог веб прегледача на корисничком уређају.
ТајпСкрипт је објектно орјентисани програмски језик високог нивоа који је развио Мајкрософт (енгл. Microsoft) и он проширује ЈавaСкрипт додавањем типова. ТајпСкрипт представља надскуп ЈавaСкрипта.
Фронтенд програмски оквири је унапред написана колекција стандардизованог HTML-а, CSS-а (ЦСС – каскадни стилови) и ЈавaСкрипт кода који програмери могу да користе за ефикасније прављење веб апликација [2]. Они обухватају скуп алата, библиотека и компоненти које програмерима олакшавају имплементирање корисничког интерфејса, а то укључује дизајн, изглед, корисничко искуство, управљање догађајима, управљање стањима апликације и интеракцију са АПИ-јима. Уз помоћ фронтенд програмских оквира може се избећи писање свега од нуле, убрзавају процес развоја.

3. УПРАВЉАЊЕ ДОГАЂАЈИМА УПОТРЕБОМ ВЈУ.ЏЕЈ-ЕСА

Вју.џеј-ес представља ЈавaСкрипт фронтенд програмски оквир који омогућава лакше креирање интерактивних и реактивних веб страница. Његов творац је Еван Ју (енгл. Evan You). Према спроведеном истраживању, Вју.џеј-ес се убраја међу једноставније ЈавaСкрипт оквире. Неке од његових карактеристика су брзина, једноставан је за употребу, има веома детаљну документацију и велику заједницу.

3.1. Вју.џеј-ес директиве

Вју.џеј-ес за руковање догађајима користи директиве које се каче на DOM елементе. Главна је v-on (скраћено @) и њом се повезује догађај са обрађивачем. Обрађивач може бити инлајн, метода у компоненти или метода са прослеђеним аргументима.

3.2. Вју.џеј-ес модификатори

Модификатори догађаја проширују могућности руковања догађајима у Вју.џеј-есу, додају додатни ниво контроле. Функционишу тако што се додају постфикси као што су .stop, .prevent, .capture, .self, .once, .passive на директиве. Омогућавају прецизно и читљиво управљање понашањем без додатног кода у методама.

3.3. Прилагођени догађаји (енгл. Custom Events)

Прилагођени догађаји пружају посебан начин за руковање комуникацијом међу компонентама. Вју.џеј-ес омогућава употребу пропса за пренос података од родитеља ка детету, али за комуникацију у супротном смеру се користи емитовање догађаја, односно прилагођени догађаји. Компонента дете као одговор родитељској компоненти емитује догађај употребом $emit методе. Родитељ ослушкује те догађаје у темплејту и позива своје методе.

3.4. Управљање стањем у Вју.џеј-есу употребом Вуекса

Вјуекс је библиотека за управљање стањем у Вју.џеј-есу са централним стором (енгл. store) који је реактиван. Стање (енгл. state) стора се мења искључиво преко мутација (енгл. mutations). Мутације не садрже пословну логику, већ служе искључиво за измену стања. Акције (енгл. actions) су те које служе за које имплементирају логички део и затим позивају мутације. Мутације је могуће и директно комитовати. Гетери (енгл. getters) изводе податке из стања, а модули (енгл. modules) организују стор на мање целине.

4. УПРАВЉАЊЕ ДОГАЂАЈИМА УПОТРЕБОМ АНГУЛАРА

Ангулар је фронтенд оквир заснован на HTML-у и ТајпСкрипту за креирање интерактивних, реактивних веб апликација, са нагласком на јасну архитектуру и добру документацију. Настао је као AngularJS (2010), а потпуно је ревидиран у Angular 2 (2016) и од тада се развија као засебан, типизован оквир. Истраживање управљања догађајима у Ангулару је спроведено на темељима његове архитектуре коју чине компоненте, модули, шаблони, директиве, сервиси и Dependency Injection (DI - инјектовање зависности). Компоненте су основни градивни блокови (класе са логиком и руковаоцима догађаја повезане са HTML шаблоном), модули логички групишу функционалности, директиве мењају структуру или понашање DOM-а, док сервиси инкапсулирају пословну логику и убризгавају је путем DI ради боље организације, тестабилности и поновне употребе.

4.1. Везивање догађа (енгл. Event Binding)

Везивање догађаја омогућава ослушкивање и реаговање на догађаје стављањем имена догађаја у заграде у HTML шаблону и повезивањем са методом компоненте (нпр. *(click)="onClick($event)"*). Метод дефинише радњу која се извршава када се догађај догоди.

4.2. Прилагођени догађаји

Прилагођени догађаји у Ангулару омогућавају комуникацију између компоненти. Емитују се из компоненте дете ка родитељској компоненти помоћу EventEmitter класе и @Output() декоратора, а слање догађаја се врши преко методе EventEmitter.emit().

4.3. Управљање стањем у Вју.џеј-есу употребом ЕнЏиАрИкса (енгл. NgRx)

У Ангулару се стање може чувати локално у компонентама, што је једноставно, али се губи при навигацији и није погодно за сложеније апликације. За предвидљиво и централизовано управљање препоручује се употреба ЕнЏиАрИкса. То је библиотека која уводи стор (енгл. store) као централни репозиторијум, док се промене стања врше искључиво преко акција које обрађују редуктори (енгл. reducer), а приступ подацима преко селектора (енгл. selector). Овим се добија структуриран, контролисан и трајнији модел управљања стањем током рада апликације.

5. КОМПАРАТИВНА АНАЛИЗА

У овој секцији је кроз примере урађена компаративна анализа управљања догађајима у фронтенд програмским оквирима Вју.џеј-ес и Ангулар. Приказане су методе и механизми управљања догађајима, њихове карактеристике у погледу лакоће имплементације, читљивости и погодности за различите типове апликација.

5.1. Везивање догађаја

Вју.џеј-ес користи v-on директиву, скраћено @, што је једноставније и прегледније. Ангулар користи (event) синтаксу у темплејту која позива методу у класи, формално и дужег облика. Вју.џеј-ес пружа већу једноставност, Ангулар више формалности и конзистентности.

5.2. Модификатори догађаја

Вју.џеј-ес има уграђене модификаторе (.prevent, .stop, .once, .self, .right) који омогућавају чисту логику, без додатног кода у методама. Ангулар нема уграђене модификаторе, па је потребно ручно управљати DOM догађајима у методама и то захтева више знања о DOM API-ју, уместо да методе садрже само чисту логику. Модификатори у Вју се дефинишу заједно уз догађај, директно у шаблону, што омогућава јаснију, краћи код и лакше разумевање. Овај приступ је интуитивнији за почетнике и поједностављује комбиновање више услова. У Ангулару се иста логика мора имплементирати у методама због чега недостаје директна повезаност са самим догађајем у темплејту.

5.3. Прилагођени догађаји и комуникација родитељ–дете компоненти

У Вју компоненти дете на слици 1, унутар *methods* дефинисане су три методе које позивом *$emit* емитују догађај са подацима. Догађај *this.$emit("archive-fiesta", this.fiesta.id)* родитељ хвата преко *@archive-fiesta="archiveFiesta"*.

```
<script>
export default {
  name: "FiestaCard",
  props: {
    fiesta: Object,
  },
  methods: {
    editFiesta() {
      this.$emit("edit-fiesta", this.fiesta);
    },
    archiveFiesta() {
      this.$emit("archive-fiesta", this.fiesta.id);
    },
    deleteFiesta() {
      this.$emit("delete-fiesta", this.fiesta.id);
    },
  },
};
</script>
```

Слика 1. Компонента дете у Вју.џеј-есу

У Ангулару компонента дете емитује догађај преко декоратора *@Output()* и класе *EventEmitter<T>*. На слици 2 је приказана имплементација догађаја *@Output() archiveFiesta = new EventEmitter<any>()*. Родитељ догађај хвата преко *(archiveFiesta)= "onArchive($event)"*.

```
import { Component, EventEmitter, Input, Output } from '@angular/core';

@Component({
  selector: 'fiesta-card',
  standalone: true,
  imports: [],
  templateUrl: './fiesta-card.component.html',
  styleUrl: './fiesta-card.component.css'
})
export class FiestaCardComponent {
  @Input() fiesta!: { title:string; date: Date; venue: string; description: string };

  @Output() archiveFiesta = new EventEmitter<any>();
  @Output() deleteFiesta = new EventEmitter<any>();
  @Output() editFiesta = new EventEmitter<{ id: number, content: string }>();

  onArchive(id: number) {
    this.archiveFiesta.emit(id);
  }

  onDelete(id: number) {
    this.deleteFiesta.emit(id);
  }

  onEdit(id: number, content: string) {
    this.editFiesta.emit({ id, content });
  }
}
```

Слика 2. Компонента дете у Ангулару

Иако Вју има једноставнији и бржи начин емитовања догађаја, Ангуларов приступ са EventEmitter<T> је професионалнији и поузданији у већим системима. Разлог је јака типизација и боље контроле података. У Вју то није подразумевано понашање, већ је потребно додатно подешавање.

5.4. Управљање стањем

У већим системима прилагођени догађаји брзо постају непрегледни, па је бољи приступ да се подаци централизовано чувају и ажурирају у оквиру целе апликације. У Вју.џеј-есу то обезбеђује Вјуекс, а у Ангулару ЕнЏиАрИкс. Тригеровање догађаја у шаблону остаје исто, за Вју @click, а за Ангулар (click). Компоненте само диспечују акције (енгл. actions), док се стварне измене стања изводе у мутацијама (енгл. mutations) код Вјуекса и редукторима (енгл. reducers) код ЕнЏиАрИкса. Податке компоненте читају преко гетера (енгл. getters) у Вјуексу, односно селектора (selectors) у ЕнЏиАрИксу. Оваква организација пребацује логику измена из компоненти у централизовани стор (енгл. store), поједностављује компоненте и јасно раздваја акције од измена (мутације/редуктори). Резултат је предвидљив,

тестабилан и скалабилан ток промена, са мање логике у компонентама и јаснијим током података кроз апликацију.
Вјуекс је лакши за интеграцију у мањим и средњим апликацијама, али је проблем валидација типова, што може бити ограничење у већим системима. ЕнЏиАрИкс је постављен сложеније, али систем је стабилан, скалабилан и једноставан за тестирање, што га чини погоднијим за велике пројекте.

5.5. Општа оцена

У Вју је код краћи, једноставнији и визуелно јаснији јер је већина логике ближа темплејту, а то значи да су логика и изглед компоненте повезани, налазе се у истом фајлу. Ово омогућава брже разумевање и лакше учење, али може бити и проблем на дуже стазе када апликације нарасте. Зато се за Вју често каже да је погодан за мање апликације.
Ангулар код је обимнији и садржи више структура (класе, декораторе, типове), али зато пружа бољу организацију и лакше тестирање на нивоу система. Велика предност Ангулара је типизација података и то му је главна предност спрам Вју.
Избор између ова два фронтенд програмска оквира зависи од потреба конкретне апликације, Вју је идеалан када је приоритет једноставност и брзина, док је Ангулар погоднији за велике системе са строгим захтевима.

6. ЗАКЉУЧАК

Догађаји представљају суштински део сваке интерактивне веб апликације, омогућавајући корисницима интеракцију, комуникацију и динамичко искуство. У овом раду су анализирани програмски оквири Вју.џеј-ес и Ангулар који пружају различите начине за руковање догађајима. Акценат рада је на компарацији имплементације истих функција везаних за управљање догађајима, као и на анализи предности и недостатака оба програмска оквира у различитим контекстима употребе.
Вју.џеј-есова синтакса је једноставнија и интуитивнија, приликом читања кода лако је формирати реченице које објашњавају како се управља неким догађајем и шта он ради. Цео ток је јасно исказан у једном реду, што значајно олакшава читање и одржавање кода, као што су на пример уграђени модификатори догађаја. Сам еханизам управљања догађајима у Вју је флексибилан и брз за имплементацију у мањим и средње сложеним апликацијама. Међутим, за сваки догађај потребно је имплементирати неку комплекснију логику и ту све постаје компликованије, бар кад су у питању већи тимови и пројекти који немају стриктно дефинисана правила организације кода.
Са друге стране, Ангулар је погоднији за апликације које имају велики број интеракција, сложених догађаја и захтевну динамику корисничког интерфејса, због своје структуре и контроле над логиком апликације, као и због боље организације кода. Иако је тежи почетницима за учења и разумевање, искуснији програмери ће га лако савладати. Још неке од предности су ТајпСкрипт, што значи да се јасно дефинише тип података, подстиче архитектуру по шаблону и има ефикасан алат за рад преко командне линије.
При избору између ових оквира, важно је размотрити специфичне захтеве пројекта, величину и искуство тима, као и дугорочне циљеве одржавања и развоја [3]. На основу личног искуства стеченог радом на академским пројектима са Вју.џеј-есом и на комерцијалном пројекту са Ангуларом, може се потврдити да је Вју.џеј-ес погоднији за мање апликације и брзу имплементацију, а Ангулар за веће и сложеније апликације.
Као будући правац истраживања може се предложити проширење компаративне анализе и на друге популарне фронтенд програмске оквире као што су Риект (енгл. React), који користи модел синтетичких догађаја (енгл. Synthetic Events), као и Ванила ЈавaСкрипт (енгл. Vanilla JavaScript). На тај начин могла би се спровести анализа како сваки од њих управља догађајима и на који начин приступају DOM-у, као и перформансе свакога од њих. Када је реч о Вју.џеј-есу, била би занимљива компарација Вјуекса и Пиније (енгл. Pinia), истражити да ли Пинија заиста доноси побољшања у односу на Вјуекс.

7. ЛИТЕРАТУРА

[1] https://www.geeksforgeeks.org/blogs/introduction-to-scripting-languages/ (приступљено у септембру 2025).

[2] https://www.geeksforgeeks.org/blogs/top-front-end-frameworks/ (приступљено у септембру 2024).

[3] https://www.capitalnumbers.com/blog/state-management-front-end-development (приступљено у октобру 2024).

Кратка биографија:

Кристина Ђурић рођена је у Лозници 1998. год. Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства – Рачунарство и аутоматика одбранила је 2025.год.
Контакт:
kristinadjuriic@gmail.com

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/34BE06Ciric

RAZVOJ VIŠEPOTPISNOG DIGITALNOG NOVČANIKA NAD BLOKČEJN MREŽOM SOLANA
DEVELOPMENT OF A MULTI-SIGNATURE WALLET ON THE SOLANA BLOCKCHAIN NETWORK

Luka Ćirić, *Fakultet tehničkih nauka, Novi Sad*

OBLAST – PRIMENJENE RAČUNARSKE NAUKE I INFORMATIKA

Kratak sadržaj – *Ovaj rad predstavlja razvoj višepotpisnog digitalnog novčanika na Solana blokčejn mreži, sa fokusom na bezbednost, efikasnost i decentralizaciju. Kroz analizu arhitekture Solana mreže i implementaciju pametnih ugovora, demonstrira se kako se višepotpisni sistem može koristiti za zaštitu digitalne imovine u Web3 okruženju.*

Ključne reči: *Blokčejn, Solana, višepotpisni novčanik, decentralizacija, Web3*

Abstract – *This paper presents the development of a multi-signature digital wallet on the Solana blockchain network, focusing on security, efficiency, and decentralization. Through analysis of Solana's architecture and smart contract implementation, the paper demonstrates how multi-signature systems can be used to protect digital assets in a Web3 environment.*

Keywords: *Blockchain, Solana, multi-signature wallet, decentralization, Web3*

1. UVOD

U poslednjih nekoliko godina svedoci smo ogromnog napretka u svetu digitalnih tehnologija. Sve veći deo naših života, poslovanja i finansijskih aktivnosti preselio se na digitalni prostor. Sa tim razvojem pojavila se i potreba za novim načinima čuvanja i prenosa vrednosti na internetu bez posrednika i uz veću sigurnost. Upravo iz te potrebe nastala je blokčejn tehnologija, koja je promenila način na koji razmišljamo o poverenju, vlasništvu i decentralizaciji. Blokčejn (engl. blockchain) se najjednostavnije može opisati kao lanac blokova koji sadrže zapise o transakcijama, a koji su međusobno povezani i kriptografski zaštićeni. Za razliku od klasičnih baza podataka koje imaju centralni autoritet, blokčejn funkcioniše kao distribuirana mreža u kojoj svi učesnici imaju jednak uvid u informacije [1]. Na taj način, mogućnost zloupotrebe podataka je znatno manja, a poverenje između učesnika u sistemu ostvaruje se kroz transparentnost i verifikaciju transakcija od strane same mreže. Jedna od najpoznatijih i najrašireniji primena blokčejn tehnologije su digitalni novčanici, koji korisnicima omogućavaju da bezbedno čuvaju i koriste kriptovalute, tokene i druge digitalne vrednosti.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, red. prof.

Ipak, većina postojećih novčanika zasniva se na konceptu jednog privatnog ključa što znači da, ako se taj ključ izgubi ili kompromituje, korisnik gubi pristup svim svojim sredstvima. Da bi se ovakav rizik smanjio, razvijen je model višepotpisnih (engl. multisignature) novčanika, koji zahteva da više različitih korisnika (ili uređaja) potpiše transakciju pre nego što ona bude izvršena [2]. Na taj način postiže se dodatni nivo bezbednosti i poverenja, posebno u situacijama kada novčanik koristi više osoba ili organizacija. Tema ovog rada izabrana je upravo zbog aktuelnosti ove problematike i sve veće potrebe za bezbednim i efikasnim rešenjima u oblasti upravljanja digitalnom imovinom. Među brojnim blokčejn mrežama, Solana se istakla kao jedno od najbržih i najskalabilnijih rešenja. Zahvaljujući svom jedinstvenom mehanizmu konsenzusa nazvanom Dokaz istorije (engl. Proof of History – PoH), Solana je u stanju da obradi hiljade transakcija u sekundi, uz minimalne troškove [3][4]. Ove performanse čine je idealnom platformom za razvoj aplikacija koje zahtevaju brzinu, sigurnost i pouzdanost, upravo ono što je neophodno kod višepotpisnih novčanika. Cilj ovog rada je da istraži i prikaže proces projektovanja i razvoja višepotpisnog digitalnog novčanika na Solana mreži, uz poseban osvrt na način na koji se postiže bezbednost, efikasnost i jednostavnost korišćenja. Pored tehničkog aspekta, rad ima za cilj da doprinese boljem razumevanju mogućnosti koje Solana nudi za razvoj naprednih Web3 rešenja, kao i da ukaže na prednosti višepotpisnih sistema u zaštiti korisničke imovine.

2. POJAM BLOKČEJNA

Ideja o blokčejnu pojavila se kao odgovor na potrebu da se poverenje u digitalnom svetu zasnuje na tehnologiji, a ne na ljudskim ili institucionalnim autoritetima. Do pojave blokčejna, gotovo svi digitalni sistemi počivali su na nekoj vrsti centralizacije. Postojala je institucija, kompanija ili entitet koji je imao kontrolu nad bazom podataka i potvrdama transakcija. Takav model funkcioniše, ali ima očigledne nedostatke: mogućnost zloupotrebe podataka i potreba za poverenjem u centralni autoritet. Blokčejn je upravo odgovor na te probleme.

U najjednostavnijem smislu, blokčejn je distribuirana i decentralizovana baza podataka koja čuva zapise o transakcijama u nizu blokova koji su međusobno povezani. Svaki blok sadrži određeni broj transakcija i referencu na prethodni blok u lancu, što formira neprekidnu, hronološki uređenu strukturu podataka [1].

Kada se jednom doda u lanac, blok se više ne može menjati bez promene svih narednih blokova, što obezbeđuje visok nivo integriteta i otpornosti na manipulacije.

Ključni element koji omogućava ovaj sistem je kriptografija. Svaki blok u lancu ima svoj kriptografski potpis (heš), koji zavisi od sadržaja samog bloka i potpisa prethodnog bloka. Na taj način se stvara lanac poverenja u kojem svaka izmena podataka u bilo kom delu lanca automatski narušava sve naredne blokove.

2.1. Način funkcionisanja blokčejna

Svaka blokčejn mreža zasniva se na distribuiranoj glavnoj knjizi (engl. Distributed Ledger Technology - DLT) koju održavaju učesnici u mreži, poznati kao čvorovi (engl. nodes).

Proces potvrde transakcija obično se sprovodi kroz mehanizam konsenzusa – to je algoritam koji omogućava da se svi učesnici mreže usaglase oko trenutnog stanja baze podataka. Najpoznatiji mehanizmi konsenzusa su Dokaz posla (engl. Proof of Work - PoH), koji koristi Bitcoin mreža i Dokaz uloga (engl. Proof of Stake - PoS) koji koriste mnoge novije platforme, uključujući i Solanu [2]. Ovakvi mehanizmi omogućavaju mreži da funkcioniše bez centralnog autoriteta, jer se poverenje postiže matematičkim i kriptografskim pravilima.

2.2. Prednosti blokčejn tehnologije

Blokčejn je revolucionaran jer rešava jedan od najvažnijih problema u digitalnom svetu – problem poverenja bez posrednika. Zahvaljujući svojoj decentralizovanoj prirodi i kriptografskoj sigurnosti, blokčejn donosi niz ključnih prednosti:

Transparentnost i verifikacija – Sve transakcije na javnom blokčejnu su dostupne svima i mogu se proveriti u svakom trenutku. To omogućava visok nivo poverenja među učesnicima, jer niko ne može jednostrano menjati ili skrivati podatke.

Otpornost na manipulacije – Jednom kada se blok doda u lanac, njegovi podaci se ne mogu menjati bez saglasnosti većine učesnika u mreži. Time se postiže integritet sistema koji je gotovo nemoguće kompromitovati.

Decentralizacija – Ne postoji centralna tačka upravljanja ili kontrole. To znači da ne postoji entitet koji može jednostrano da utiče na sistem, što blokčejn čini otpornim na cenzuru i kvarove.

Sigurnost – Kriptografski algoritmi obezbeđuju da samo vlasnici odgovarajućih privatnih ključeva mogu izvršavati transakcije. Na taj način korisnici imaju potpunu kontrolu nad svojom digitalnom imovinom.

Efikasnost i automatizacija – Uvođenjem pametnih ugovora (engl. smart contracts) ili kako se drugačije zovu na Solana mreži programi (engl. programs), blokčejn omogućava da se procesi automatizuju i izvršavaju bez ljudske intervencije, čime se smanjuju troškovi i mogućnost greške.

2.3. Implementacije i primene blokčejna

Iako se blokčejn najčešće povezuje sa kriptovalutama poput Bitcoin i Ethereum, njegova primena je mnogo šira i raznovrsnija. Danas se blokčejn koristi u brojnim oblastima koje zahtevaju poverenje, transparentnost i verifikaciju podataka.

Finansijski sektor – Najveći broj implementacija vezan je upravo za finansije. Pored kriptovaluta, blokčejn se koristi za decentralizovane finansije (DeFi), koje omogućavaju korisnicima da pozajmljuju, ulažu i trguju digitalnom imovinom bez banaka i posrednika [5].

Lanci snabdevanja – U oblasti logistike i trgovine, blokčejn omogućava praćenje porekla i kretanja proizvoda od proizvođača do krajnjeg kupca. Time se smanjuju prevare i povećava transparentnost u globalnim lancima snabdevanja.

Zdravstvo – Medicinski podaci pacijenata mogu se čuvati na blokčejnu na bezbedan i transparentan način, uz potpunu kontrolu korisnika nad pristupom tim podacima.

Digitalni identitet – Blokčejn omogućava razvoj sistema za decentralizovani identitet (DID), gde korisnici sami upravljaju svojim identitetima bez potrebe za centralizovanim bazama podataka.

Upravljanje i glasanje – Neke zemlje i organizacije eksperimentišu sa blokčejn sistemima za elektronsko glasanje, kako bi se osigurala verodostojnost rezultata i sprečile manipulacije.

Umetnost i vlasništvo – Sa pojavom NFT (engl. Non-Fungible Token), umetnici i kreatori sadržaja mogu dokazati vlasništvo nad digitalnim delima i ostvarivati prihode bez posrednika.

3. ARHITEKTURA ČVORA I IZVRŠAVANJE MREŽE

Solana blokčejn mreža predstavlja jedno od najnaprednijih rešenja u domenu decentralizovanih sistema, zahvaljujući svojoj visoko optimizovanoj arhitekturi čvorova i inovativnim mehanizmima konsenzusa. U kontekstu razvoja višepotpisnih digitalnih novčanika, razumevanje unutrašnje strukture mreže i načina obrade transakcija od suštinskog je značaja za postizanje sigurnosti, pouzdanosti i skalabilnosti.

3.1. Struktura čvorova i distribuirana verifikacija

U Solana mreži, čvorovi (nodes) funkcionišu kao temelj decentralizacije. Svaki čvor poseduje kopiju blokčejna i učestvuje u validaciji transakcija. Posebno važni su validator čvorovi, koji formiraju nove blokove i obezbeđuju integritet mreže. Arhitektura čvora u Solani je projektovana za horizontalno skaliranje, što omogućava obradu hiljada transakcija u sekundi bez kompromisa po pitanju sigurnosti.

Solana koristi kombinaciju konsenzus mehanizama: Proof of Stake (PoS) i Proof of History (PoH). PoH omogućava vremensko redosledno obeležavanje događaja bez potrebe za sinhronizacijom među čvorovima, čime se značajno ubrzava obrada transakcija. Ova kombinacija omogućava

mreži da postigne izuzetno nisku latenciju i visoku propusnost.

3.2. Ključne komponente arhitekture

Arhitektura Solana čvora obuhvata niz specijalizovanih modula:

Gulf Stream: mehanizam za prosleđivanje transakcija unapred, čime se rasterećuju čvorovi i ubrzava validacija.

Turbine: protokol za distribuciju podataka u mreži, zasnovan na strukturi stabla, koji omogućava efikasno širenje informacija.

TPU (Transaction Processing Unit): jedinica zadužena za obradu transakcija, optimizovana za paralelno izvršavanje.

TVU (Transaction Validation Unit): komponenta koja verifikuje transakcije pre nego što se dodaju u blok.

PoH lanac: vremenski niz koji obezbeđuje deterministički redosled događaja.

Ove komponente zajedno omogućavaju mreži da funkcioniše sa izuzetnom efikasnošću, što je ključno za aplikacije koje zahtevaju visoku dostupnost i brzinu, poput višepotpisnih novčanika.

3.3. Model naloga i sigurnosna infrastruktura

Solana koristi model naloga zasnovan na strukturi ključ-vrednost u okviru AccountDB baze. Postoje dve vrste naloga: korisnički (user accounts) i programski (program accounts). Programske adrese se generišu pomoću PDA (Program Derived Address), što omogućava determinističko kreiranje sigurnih adresa koje ne zahtevaju privatne ključeve.

4. REŠENJE

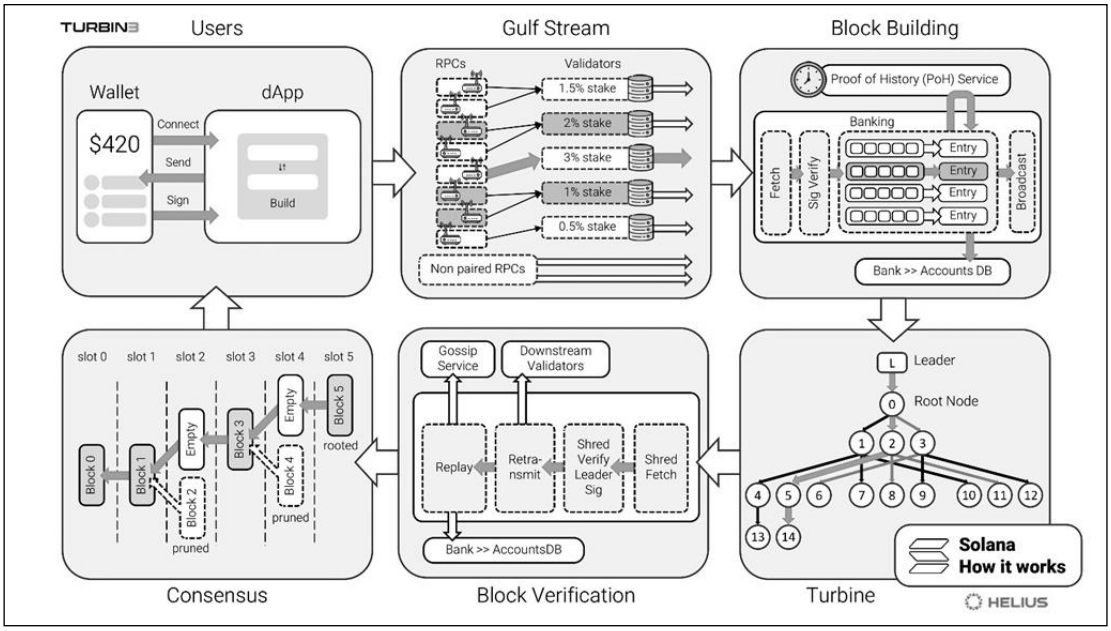
Implementacija višepotpisnog digitalnog novčanika na Solana mreži zasniva se na korišćenju Rust programskog jezika i Solana programskog okruženja. Rešenje je razvijeno kao programski modul koji omogućava kreiranje, upravljanje i izvršavanje transakcija koje zahtevaju više potpisa. Arhitektura sistema obuhvata jasno definisane funkcionalne komponente za inicijalizaciju novčanika, predlaganje transakcija i njihovo izvršavanje, uz podršku za konfiguraciju broja potpisnika i potrebnog praga.

Za razvoj su korišćeni standardni alati iz Solana ekosistema, uključujući *Anchor framework* za pojednostavljenu izradu pametnih ugovora, kao i *CLI* interfejs za testiranje i deployment. Projektna struktura organizovana je u više datoteka koje pokrivaju definiciju naloga, greške, konstante i funkcionalnosti za upravljanje novčanikom. Svaka funkcionalna jedinica je modularno implementirana i povezana kroz interni API programa.

Proces inicijalizacije novčanika podrazumeva kreiranje programskog naloga sa definisanim brojem potpisnika i pragom potrebnim za autorizaciju transakcija. Predlaganje transakcije uključuje evidentiranje predloga u okviru novčanika, dok se izvršenje vrši tek nakon što dovoljan broj potpisnika potvrdi predlog. Ova logika omogućava višeslojnu kontrolu pristupa i sprečava neautorizovano raspolaganje sredstvima.

Testiranje rešenja obavljeno je lokalno uz pomoć Solana testnet mreže, pri čemu su simulirane različite situacije — od inicijalizacije novčanika do izvršavanja transakcija sa nepotpunim brojem potpisa. Poseban fokus stavljen je na proveru sigurnosnih aspekata, kao što su validacija ulaznih podataka i zaštita od neovlašćenih poziva. Deployment je realizovan kroz *CLI* alatke, uz generisanje *IDL* fajla za dalju integraciju.

Rešenje je projektovano tako da bude proširivo i prilagodljivo za različite scenarije korišćenja, uključujući organizacione novčanike, DAO strukture i zajedničke fondove. Modularna arhitektura omogućava jednostavno dodavanje novih funkcionalnosti, dok korišćenje Solana mreže obezbeđuje visoku brzinu i niske troškove transakcija. Time se postiže balans između sigurnosti, efikasnosti i korisničke pristupačnosti u upravljanju digitalnom imovinom.



Slika 1. *Izvršavanje transakcije [6]*

5. ZAKLJUČAK

Razvoj višepotpisnog digitalnog novčanika na Solana mreži pokazao je kako se savremene blokčejn tehnologije mogu iskoristiti za unapređenje bezbednosti i pouzdanosti u upravljanju digitalnom imovinom. Kroz analizu arhitekture Solane, njenog jedinstvenog mehanizma konsenzusa i performansi, potvrđeno je da ova mreža predstavlja pogodno okruženje za implementaciju rešenja koja zahtevaju veliku brzinu obrade i niske troškove transakcija.

Implementacija višepotpisnog novčanika demonstrirala je praktične mogućnosti korišćenja programa u cilju postizanja višeg nivoa sigurnosti, jer se odluke o transakcijama ne oslanjaju na jednog korisnika, već na kolektivnu potvrdu više potpisnika. Time se značajno smanjuje rizik od kompromitovanja privatnih ključeva i gubitka sredstava, što je jedan od ključnih izazova u svetu digitalnih novčanika.

Pored tehničkog aspekta, ovaj rad ukazuje i na šire implikacije višepotpisnih sistema, od njihove primene u porodičnim i poslovnim finansijama, do uloge u decentralizovanim autonomnim organizacijama (DAO). Time se potvrđuje da višepotpisni modeli nisu samo tehničko rešenje, već i važan korak ka većem poverenju i decentralizaciji u digitalnoj ekonomiji.

Zaključno, rad potvrđuje da kombinacija Solanine arhitekture i višepotpisnog modela predstavlja snažan temelj za razvoj sigurnih i efikasnih Web3 aplikacija, čime se otvara prostor za dalji napredak u oblasti digitalnih finansija i decentralizovanih sistema.

LITERATURA

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. (Poslednji pristup: 19.10.2025) https://bitcoin.org/bitcoin.pdf

[2] A. M., & Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

[3] Yakovenko, A. (2020). Solana: A New Architecture for a High Performance Blockchain. [Online]. (Poslednji pristup: 19.10.2025) https://solana.com/solana-whitepaper.pdf

[4] Solana Foundation. (2023). Solana Documentation. [Online]. (Poslednji pristup: 19.10.2025) https://docs.solana.com

[5] Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review.

[6] Helius (2024). Solana Executive Overview. [Online]. (Poslednji pristup: 19.10.2025) https://www.helius.dev/blog/solana-executive-overview

Kratka biografija:

Luka Ćirić rođen je u Šapcu 2000. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Primenjeno softversko inženjerstvo odbranio je 2023.god. Nakon osnovnih strudija upisuje master studije na smeru Računarstvo i automatika, modul Računarstvo visokih performansi.
kontakt: ciric.e218.2023@uns.ac.rs

УДК: 621.31
ДОИ: https://doi.org/10.24867/34BE07Radovic

РХЕ: ПРОРАЧУНИ КРАТКИХ СПОЈЕВА – ЕВРОПСКА ПРАКСА И ПРИМЕНА

PSPP: SHORT CIRCUIT CALCULATION – EUROPEAN PRACTICE AND APPLICATION

Стефан Радовић, Факултет техничких наука, Нови Сад

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Припрема прикључења реверзибилне хидроелектране (РХЕ) у електроенергетски систем (ЕЕС), уз поштовање европских пракси и норми, представља основну тему овог рада. У ту сврху, за разне режиме рада РХЕ, анализиране су вредности струје кратког споја и расподеле напона. На основу добијених резултата, одабрана је адекватна заштитна и прекидачка опрема уз пропратну дискусију.*

Кључне речи: *Реверзибилна хидроелектрана, електроенергетски систем, прорачун кратких спојева*

Abstract – *Preparation of the connection of a pumped storage power plant (PSPP) to the power system, while respecting European practices and standards, is the main topic of this paper. For this purpose, the values of short-circuit current and voltage distribution were analyzed for various PSPP operating modes. Based on the results obtained, adequate protective and switching equipment was selected, along with an accompanying discussion.*

Keywords: *Pumped storage power plant, power system, short circuit calculation*

1. УВОД

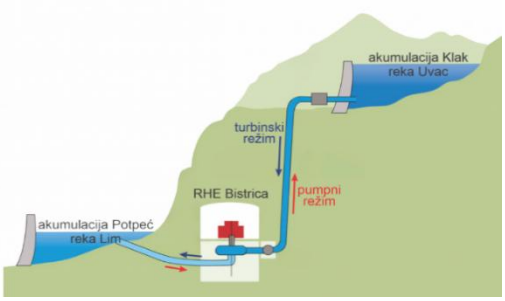
Реверзибилна хидроелектрана (РХЕ) је значајан ресурс за балансирање енергије електроенергетских система (ЕЕС), посебно у комбинацији са обновљивим изворима енергије. РХЕ омогућава складиштење вишка енергије у периодима ниске потрошње и њено ослобађање у периодима вршног оптерећења, чиме побољшава стабилност фреквенције и вредности напона [1].

У Европској унији постоји више успешних примера интеграције РХЕ у преносне мреже, где су примењени различити режими рада, методе регулације и заштита система [2]. Анализа ових искустава пружа драгоцене смернице за планирање и оптимизацију прикључења нових РХЕ на ЕЕС.

У ту сврху разматра се реална РХЕ, која треба да се интегрише у ЕЕС, преко 400 i 220 kV далековода и трансформаторске станице 400/220/18kV. Њена укупна апроксимативна инсталисана снага је око 640 MW (са четири генератора појединачне снаге приближно 160 MW). Генератори су предвиђени да раде као реверзибилне Франсис турбине са асинхроно-синхроним моторима-генераторима. Висински пад између горње и доње акумулације је 60 m, што обезбеђује погодне услове за овакав тип постројења. Разматрају се два основна режима рада:

1. Генераторски режим – производња електричне енергије у периодима вршног оптерећења.
2. Пумпни режим – акумулација вишка енергије у периодима ниске потрошње.

У оба режима, РХЕ ће доприносити стабилности фреквенције и напонског профила ЕЕС. Посебна пажња посвећена је управљању излазном снагом, да би се избегле нагле флуктуације које могу изазвати проблеме у мрежи.



Слика 1. *Приказ РХЕ са горњом и доњом акумулацијом*

2. ПРЕГЛЕД ЕВРОПСКИХ ПРАКСИ

Неки од примера европских пракси су:

Аустрија – Капрун и Малта: Аустријске РХЕ, попут постројења у Капруну, користе пумпно-турбински режим рада да би складиштиле вишак енергије и ослобађале је током вршних оптерећења. Систем омогућава брзо пребацивање између режима рада и доприноси секундарној и терцијарној регулацији.

Швајцарска – Linthal и Nant de Drance: Швајцарске РХЕ су интегрисане у планирање и често раде у комбинацији са регулационим центрима који управљају фреквенцијом и напонским профилима. Linthal и Nant de Drance користе велике акумулације и вишестепене турбинске системе, што омогућава ефикасну реакцију на промене оптерећења у преносом систему

Немачка – Goldisthal и Markerbach: Немачке РХЕ су интегрисане са ЕЕС тако да активно учествују у стабилизацији мреже током променљивих производних капацитета из ветро и солар електрана. Управљање пумпно-турбинским режимом омогућава брзо повећање или смањење снаге у ЕЕС.

НАПОМЕНА:
Овај рад је пристекo из мастер рада чији је ментор проф. др Горан Швенда.

Закључци из европских искустава [3] су:

- РХЕ треба да буде флексибилно повезана са мрежом, са могућношћу брзог пребацивања режима рада.
- Планирање прикључења мора укључити анализу напонских профила, струје кратког споја и заштитних система.
- Коришћење стандарда IEC 60909 и детаљна симулација динамике мреже су неопходни за безбедну интеграцију.
- Интеграција РХЕ доприноси не само производњи вршне енергије већ и секундарној резерви, стабилизацији фреквенције и напонској подршци.
- Ове смернице и искуства представљају основу за планирање прикључења РХЕ на ЕЕС, са циљем да се електрани максимизира допринос сигурности и поузданости мреже.

3. АНАЛИЗА УТИЦАЈА НА НАПОНЕ И СТРУЈЕ КРАТКОГ СПОЈА

3.1. Анализа утицаја на струје кратког споја

Интеграција РХЕ у ЕЕС захтева анализу утицаја струја кратког споја и напона у тачки прикључења и околним чворовима. На основу искуства из европске праксе:

- Прикључење РХЕ повећава струју кратког споја у непосредној близини електране, што захтева одговарајућу прекидачку и заштитну опрему.
- Удаљени чворови преносне мреже су обично погођени минимално, под условом правилног димензионисања трансформаторских станица и далековода.
- Управљање РХЕ помоћу аутоматизованих контролних система смањује ризик од дестабилизације ЕЕС.

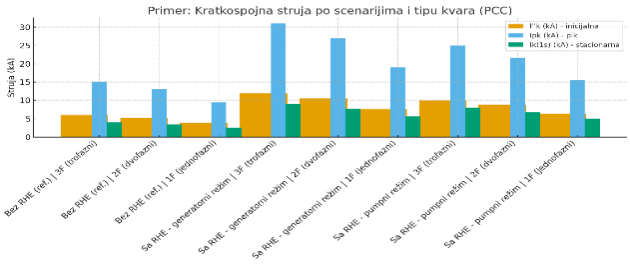
Анализа утицаја на струју кратког споја представља кључни део студија прикључења великих производних електрана на ЕЕС. Циљ ових прорачуна је да се одреде максималне и минималне вредности струја квара у тачки прикључења, као и њихов утицај на околне чворове и опрему. На основу добијених резултата доносе се закључци о потребним мерама заштите, избору прекидачке опреме и поузданости рада ЕЕС у хаваријским стањима.

За потребе овог рада коришћена је методологија дефинисана у међународном страндарду IEC 60909 - Short-Circuit Currents in Three-Phase a.c. Systems [4]. Стандард омогућава прорачун симетричних и асиметричних кратких спојева. Прорачун је спроведен за следеће типове кратких спојева:

- Трофазни симетрични квар (3Ф) – квар који највише напреже прекидачку и заштитну опрему.
- Двофазни кратак спој (2Ф) – значајан због могућег асиметричног режима у ЕЕС.
- Једнофазни кратак спој (1Ф) – најчешћи тип квара у ЕЕС.

Прорачун струја кратког споја је урађен за различите сценарије:

1. Рад без прикључења РХЕ (референтно стање).
2. Рад са прикљученом РХЕ у генераторском режиму.
3. Рад са прикљученом РХЕ у пумпном режиму.



Слика 2. *Поређење иницијалне I“k, вршне ударне Ipk и стационарне Ik(1s) струје по сценаријима и типу кратког споја (без РХЕ, са РХЕ у режиму генератора, са РХЕ у пумпном режиму)*

Scenario	Tip kvara	(kA) - inicijal	Ipk (kA) - pik	) (kA) - stacionarna
Bez RHE (ref.	3F (trofazni)	6	15	4
Bez RHE (ref.	2F (dvofazni)	5,2	13	3,5
Bez RHE (ref.	1F (jednofaz	3,8	9,5	2,6
Sa RHE - gen	3F (trofazni)	12	31	9
Sa RHE - gen	2F (dvofazni)	10,5	27	7,8
Sa RHE - gen	1F (jednofaz	7,6	19	5,6
Sa RHE - pum	3F (trofazni)	10	25	8
Sa RHE - pum	2F (dvofazni)	8,8	21,5	6,8
Sa RHE - pum	1F (jednofaz	6,4	15,5	4,9

Слика 3. *Табеларни приказ вредности иницијалне симетричне краткоспојне струје I“k, вршне ударне струје Ipk и стационарне вредности струје на 1с (Ik) за три типа кратког споја*

На овај начин могуће је сагледати утицај електране на промену вредности струје кратког споја у тачки прикључења, али и у околним чвориштима. Резултат прорачуна кратког споја показује да прикључење РХЕ значајно утиче на нивое струја кратког споја у ЕЕС. У генераторском режиму рада, вредности струја кратког споја су скоро двоструко веће у односу на референтни случај без РХЕ (у пумпном режиму оне, такође, расту, али нешто мање). Највеће вредности, очекивано, се јављају при трофазном кратком споју, док су најмање за једнофазне кратке спојеве.

3.2. Избор адекватне прекидачке и заштитне опреме

1) На основу израчунатих вредности струја кратког споја, I“k, Ipk i Ik (1s) следи да:
   - називна прекидна моћ прекидача мора бити >= од највеће израчунате иницијалне симетричне компоненте струје у тачки прикључења,
   - динамичка издржљивост (механичка, да изрдржи ударну струју) мора бити >= вршне ударне струје Ipk,
   - термичка издржљивост (1s), мора бит >= Ik (1s).

   То значи да треба да се користи 110kV SF6 прекидач са називном прекидном способношћу мин. 31,5kA (1s) и вршном издржљивошћу 63 kA.
2) Заштитна опрема

   Струјни трансформатори CTs морају бити димензионисани да мере у класи тачности и при

струјама кратког споја (класе 5P20, 10P20 за заштиту). Одабир примарних вредности СТ (нпр. 600/1 А, 800/1 А) се ради према струјама оптерећења (изабране вредности су опсегу од 50% до 120% називне струје штићеног објекта), а гранични фактор тачности (у овом случају 20) се бира тако да не дође до засићења при највећим струјама кратког споја.

Одводници пренапона (пренапонска заштита) се бира према називном напону система (110kV).

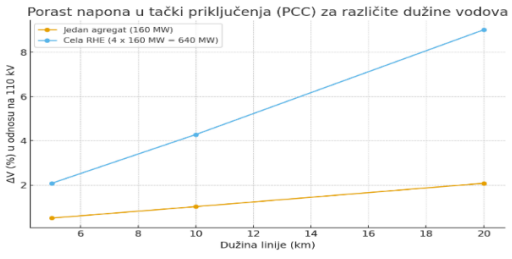
Релејна заштита: Диференцијална заштита генератора и трансформатора, прекострујна и земљоспојна заштита морају бити подешене на основу нових нивоа кратког споја.

3.3. Анализа напонских прилика

Урађен је прорачун и анализа напонских прилика за пример: агрегат 160 MW, PF=0.95lag, прикључење на 110kV. Коришћени су поједностављени једнолинијски модели (мрежа референтни „infinite bus“ на 110kV и типични параметри водова. Коришћени су следећи подаци у прорачуну: фактор снаге PF=cosα=0.95 (инд.); привидна снага S=P/cosα= 168.42 [MVA]; напонски ниво прикључења U_{LL}=110 [kV]; струја (магнитуда), $I = \frac{S}{ULL}$ = 884 [A]; линијски параметри (претпоставка, типичне вредности за средње удаљености): R' = 0.05 Ω/km ; X' =0.25 Ω/km; референтна мрежа је узета као 110kV, 0^0.

Scenario	ужина линије (ku	R (Ω)	X (Ω)	I (A)	|V_pcc| (V)	ΔV (%)
Jedan agreg	5	0,25	1,25	884	110559,3	0,508
Jedan agreg	10	0,5	2,5	884	111127,3	1,025
Jedan agreg	20	1	5	884	112288,4	2,08
Cela RHE (4 x	5	0,25	1,25	3535,9	112288,4	2,08
Cela RHE (4 x	10	0,5	2,5	3535,9	114708,4	4,28
Cela RHE (4 x	20	1	5	3535,9	119910,7	9,01

Слика 4. *Вредности струје и напона за наведене сценарије и дужине водова*



Слика 5. *Пораст напона у тачки прикључења*

Промене напона, за један агрегат (160 MW), су релативно мале (<~1% за вод до 10 km). Међутим, ако се прикључе четири агрегата (640 MW), на већој удаљености, пораст напона може достићи и премашити техничке границе.

Зашто се напон мења: Када агрегат испоручује активну снагу у мрежу, изворна струја тече кроз серијску импедансу водова и производи пад/пораст напона ΔV = Z_l*I, што мења напон у тачки прикључења. Ако је ΔV близу или изнад дозвољених граница, треба размотрити техничка решења. Повећане вредности напона утичу и на рад заштите, трансформатора и макс./мин. вредности за опрему.

4. ЗАКЉУЧАК

РХЕ са значајним капацитетом за акумулацију и балансирање, игра кључну улогу у ублажавању флуктуације које су узроковане обновљивим изворима енергије. Прикључење РХЕ има позитиван ефекат на флексибилност и сигурност снабдевања, али доводи до повећања струја кратког споја и пораста напона у тачки прикључења. Зато се интеграција РХЕ посматра целовито, енергетски и са аспекта стабилности и заштите ЕЕС.

Анализа европских пракси показује да флексибилно управљање режимом рада и аутоматски контролисани излаз снаге значајно смањује ризик од дестабилизације ЕЕС.

Са аспекта кратких спојева, прикључење генератора доводи до повећања иницијалне и ударне вредности струје у тачки прикључења, нарочито у генераторском режиму. Док би вредности у референтном стању биле у границама капацитета постојеће опреме, прикључење РХЕ може захтевати додатну проверу прекидне моћи прекидача, као и координацију релејне заштите.

Са аспекта напонских прилика, резултати показују да један генератор од 160 MW практично не угрожава напоне система – промена напона у тачки прикључења су у границама +-1%. Међутим, при раду целе електране (640 MW) промене постају израженије и достижу +4% на удаљености 10 km, односно +9% (прелазе дозвољене границе) на раздаљини 20 km. Ово показује да интеграција великих снага у мрежу нижег напонског нивоа (110 kV) може изазвати неприхватљиве порасте напона.

5. ЛИТЕРАТУРА

[1] International Energy Agency (IEA) – Pumped Storage Hydropower – A key Enabler for Renewable Energy Integration, IEA Report, Paris 2022.

[2] ENTSO-E, Hydro Power and Pumped Storage in the European Power System, Brussels, 2021.

[3] European Commission: The Role of Energy Storage in the EU Power System, Technical Report, 2020.

[4] IEC 60909-0: Short-Circuit Currents in Three-Phase a.c. Systems – Part 0: Calculation of Currents, International Electrotechnical Commission, Geneva, 2016.

Кратка биографија:

Стефан Радовић је рођен у Новом Пазару 1999. године. Основне студије уписао на ФТН-у 2018. године из области Електротехника и рачунарство, и завршио 2023.године. Исте године уписао мастер студије на ФТН у Новом Саду – смер Дистрибуирани енергетски ресурси. Тренутно запослен у АД ЕМС, Београд.

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004:007.5
DOI: https://doi.org/10.24867/34BE08Milic

ANALIZA I PRIMENA OPC UA ZA DIGITALNU TRANSFORMACIJU MAŠINE ZA BRIZGANJE PLASTIKE

ANALYSIS AND IMPLEMENTATION OF OPC UA IN THE DIGITAL TRANSFORMATION OF AN INJECTION MOLDING MACHINE

Milica Milić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U okviru ovog rada obrađena je primena OPC UA specifikacije u industriji prerade plastike, kako bi se implementiralo proizvodno postrojenje u skladu sa karakteristikama postavljenim Industrijom 4.0. Tema rada obuhvata konfigurisanje OPC UA servera primenom EUROMAP 77 informacionog modela, kao i testiranje bezbednosnih aspekata OPC UA na primeru mašine za brizganje plastike. Predstavljene su ključne prednosti OPC UA u odnosu na klasičnu implementaciju proizvodnog postrojenja.*

Ključne reči: *OPC UA, Industrija 4.0, Mašina za brizganje plastike, Industrijska komunikacija, Distribuirani računarski upravljački sistemi*

Abstract – *This work addresses the application of the OPC UA specification in the plastic processing industry, aiming to implement a production facility in accordance with Industry 4.0 principles. The scope of the paper includes the configuration of the OPC UA Server using the EUROMAP 77 information model, as well as the evaluation of OPC UA security aspects on the example of an injection molding machine. The key advantages of OPC UA compared to traditional production plant implementations are presented.*

Keywords: *OPC UA, Industry 4.0, Injection Molding Machine, Industrial communication, Distributed control systems*

1. UVOD

Razvoj novih tehnologija otvorio je puteve ka uspostavljanju novog industrijskog okruženja, koje se definiše terminom Industrija 4.0. Ovaj termin se odnosi na tehnološke promene na nivou proizvodnih postrojenja, koje su zasnovane na savremenim tehnologijama, poput interneta stvari, mašinskog učenja i veštačke inteligencije, a koje treba da ostvare pametnu proizvodnju, u potpunosti okrenutu tržišnim zahtevima. Kompleksnost proizvodnog postrojenja se ogleda u velikom broju mašina, hardverskih uređaja, kao i softvera, različitih proizvođača i nivoa složenosti. Kako bi se obezbedilo skalabilno i fleksibilno proizvodno postrojenje, neophodna je ostvariti uniformnu i transparentnu komunikacija između ovih različitih komponenata. Brojne arhitekture, poput RAMI 4.0, izdvajaju OPC UA specifikaciju kao ključnu tehnologiju koja, prema svojim karakteristikama standardizovane, platformski nezavisne i bezbedne komunikacije, obezbeđuje ostvarivanje fleksibilne, adaptivne i transparentne proizvodnje [1]. Podaci unutar čitavog postrojenja se prikupljaju i pothranjuju OPC UA server, kojem klijenti, odnosno različite komponente postrojenja, pristupaju radi čitanja, pisanja, čuvanja i manipulacije podataka.

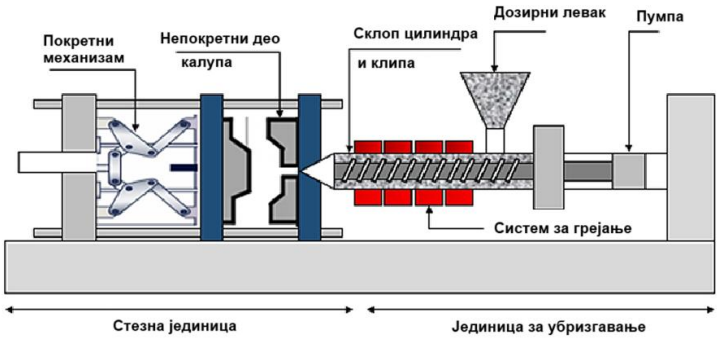
U industriji prerade plastike, mašina za brizganje plastike ima ulogu u proizvodnji plastičnih proizvoda predefinisanih oblika. OPC UA se u ovoj industriji izdvaja kao tehnologija za praćenje rada postrojenja u realnom vremenu i planiranje poslovnih procesa, a sama integracija ove mašine u okruženje pametne fabrike je omogućena i znatno olakšana uvođenjem EUROMAP standarda, koji uniformiše OPC UA informacione modele i interfejse za komunikaciju sa drugim mašinama i softverima [2].

2. AUTOMATIZACIJA U INDUSTRIJI PRERADE PLASTIKE

Proces prerade i dobijanja proizvoda od plastike je kompleksan i odvija se u više faza uz integraciju velikog broja mašina, koje svojom interoperabilnošću održavaju skladan i nesmetan rad čitavog postrojenja. Mašina za brizganje plastike (eng. *Injection Molding Machine*) je specijalizovana namenska mašina za obradu ovog materijala. Primenjuje se za potrebe masovne proizvodnje plastičnih predmeta i delova predefinisanih oblika ubrizgavanjem otopljene plastične materije u prethodno specificirane i dizajnirane kalupe.

Funkcionalno, mašina se posmatra kroz dve jedinice sa svojim podprocesima, odnosno upravljačkim petljama, dok se sam proces dobijanja plastičnog proizvoda u nekoliko faza. Funkcionalne celine mašine za brizganje plastike čine jedinica za ubrizgavanje i stezna jedinica. Faze u ciklusu proizvodnje su redom: faza doziranja i plastifikacije, faza ubrizgavanja, faza ulivanja u kalup i hlađenje i konačno, faza izbacivanja radnog komada iz kalupa. Na Slici 1 predstavljen je strukturni pregled mašine za brizganje plastike, sa označenim njenim najvažnijim delovima. Jedinica za ubrizgavanje je zadužena za zagrevanje i topljenje plastične mase, odnosno granulata, koji se dozira u sklop cilindra i klipa kroz dozirni levak i zatim se ta otopljena smesa pod pritiskom istiskuje u kalup kroz nepovratni ventil pomera-

NAPOMENA: Ovaj rad proistekao je iz master rada čiji mentor je bio dr Darko Čapko, red. prof.

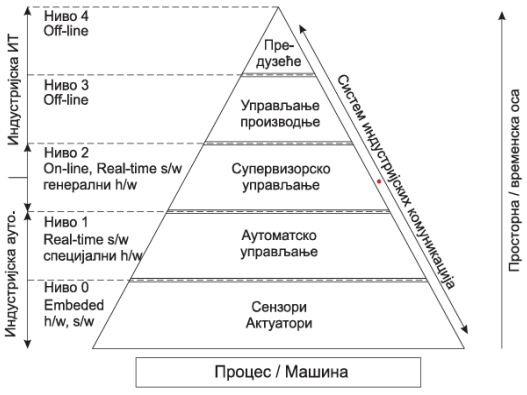


Slika 1. *Strukturni prikaz mašine za brizganje plastike [3]*

njem klipa (zavojnog vretena). Tokom ovog procesa, PLC upravlja pritiskom i temperaturom, ali kontroliše i količinu plastike koja ulazi u kalup, kao i položaj klipa. Stezna jedinica je zadužena za oblikovanje otopljene plastične mase. Prilikom brizganja, kalup je zatvoren zahvaljujući pokretnom mehanizmu, odnosno hidrauličkoj pumpi, koja obezbeđuje optimalnu vrednost pritiska držanja, kako bi kalup ostao zatvoren tokom oblikovanja. Tom prilikom, plastika se hladi usled razmene temperature sa zidovima kalupa, učvršćuje se i nakon određenog vremena, pumpa otpušta pritisak i gotov proizvod biva izbačen iz kalupa. Tokom jednog ciklusa proizvodnje, PLC deluje obrađuje informacije sa senzora i tajmera, na osnovu kojih deluje na motore, pumpe i druge aktuatore u okviru mašine.

2.1. Piramida industrijske automatike u industriji prerade plastike

Tradicionalna implementacija industrijskog proizvodnog postrojenja zasnovana je na konceptu piramide industrijske automatike. Piramida automatike je vizuelni koncept, odnosno teorijski model koji definiše pet nivoa unutar automatizovanog postrojenja i ilustruje integraciju različitih tehnologija u cilju uspostavljanja kontinuiranog rada postrojenja. Dizajnirana je tako da bude univerzalna i primenjiva na širok spektar procesa. Na Slici 2 prikazani su nivoi piramide automatike. Prva tri nivoa čine nivo operativnih tehnologija, dok su poslednja dva deo nivoa informacionih tehnologija, te se stoga i načini komunikacije između ovih tehnologija razlikuju.



Slika 2. *Piramida industrijske automatike [4]*

Senzori i aktuatori čine nivo 0, dok se PLC nalazi na nivou automatskog upravljanja. Postrojenje za preradu plastike podrazumeva interakciju velikog broja mašina za brizganje plastike i drugih mašina, te da bi se kontrolisao čitav rad postrojenja, na nivou 2 nalazi se SCADA sistem, koji preko kontrolera prikuplja procesne parametre sa senzora i aktuatora i prikazuje ih na centralizovanom računaru. Nivoi 3 i 4 predstavljaju viši nivo postrojenja, koje čine MES i ERP softveri. Na tom nivou prati se stanje mašina, otkazi i planira se remont, ali se vrši i planiranje proizvodnje, dopremanje materijala i transport gotovih proizvoda.

Komunikacija na nivou operativnih tehnologija uobičajeno je zasnovana na nekom od *Fieldbus* protokola, koji omogućavaju povezivanje procesne instrumentacije i industrijskih računara u digitalnu komunikacionu mrežu. Predstavnik ove grupe protokola, koji je ujedno najrasporostranjeniji u industriji je *Modbus* protokol. Pored ovog, u industriji su zastupljeni i mnogi drugi protokoli, razvijani od strane različitih proizvođača industrijske opreme, poput *S7* protokola kompanije Siemens. Nedostatak ovih protokola jeste striktna vezanost za proizvođača, što ih čini nekompatibilnim sa opremom drugih proizvođača usled razlika u implementaciji. Podaci, koji imaju ključni značaj za razvoj i održavanje procesa, razmenjuju se sa višim nivoima piramide, gde se obrađuju u okviru MES i ERP sistema. Na ovom nivou komunikacije, uočavaju se nedostaci *Modbus* protokola, obzirom da njegova implementacije ne obuhvata bezbednosne mehanizme, što sa stanovišta kritičnosti opreme i procesa može imati nenadoknadive posledice.

Rešenje bezbednosnih nedostaka i nestandardizovane komunikacije tradicionalnih postrojenja nalazi se u OPC UA specifikaciji. OPC UA se može posmatrati kao pokušaj destruktuiranja piramide industrijske automatike i uniformisanja komunikacije između uređaja i komponenata različitih nivoa. Rešenje je bazirano na servisnoj arhitekturi i posebnom informacionom modelu, kao nivou apstrakcije koji omogućava pojednostavljen i bezbedan pristup i manupulaciju procesnim podacima.

2.1. Industrija 4.0 i OPC UA

Termin Industrija 4.0 skovan je u Nemačkoj 2011. godine i odnosi se na novi industrijski model, koji podrazumeva transformaciju proizvodnih procesa sa centralizovanog na decentralizovani model upravljanja, u okviru kojeg pojedinačne mašine, putem prikupljenih i obrađenih podataka, mogu donositi autonomne odluke, što otvara puteve ka uspostavljanju personalizovane, fleksibilne i efikasne proizvodnje, koja je prilagođena zahtevima tržišta

i korisnika [5]. Tehnologija koja je postavila temelje Industrije 4.0 je IIoT, i omogućila je povezivanje senzora, aktuatora, opreme i mašina u informacionu mrežu, čime je olakšana komunikacija i omogućena brza razmena podataka u realnom vremenu.

Razvijen je veliki broj decentralizovanih arhitektura kako bi se olakšala razmena podataka, među kojima se izdvaja RAMI 4.0, koja OPC UA definiše kao jedan od komunikacionih standarda Industrije 4.0. Ovaj protokol omogućava semantički uniformnu i bezbednu razmenu podataka između uređaja različitih proizvođača, čineći PLC integralnim delom IIoT ekosistema. Standardizacija komunikacije smanjuje troškove integracije, ubrzava implementaciju novih rešenja i omogućava veću fleksibilnost u razvoju pametnih fabrika.

OPC UA je platformski nezavisan, IEC 62541 standard otvorenog koda za razmenu podataka. Fleksibilnost OPC UA ogleda se u mogućnosti jednostavnog prikupljanja procesnih podataka, monitoringa, kontrole i analize istih, što se ostvaruje standardizovanom reprezentacijom podataka kroz informacioni model. Pored toga, OPC UA komunikacija je bezbedna, uključujući autentifikaciju, autorizaciju, enkripciju i kontrolne sume i otvorena je za integraciju i kombinovanje sa drugim standardima [1]. Ovaj komunikacioni standard zasnovan je na servisno-orijentisanoj arhitekturi, i putem ugrađenog informacionog modela, definiše osnovna pravila razmene informacija i odgovarajuće interfejse.

3. ANALIZA PRIMENE OPC UA U INDUSTRIJI PRERADE PLASTIKE

3.1 Testiranje OPC UA informacionog modela

OPC UA koristi objektno-orijentisano modelovanje koje omogućava hijerarhijsku organizaciju podataka kroz čvorove i adresne prostore. Na taj način se svi relevantni podaci sa mašine, poput temperatura grejača, pozicije klipa, statusa ciklusa obrade, alarmi i slično, predstavljaju na struktuiran i standardizovan način. Ove podatke OPC UA server prikazuje u struktuiranom modelu podataka, gde svaki parametar ima svoje ime, jedinicu mere, trenutnu vrednost, kao i meta-informacije i na taj način svi OPC UA klijenti mogu da im pristupe na jednoobrazan način i da njima manipulišu. Klijentska aplikacija može biti PLC druge mašine, SCADA, kao i MES i ERP aplikacije.

EUROMAP standardi omogućavaju integraciju mašina različitih tipova i proizvođača kroz standardizovane interfejse i informacione modele, čime se smanjuje kompleksnost uspostavljanja i implementacije proizvodnog postrojenja. Među trenutno objavljenim standardima, izdvaja se EUROMAP 77, koji opisuje jedinstvene interfejse za razmenu podataka između mašina za brizganje plastike i MES sistema različitih proizvođača.

Implementacija informacionog modela zasnovanog na EUROMAP 77 standardu, eksperimentalno je testirana pomoću softvera *KeStudio* kompanije *Keba* i korišćenjem softvera *UaExpert*, OPC UA test klijenta opšte namene, koji podržava vizuelni pristup podacima. PLC, koji upravlja mašinom za brizganje plastike, konfigurisan je pomoću okruženja *KeStudio*, tako da OPC UA server implementira informacioni model prema definisanom standardu, koji omogućava MES sistemu da direktno pristupa njegovim varijablama. Na PLC kontoleru je kroz blok dijagram (*FBSimulateIMMProcess*) simuliran rad mašine, i to redom faze doziranja i plastifikacije, ubrizgavanja, ulivanja u kalup, hlađenja i fazu izbacivanja komada iz kalupa. Varijable koje figurišu u simulaciji su *MoldIsOpen* i *MoldIsClosed*, koje se odnose na položaj kalupa i govore da li je formiranje proizvoda u toku ili ne, kao i *EjectorIsForward* i *EjectorIsBackward*, koje se odnose na položaj klipa i ujedno su definisane kroz EUROMAP standard. Ove varijable se na uniforman način izlažu klijentima, te se njihove vrednosti mogu čitati i menjati direktno na PLC-u, tokom simulacije, ali od strane klijenata. Za vizualizaciju serverskih varijabli i čitanje njihovih verdnosti korišćen je *UaExpert* test klijent. Prvi korak jeste uspostavljanje konekcije između OPC UA klijenta i servera na osnovu URL adrese krajnje tačke, uz odabir odgovarajuće bezbednosne politike i bezbednosnog nivoa. Po uspostavljanju konekcije, klijent pristupa hijerarhijski organizovanom adresnom prostoru servera, gde svaki od čvorova sadrži podčvorove i atribute definisane u skladu sa standardom. Na ovom primeru, prikazano je konfigurisanje serverskih varijabli na dva načina, kroz aplikativni program na PLC kontroleru, koje se ažuriraju tokom upravljanja procesom i na taj način prikazuju klijentima, koji im pristupaju i koji ujedno slanjem zahteva mogu menjati stanje istih tih varijabli.

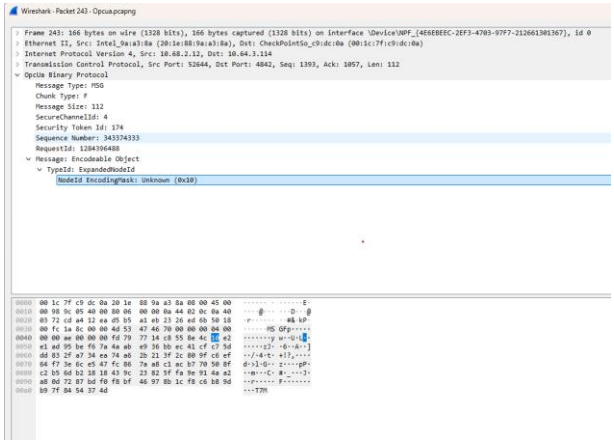
3.2 Testiranje bezbednosnih karakteristika OPC UA komunikacije

Bezbednosne karakteristike OPC UA komunikacije analizirane su na studiji slučaja, gde ERP sistem upravlja dvema mašinama za brizganje plastike - jednom koja proizvodi flaše i drugom koja proizvodi čepove. Testiranje je odrađeno korišćenjem softvera *Wireshark*, besplatnog alata za analizu mrežnog saobraćaja. OPC UA klijent i server su implementirani u programskom jeziku C pomoću biblioteke *open62541*, biblioteke otvorenog koda koja implementira OPC UA protokol.

Strukturu sistema čine ERP klijent, koji planira proizvodnju i šalje nalog ka mašini, zatim PLC, koji je ugrađen u mašinu za brizganje plastike i implementira OPC UA server i klijentima izlaže varijable i metode, kao i HMI panel, lokalni interfejs operatera koji sa PLC-om komunicira putem *Modbus* i OPC UA protokola. Na PLC-u se nalaze i komponente vezane za fizičke prekidače i sigurnosne elemente, koju server implementira kao *KeySwitch* varijablu. Ova varijabla definiše režim rada, odnosno da li je upravljanje lokalno ili daljinsko. ERP šalje PLC kontroleru proizvodni zahtev, koji sadrži broj komponenata koje treba proizvesti. Preko OPC UA klijenta se upisuju vrednosti u varijable *TargetQuantity*. PLC proverava stanje varijable *KeySwitch*, u zavisnosti od koje ERP može ili ne može

pokrenuti proces proizvodnje. Server u ovom slučaju prikazuje *KeySwitch* i *TargetQuantity* varijable, definisane unutar njegovog adresnog prostora.

Komunikacija na nivou HMI panela i PLC-a koja je uspostavljena pomoću *Modbus* protokola, iako brza, jednostavna i robusna, i kao takva široko rasprostranjena u industriji, testiranjem pomoću *Wireshark-a* pokazala se kao nebezbedna, obzirom da se poruke ne enkriptuju, jasno su čitljive i ne podržava autentifikaciju korisnika, te je podložna presretanju i manipulacijama. Sa druge strane, OPC UA podržava *None, Sign* i *Sign and Encrypt* nivoe bezbednosti, što je takođe eksperimentalno testirano pomoću *Wireshark-a. None* nivo enkripcije poruke izlaže kao neenkriptovane i jasno čitljive, međutim sama komunikacija se može nadograditi *Sign and Encrypt* nivoom. Komunikacija koja podrazumeva ovaj nivo enkripcije prikazana je na Slici 3. Poruke su u ekriptovanom, nečitljivom binarnom formatu i na taj način se u složen i kritičan industrijski sistem uvodi visok nivo bezbednosti i zaštita podataka od neovlašćenih pristupa.



Slika 3. *OPC UA Sign and Encrypt nivo enkripcije*

4. ZAKLJUČAK

Ovaj rad prezentuje ključne karakteristike Industrije 4.0 i značaj OPC UA, kao centralne specifikacije koja obezbeđuje interoperabilnu, uniformnu, skalabilnu i bezbednu razmenu podataka u okviru novog industrijskog okruženja. Njena primena u industriji prerade plastike, konkretno na mašini za brizganje plastike, predstavlja primer koji je obrađen u radu, na kome se uočavaju prednosti informacionog modelovanja podataka postrojenja za ostvarivanje komunikacije između OPC UA klijenta i servera. Informacioni model, predstavljen kroz *UaExpert*, prikazuje uniformne podatke sa servera, kojima se direktno može manipulisati. Podaci se ujedno konfigurišu u programu *KeStudio* direktno na PLC-u, na kome je implementiran OPC UA server. Standardizacija kroz EUROMAP u ovoj oblasti je od ključnog značaja za jednostavnu implementaciju Industrije 4.0. Razvoj industrijskih komunikacionih protokola pokazuje jasnu evoluciju od jednostavnih, ali nesigurnih rešenja poput *Modbus*-a, ka naprednijim i sigurnim standardima kao što je OPC UA. Implementacija OPC UA servera i klijenta pomoću *open62541* biblioteke u C jeziku pokazuje da je ovaj protokol fleksibilan i dovoljno jednostavan za integraciju i na ugrađenim sistemima, ali i dovoljno robustan za velike industrijske sisteme. Primer sa varijablom *KeySwitch* jasno demonstrira kako se fizički elementi mašine (prekidači, tasteri) mogu preslikati u OPC UA adresni prostor i učiniti dostupnim višim slojevima sistema. Time se postiže potpuna transparentnost između fizičkog sloja i ERP sistema, što je osnov za digitalizaciju i Industriju 4.0. Bezbednosni aspekti posebno dolaze do izražaja prilikom poređenja *Modbus*-a i OPC UA. Analiza komunikacije pomoću *Wireshark* alata pokazuje da *Modbus* šalje sve podatke u vidu čistog teksta, bez enkripcije ili autentifikacije, što ga čini podložnim prisluškivanju i manipulaciji. OPC UA poruke sa aktivnom enkripcijom prikazuju se samo kao šifrovani binarni blokovi. Time se obezbeđuje poverljivost, integritet i autentifikacija– osobine koje su u modernim industrijskim okruženjima nužne.

Sve navedene karakteristike ukazuju na to da OPC UA predstavlja budućnost industrijske komunikacije, jer u isto vreme obezbeđuje interoperabilnost, fleksibilnost i visok nivo bezbednosti. Integracijom OPC UA servera u PLC, mogućnošću jednostavne implementacije pomoću biblioteka, kao što je *open62541*, te podrškom za ERP sisteme, industrija dobija jedinstveno komunikaciono rešenje koje prevazilazi ograničenja starijih protokola.

5. LITERATURA

[1] M. Schleipen, H. S. Gilani, T. Bischoff, and J. Pfrommer, ‘OPC UA & Industrie 4.0 - Enabling Technology with High Diversity and Variability’, *Procedia CIRP*, vol. 57, pp. 315–320, 12 2016.

[2] A. Martins, B. M. L. Silva, H. Costelha, C. Neves, J. Lyons, and J. Cosgrove, ‘An approach to integrating manufacturing data from legacy Injection Moulding Machines using OPC UA’, 09 2021.

[3] F. Tayalati, I. Boukrouh, A. Azmani, and M. Azmani, ‘Implementation of Digital Twin and Deep Learning for Process Monitoring: Case Study in Injection Molding Manufacturing’, 08 2024, p. 8.

[4] M. R. Ristanović, ‘Arhitektura sistema industrijske automatike’, Mašinski fakultet Univerziteta u Beogradu, 2020, p. 3–4.

[5] O. Antons, J. C. Arlinghaus, ‘Distributed control for industry 4.0 - a comparative simulation study’, IFAC-PapersOnLine 54 (1) (2021) 516–521, 17th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2021.

Kratka biografija:

Milica Milić rođena je u Kragujevcu 2000. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Računarstvo i automatike odbranila je 2023.god.
kontakt: mmilica034@gmail.com

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.3
DOI: https://doi.org/10.24867/34BE09Miskovic

ULOGA I ZNAČAJ ELEKTRIČNIH AUTOMOBILA U PAMETNIM MREŽAMA

THE ROLE AND IMPORTANCE OF ELECTRIC VEHICLES IN SMART GRIDS

Maja Mišković, Boris Dumnić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Rad analizira ulogu električnih vozila u konceptu pametnih elektroenergetskih mreža i njihovu povezanost sa obnovljivim izvorima energije. U MATLAB/Simulink okruženju modelovana je IEEE 13-čvorna test mreža sa integrisanom solarnom elektranom i baterijskim skladištem energije. Cilj je prikaz uticaja ovih sistema na stabilnost i efikasnost distributivne mreže, kao i procena potencijala električnih vozila kao aktivnih elemenata u budućim pametnim mrežama.*

Ključne reči: *pametne mreže, električna vozila, obnovljivi izvori energije, solarna elektrana, baterijsko skladište energije, IEEE 13 test mreža, MATLAB/Simulink*

Abstract – *This paper analyzes the role of electric vehicles within the concept of smart power grids and their interaction with renewable energy sources. In the MATLAB/Simulink environment, the IEEE 13-bus test network was modeled with an integrated solar power plant and battery energy storage system. The aim is to evaluate the impact of these components on the stability and efficiency of the distribution network, as well as to assess the potential of electric vehicles as active elements in future smart grids.*

Keywords*: smart grids, electric vehicles, renewable energy sources, solar power plant, battery energy storage system, IEEE 13 test network, MATLAB/Simulink*

1. UVOD

Tokom poslednjih decenija, energetski sektor suočava se sa izazovima održivosti i potrebom za smanjenjem emisije štetnih gasova, dok se tradicionalni energetski sistem, zasnovan na fosilnim gorivima sve više dovodi u pitanje zbog negativnog uticaja na životnu sredinu i klimatske promene. Smanjenje ovih uticaja moguće je kroz energetsku tranziciju i postepeno uvođenje obnovljivih izvora energije, koji doprinose dekarbonizaciji i očuvanju životne sredine. U okviru procesa energetske tranzicije, posebno mesto zauzima razvoj električnih vozila i njihova integracija u koncept pametnih mreža. Električna vozila predstavljaju jedan od ključnih elemenata modernog energetskog sistema, jer ne deluju samo kao potrošači, već i kao aktivni učesnici u stabilizaciji i optimizaciji rada elektroenergetske mreže. Cilj ovog rada jeste da se istraži uloga i značaj električnih automobila u kontekstu pametnih mreža, sa posebnim osvrtom na njihov uticaj na stabilnost i fleksibilnost sistema, balansiranje potrošnje i mogućnost integracije u savremene energetske koncepte.

Struktura rada organizovana je na sledeći način.

- U prvom poglavlju data su uvodna razmatranja o značaju upotrebe obnovljivih izvora energije. Poseban akcenat stavljen je na ulogu električnih vozila u okviru pametnih mreža, njihov doprinos fleksibilnosti, stabilnosti i balansiranju energetskog sistema.
- U drugom poglavlju razmatra se razvoj elektroenergetskih sistema od tradicionalnog koncepta ka savremenom, koji uključuje decentralizovane izvore energije i napredne tehnologije upravljanja.
- Treće poglavlje se odnosi na pouzdanost i sigurnost kao ključne parametre elektroenergetskog sistema.
- Četvro poglavlje posvećeno je električnoj mobilnosti. Tipovi električnih vozila, infrastruktura za punjenje, pregled novih tehnologija, detaljno su obrađeni u ovom poglavlju.
- U petom poglavlju izvršena je simulaciona analiza IEEE 13 test mreže u koju su integrisani fotonaponska elektrana kao obnovljivi izvor energije i baterijski sistem skladištenja energije.
- Završno, šesto poglavlje, ističe najvažnije zaključke dobijene analizom. Posebno se naglašava značaj električnih vozila i pametnih mreža za moderni elektroenergetski sistem, kao i njihov potencijal za dalji razvoj i primenu u okviru održive energetske tranzicije.

2. PAMETNE MREŽE

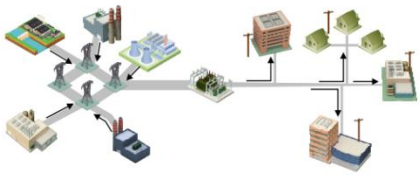
Osnovni zadatak elektroenergetskog sistema jeste da obezbedi sigurnu, kvalitetnu i ekonomičnu isporuku električne energije. Međutim, tradicionalni elektroenergetski sistem sve više se suočava sa ekološkim, finansijskim i tehničkim izazovima, što uslovljava potrebu za njegovom modernizacijom. Kao odgovor na ove izazove, javlja se koncept pametne električne mreže, čiji je cilj unapređenje pouzdanosti, energetske efikasnosti i kvaliteta napajanja električnom energijom [1].

2.1. TRADICIONALNI ELEKTROENERGETSKI SISTEM

Na slici 2.1.1. prikazan je tradicionalni model proizvodnje, prenosa i distribucije električne energije. U ovom modelu energija se proizvodi u velikim

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Boris Dumnić, red. prof.

centralizovnim elektroenergetskim postrojenjima, zatim se prenosi putem mreže visokog napona do lokalnih distributivnih sistema, koji obezbeđuju snabdevanje domaćinstva, industrijskih i poslovnih objekata [2].



Slika 2.1.1. *Infrastruktura tradicionlnog elektroenergetskog sistema [2]*

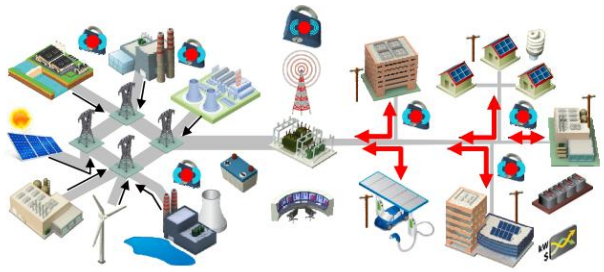
2.1.1. POJAVA DECENTRALIZOVANIH IZVORA ENERGIJE

Pojava decentralizovanih izvora energije, kao što su solarne elektrane, vetroelektrane i biogasna postrojenja, značajno menja tradicionalnu strukturu elektroenergetskog sistema. Potrošači postaju i proizvođači energije, što omogućava dvosmerni tok električne energije i veću energetsku nezavisnost. Ovakva transformacija zahteva primenu naprednih tehnologija za upravljanje, merenje i kontrolu, čime se postavljaju temelji za razvoj pametnih električnih mreža.

2.2. PAMETNA MREŽA KAO OSNOVA MODERNE ELEKTROENERGETIKE

Pametne mreže obuhvataju niz tehnologija koje omogućavaju efikasniju integraciju obnovljivih izvora energije u postojeći elektroenergetski sistem. Pored toga, uvode savremene tehnološke inovacije koje omogućavaju da tradicionalna mreža funkcioniše na naprednij, stabilniji i precizniji način u odnosu na dosadašnji pristup [3].

Infrastruktura pametne mreže sa svojim osnovnim funkcijama predstavljena je na slici 2.2.1. Karakteriše je dvosmerni protok električne energije, dvosmerna komunikacija u realnom vremenu, uređaji za skladištenje električne energije, kao i pametni merni uređaji.



Slika 2.2.1. *Infrastruktura pametne mreže [2]*

Nesumnjivo je da pametna mreža i dalje zavisi od velikih termo, hidro, kao i nuklearnih elektrana, ali za razliku od infrastrukture tradicionalnog elektroenergetskog sistema uključuje značajan broj uređaja za skladištenje električne energije, implementaciju obnovljivih izvora energije, veću primenu električnih automobila, kao i veću funkcionalnost čitavog elektroenergetskog sistema [4].

Pogodnosti koje se postižu integracijom pametnih mreža su brojne. Samo neke od njih navedene su u nastavku:

- efikasan prenos i distribucija električne energije, kao i trenutno prikupljanje podataka sa mreže,
- trenutno detektovanje kvarova na mreži, te brže uspostavljanje ponovnog snabdevanja potrošača električnom energijom,
- smanjenje troškova pri prenosu i distribuciji električne energije, što direktno dovodi do smanjenja troškova potrošača,
- integracija obnovljivih izvora energije,
- upotreba hibridnih i električnih automobila,
- kao i smanjenje emisije štetnih gasova.

3. POUZDANOST I SIGURNOST KAO KLJUČNI PARAMETRI SAVREMENOG ELEKTROENERGETSKOG SISTEMA

Pouzdanost i sigurnost predstavljaju ključne parametre savremenog elektroenergetskog sistema, jer od njih zavisi stabilnost, kontinuitet i kvalitet snabdevanja električnom energijom. **Pouzdanost** podrazumeva sposobnost sistema da obezbedi neprekidno i kvalitetno napajanje u svim uslovima rada, dok **sigurnost** podrazumeva otpornost sistema na poremećaje i njegovu sposobnost da spreči širenje kvarova i očuva stabilnost mreže. Razlika između ova dva pojma posebno dolazi do izražaja u uslovima integracije obnovljivih izvora energije, koji, iako doprinose energetskoj tranziciji i smanjenju emisije CO_2, unose nove tehničke i operativne izazove u pogledu stabilnosti i upravljanja sistemom.

3.1. ULOGA PAMETNIH MREŽA U POVEĆANJU POUZDANOSTI

Pametne mreže predstavljaju savremeni koncept elektroenergetskog sistema koji povećava njegovu pouzdanost, stabilnost i efikasnost. Zahvaljujući dvosmernoj komunikaciji i automatizaciji, omogućavaju brzo otkrivanje, izolaciju i otklanjanje kvarova, čime se skraćuje vreme prekida napajanja. Integracijom obnovljivih izvora energije i sistema za skladištenje energije postiže se bolje balansiranje između proizvodnje i potrošnje. Primena naprednih informacionih tehnologija i upravljačkih sistema omogućava fleksibilnije i sigurnije funkcionisanje mreže, čime se stvara osnova za dalji razvoj održivog i otpornog elektroenergetskog sistema budućnosti.

4. ELEKTRIČNA VOZILA I INFRASTRUKTURA

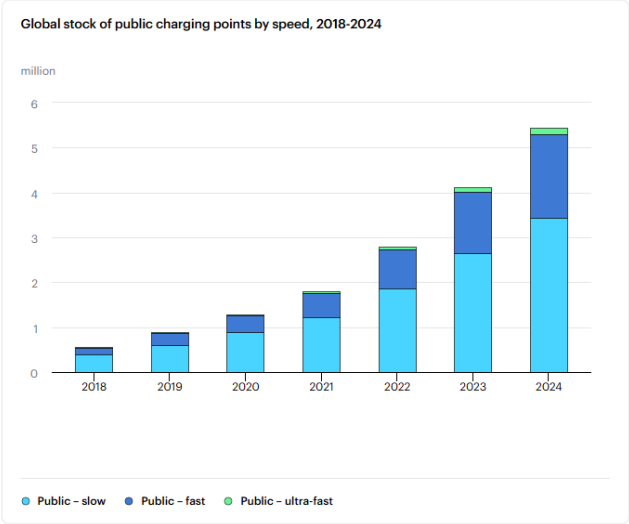
Zahvaljujući mogućnosti da smanje emisiju štetnih gasova kao i zavisnost od fosilnih goriva, električna vozila postaju sve prisutniji i traženiji oblik prevoza, koji je u poslednje vreme privukao veliku pažnju. Umesto upotrebe benzin ili dizel goriva, pokretanje električnih automobila vrši se pomoću električnog motora koji crpi energiju iz punjivih baterija. Predviđa se da će broj korisnika električnih vozila biti i do tri puta veći do 2030. godine u odnosu na 2011. godinu, što se prvenstveno pripisuje visokotehnološkom napretku u razvoju baterija i njihovom pozitivnom uticaju na autonomiju (domet) vozila – koliko daleko i koliko dugo mogu da voze bez potrebe za punjenjem [5].

4.1. TIPOVI ELEKTRIČNIH VOZILA

Električna vozila mogu se podeliti na više tipova u zavisnosti od izvora energije i načina rada [5]. **Baterijska električna vozila (BEV) -** koriste isključivo električnu energiju iz punjivih baterija i ne emituju štetne gasove, ali imaju ograničen domet. **Hibridna vozila (HEV) -** kombinuju električni i benzinski motor, pri čemu se baterija puni tokom vožnje, dok **priključna hibridna vozila (PHEV)** omogućavaju i spoljno punjenje. **Vozila na gorivne ćelije (FCEV) -** koriste vodonik za proizvodnju električne energije i imaju veći domet, ali zahtevaju posebnu infrastrukturu. **Vozila sa produženim dometom (ER-EV)** - kombinuju električni pogon sa malim benzinskim generatorom koji produžava autonomiju. Svaka tehnologija ima svoje prednosti i ograničenja – BEV i FCEV su ekološki najčistija rešenja, dok HEV i PHEV nude veću fleksibilnost i dostupnost u praksi.

4.2. INFRASTRUKTURA ZA PUNJENJE ELEKTRIČNOG VOZILA

Razvoj infrastrukture za punjenje ključan je za ubrzanje tranzicije ka održivom transportu. Sa rastom broja električnih vozila raste i potreba za brzim, pouzdanim i dostupnim sistemima punjenja.



Slika 4.2.1. *Globalni porast javnih punjača u period od 2018. Do 2024. godine [6]*

Globalni broj javnih punjača porastao je sa manje od milion u 2018. na skoro šest miliona u 2024. godini. Najviše su zastupljeni spori punjači, ali se od 2020. beleži nagli rast brzih i ultra-brzih sistema, što ukazuje na prelazak ka efikasnijoj i fleksibilnijoj infrastrukturi punjenja [6].

4.3. BUDUĆNOST ELEKTRIČNIH VOZILA

Električna mobilnost postaje novi standard savremenog transporta. Iako se baterija vozila često smatra ograničenjem, savremene tehnologije pretvaraju je u aktivan deo elektroenergetskog sistema. Zahvaljujući pametnim funkcijama kao što su *Vehicle-to-Grid (V2G)* i *Vehicle-to-Home (V2H)*, električna vozila mogu da služe ne samo kao potrošači već i kao izvori i skladišta energije. V2G omogućava dvosmerno povezivanje vozila i mreže, pri čemu se energija može vraćati nazad u mrežu tokom perioda visoke potrošnje, čime se doprinosi stabilizaciji sistema i integraciji obnovljivih izvora energije. Korisnici mogu ostvariti finansijske benefite kroz nadoknadu za isporučenu energiju, dok mreža dobija fleksibilniji i otporniji sistem [7].

Sličan princip ima i V2H, gde se energija iz baterije koristi za napajanje domaćinstva, posebno u periodima visoke potrošnje ili prekida u snabdevanju. Ova tehnologija omogućava uštedu energije i veću energetsku nezavisnost.

Iako su V2G i V2H sistemi još u fazi razvoja, interesovanje globalno raste - trenutno postoji više od 100 pilot-projekata širom sveta, što jasno ukazuje na njihov potencijal u budućim pametnim mrežama [7].

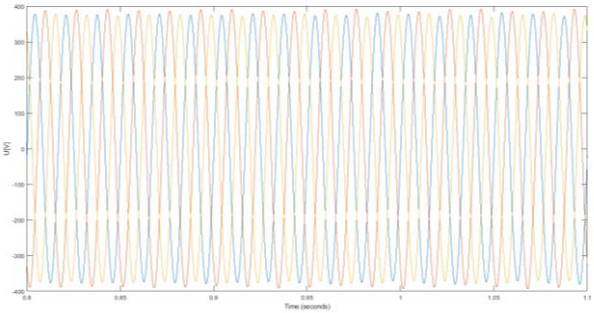
5. SIMULACIONA ANALIZA IEEE 13 TEST MREŽE SA INTEGRISANIM OBNOVLJIVIM IZVOROM I BATERIJSKIM SKLADIŠTEM

Simulaciona analiza predstavlja ključni korak u proceni performansi i stabilnosti sistema pre njegove praktične implementacije. U ovom radu, simulacija je izvršena u MATLAB/Simulink okruženju, koje omogućava integraciju različitih energetskih komponenti i njihovo ponašanje u realnim uslovima rada.

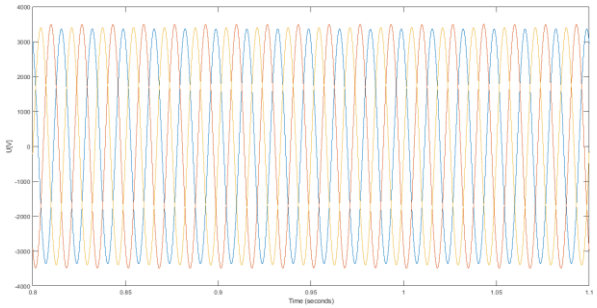
Kao referenti model korišćena je IEEE 13-bus test mreža koja predstavlja standardnu distributivnu mrežu pogodnu za analizu naponskih profila i uticaja integracije novih energetskih izvora. U okviru ove mreže izvršena je integracija fotonaponskog (PV) sistema i baterijskog sistema skladištenja energije radi simulacije rada pametne distributivne mreže sa mogućnošću lokalne proizvodnje i upravljanja energijom.

U analizi je poseban naglasak stavljen na uticaj baterijskog skladišta i solarne elektrane na naponske profile, kako u uslovima normalnog rada mreže, tako i tokom pojave kratkog spoja u čvoru 671. Na taj način ispituje se ponašanje napona u čvoru u kojem su priključeni fotonaponski sistem i baterijsko skladište, kao i njihova zajednička sposobnost da ublaže poremećaje izazvane kvarom u drugom delu mreže.

U režimu normalnog rada, integracija decentralizovanih izvora u čvoru 634 pozitivno utiče na lokalne naponske profile i doprinosi stabilnosti sistema.

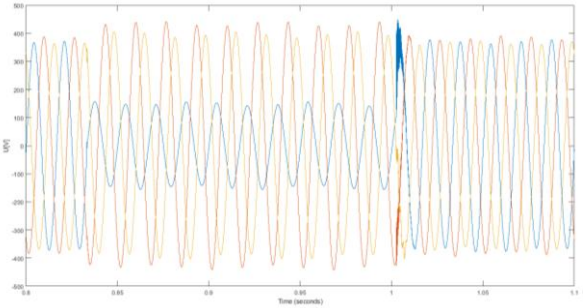


Slika 5.1. *Napon u čvoru 634*

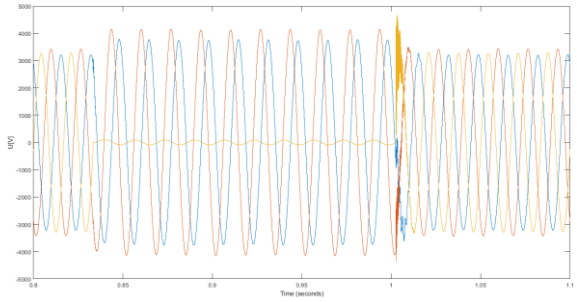


Slika 5.2. *Napon u čvoru 671*

Da bi se ispitao uticaj kvarova na naponske profile, u simulaciju je uveden jednofazni kratki spoj u čvoru 671, faza A, pri čemu je praćen napon u čvorovima 671 i 634, gde su priključeni fotonaponski sistem i baterijsko skladište. Tokom kvara u fazi A dolazi do privremenog pada napona, dok prisustvo decentralizovanih izvora omogućava delimično održavanje napona i ublažavanje oscilacija. Nakon prestanka kvara, napon se stabilizuje i vraća na nominalne vrednosti, što potvrđuje ulogu baterijskog skladišta i fotonaponskog sistema u poboljšanju stabilnosti i kvaliteta napajanja.



Slika 5.3. *Napon u čvoru 634*



Slika 5.4. *Napon u čvoru 671*

Da bi se prikazala uloga decentralizovanih izvora, simuliran je jednofazni kratki spoj u čvoru 671, faza A, bez priključenog fotonaponskog sistema i baterijskog skladišta, pri čemu je zabeležen izraženiji pad napona i duže trajanje tranzijentnih oscilacija. Prisutvo PV sistema i baterije značajno ublažava pad napona i skraćuje vreme oporavka mreže, poboljšavajući stabilnost i pouzdanost distributivnog sistema. Poređenjem oba scenarija jasno se vidi ključna uloga lokalnih izvora u održavanju naponske stabilnosti tokom kvarova, dok detaljno praćenje struja dodatno osvetljava njihovu dinamiku u trenutku kratkog spoja.

Tokom jednofaznog kratkog spoja u čvoru 671, bez prisustva decentralizovanih izvora, struja kratkog spoja u fazi A brzo dostiže vršnu vrednost, a zatim se stabilizuje na uobičajenom nivou mreže. Prisustvo DER-a (PV sistema i baterijskog skladišta) u čvoru 634 rezultira nešto višim vršnim vrednostima struje kratkog spoja, dok istovremeno doprinosi stabilizaciji napona i ublažava pad u mestu kvara. Ovi rezultati ističu ključnu ulogu decentralizovanih izvora u kontroli kratkospojnih struja i unapređenju stabilnosti distributivne mreže.

6. ZAKLJUČAK

Savremene elektroenergetske mreže sve više integrišu decentralizovane izvore i baterijska skladišta, pri čemu električni automobili kroz V2G koncept mogu doprineti stabilnosti napona i ublažavanju kratkospojnih struja. Simulacije u MATLAB/Simulinku pokazuju da prisustvo PV sistema i baterija smanjuje vršne vrednosti kratkospojnih tokova i ubrzava povratak napona u ustaljeno stanje, čak i kod manjih lokalnih skladišta. Pored tehničkih benefita, električni automobili unapređuju energetsku efikasnost i fleksibilnost mreže, čineći je stabilnijom, održivijom i spremnijom za integraciju obnovljivih izvora.

7. LITERATURA

[1] Isidora Savić, “Realizacija pametnih mreža i distribuirani generatori”, Zbornik radova, Fakultet tehničkih nauka, Novi Sad

[2] G. Horst, M. McGranaghan, P. Myrda, “Estimating the Costs and Benefits of the Smart Grid – A Preliminary Estimate of the Investment”

[3] D. Brajović, A. Rašić, “Implementacija novih tehnologija pametnih mreža sa automatizacijom u postojeće mreže elektrodistrubucije Jagodina i uticaj na kvalitet isporuke električne energije na delu područja PJ Svilajnac”

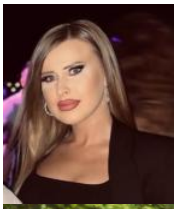
[4] Zorica Delić, “Pametna mreža – automatizacija i integracija novih tehnologija”, Elektrotehnički fakultet

[5] Electric Vehicles: Benefits, Challenges, and Potential Solutions for Widespread Adaptation

[6]https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-charging

[7] https://blog.evbox.com/v2g-v2h-difference

Kratka biografija:



Maja Mišković rođena je u Sremskoj Mitrovici 2000. god. Osnovne studije završila je na Fakultetu tehničkih nauka 2024. god. Iste godine upisuje master studije, smer– Distribuirani energetski resursi i pametne mreže.

Prof. Dr Boris Dumnić rođen je 1976. god. Redovni je profesor, dekan i šef katedre za Energetsku elektroniku i pretvarače.

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.31
DOI: https://doi.org/10.24867/34BE10Zilovic

PRORAČUN STRUJE KRATKOG SPOJA I KOORDINACIJA PREKOSTRUJNE RELEJNE ZAŠTITE U MIKROMREŽAMA

SHORT-CIRCUIT CALCULATION AND OVERCURRENT RELAY PROTECTION COORDINATION IN MICROGRIDS

Aleksej Žilović, Luka Strezoski, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ENERGETIKA, ELEKTRINIKA I TELEKOMUNIKACIJE

Kratak sadržaj – *Mikromreže, kao lokalni i fleksibilni energetski sistemi koji mogu raditi povezano s mrežom ili u ostrvskom režimu, donose izazove u analizi zbog prisustva distribuiranih energetskih resursa (DER). Posebni problemi javljaju se pri proračunu struja kratkog spoja i koordinaciji relejne zaštite, gde tradicionalne metode nisu dovoljne zbog dvosmernih tokova energije i invertorskih izvora. Ovaj rad prikazuje postojeće pristupe ovim problemima, analizira njihove prednosti i ograničenja, te kroz simulacije u ETAP-u ocenjuje najperspektivnije metode i pravce daljeg razvoja relejne zaštite mikromreža.*

Ključne reči: *Distribuirani energetski resursi (DER), Mikromreže, proračun struje kratkog spoja, podešavanje i koordinacija relejne zaštite, ETAP.*

Abstract – *Microgrids, as local and flexible energy systems capable of operating both grid-connected and islanded, present challenges in analysis due to the presence of distributed energy resources (DER). Specific issues arise in short-circuit current calculation and relay protection coordination, where traditional methods are often insufficient because of bidirectional power flows and inverter-based sources. This paper reviews existing approaches to these problems, analyzes their advantages and limitations, and evaluates the most promising methods through simulations in ETAP, providing insights into their effectiveness and directions for further development of microgrid protection.*

Keywords: *Distributed Energy Resources (DER), Microgrids, Short-circuit calculation, Relay protection setting and coordination, ETAP.*

1. UVOD

Globalna potražnja za električnom energijom stalno raste, dok fosilni izvori i tradicionalne elektrane ne mogu dugoročno zadovoljiti potrebe. Integracija distribuiranih energetskih resursa (DER) u mreže omogućava prelazak sa pasivnih na aktivne distributivne sisteme, čiji se manji delovi nazivaju mikromreže.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Luka Strezoski, vanr. prof.

Mikromreže nude prednosti poput smanjenja emisija, veće pouzdanosti i efikasnijeg upravljanja energijom, u skladu s konceptom „3D“ – dekarbonizacija, digitalizacija i decentralizacija. Ipak, one donose i tehničke, pravne i bezbednosne izazove [1,2].

Ovaj rad obrađuje dve ključne teme: proračun kratkih spojeva i koordinaciju relejne zaštite u mikromrežama sa velikim prisustvom DER-ova. Metode su analizirane teorijski i verifikovane simulacijama na primeru mikromreže univerzitetskog kampusa Case Western Reserve University u softveru ETAP.

2. DISTRIBUIRANI ENERGETSKI RESURSI (DER)

Distribuirani energetski resursi (DER) obuhvataju lokalne izvore i skladišta energije koji omogućavaju efikasniju, pouzdaniju i ekološki prihvatljiviju proizvodnju i potrošnju električne energije. U DER spadaju fotonaponske i vetroelektrane, mikroturbine i skladišta energije.

Fotonaponske elektrane pretvaraju sunčevu energiju u električnu pomoću invertera i MPPT algoritama, dok vetroelektrane koriste kinetičku energiju vetra, pri čemu savremeni inverter-based sistemi omogućavaju potpunu kontrolu snage. Mikroturbine koriste fosilna goriva u kogeneraciji i povezuju se na mrežu preko energetske elektronike. Skladišta energije (najčešće baterije i zamašnjaci) omogućavaju balansiranje sistema i podršku mreži putem dvosmernih pretvarača [3,4].

DER sistemi doprinose smanjenju emisija, povećanju fleksibilnosti i formiranju održivih mikromreža.

3. PRORAČUN KRATKIH SPOJEVA

Proračun kratkih spojeva omogućava analizu ponašanja elektroenergetskog sistema tokom kvara i služi za dimenzionisanje opreme i podešavanje relejne zaštite. Tradicionalne metode, zasnovane na matrici admitanse i Njutn–Rafsonovom postupku, pogodne su za prenosne mreže, ali ne i za radijalne distributivne sisteme sa velikim brojem čvorova i prisustvom DER-ova. Zbog toga su razvijeni efikasniji algoritmi, poput admitantno–impedantnog, modifikovanog “Backward–Forward Sweep” i kompenzacionog metoda, prilagođeni distributivnim mrežama.
U mikromrežama, prisustvo DER-ova menja topologiju i doprinosi ukupnoj struji kratkog spoja, pa korišćenje standarda IEC 60909 za modelovanje DER-ova u uslovima

kvara više nije adekvatno. DER-ovi povezani preko uređaja energetske elektronike (posebno inverter-based izvori) zahtevaju preciznije modele koji uključuju *Grid Code* standard, tačnije zahteve Fault Ride Through (FRT) i Reactive Current Injection (RCI), unutar njega. Oni određuju koliko dugo i u kom obimu DER ostaje priključen tokom kvara i kolika treba da bude reaktivna komponenta injektirane struje kako bi se popravile naponske prilike [5].

Savremene metode za proračun kratkih spojeva u mikromrežama koje se mogu naći u aktuelnoj literaturi ne uzimaju u obzir sve vrste kratkih spojeva, kao ni oba radna režima mikromreže. Stoga, u sledećem podpoglavlju je opisana već postojeća metoda za proračun kratkih spojeva u mikromrežama [3,6,7] koja sa visokom efikasnošću računa sve vrste kratkih spojeva u oba radna režima.

3.1. Izdvojena metoda za proračun kratkih spojeva u mikromrežama

U [3] je testirana metoda proračuna kratkih spojeva u mikromreži sa visokim udelom IBDER-ova, uz poređenje sa standardom IEC 60909 u oba režima rada. Pokazano je da pojednostavljeni modeli mogu izazvati greške i do 36% tokom ostrvskog rada, što dovodi do nepreciznog podešavanja relejne zaštite. Zato je neophodno modelovanje svih elemenata mikromreže u skladu sa *Grid Code* zahtevima.

Na slici 1 prikazan je modul kvara generalizovanog Δ–kola, pomoću kog je izveden kompletan matematički model generalizovanog Δ–kola mikromreže sa kvarom prikazan u sledećem izrazu

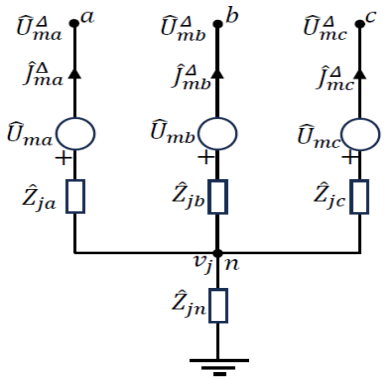
$$\begin{vmatrix} \widehat{\boldsymbol{Y}}^{dio} & \widehat{\boldsymbol{T}} & \boldsymbol{0} \\ \widehat{\boldsymbol{A}}^{U.dio} & \widehat{\boldsymbol{A}}^{J,dio} & \widehat{\boldsymbol{A}}^{v,dio} \\ \boldsymbol{0} & \widehat{\boldsymbol{C}}^{J,dio} & \widehat{\boldsymbol{C}}^{v} \end{vmatrix} x \begin{vmatrix} \widehat{\boldsymbol{U}}_K^{\Delta,dio} \\ \widehat{\boldsymbol{J}}_F^{\Delta,dio} \\ \widehat{\boldsymbol{V}}^{\Delta} \end{vmatrix} = \begin{vmatrix} \widehat{\boldsymbol{J}}_{INJ} \\ \widehat{\boldsymbol{A}}^{0} \\ \boldsymbol{0} \end{vmatrix}$$

Gde su:

- $\widehat{\boldsymbol{J}}_{INJ}^{\Delta,dio}$ predstavlja vektor injektiranih struja u domenu simetričnih komponenti u generalizovanom Δ–kolu,
- $\widehat{\boldsymbol{Y}}^{dio}$ predstavlja matricu admitansi mikromreže u domenu simetričnih komponenti,
- $\widehat{\boldsymbol{U}}_k^{\Delta,dio}$ predstavlja vektor napona čvorova mikromreže u domenu simetričnih komponenti,
- $\boldsymbol{T}$ predstavlja matricu incidencije, i
- $\widehat{\boldsymbol{J}}_F^{\Delta,dio}$ predstavlja vektor struja svih modula kvarova unutar mikromreže.

Dok se preostali vektori u izrazu (1) izračunavaju na osnovu tipa kratkog spoja, tačnije vrednosti impedansi grana sa slike 1.

Metoda proračuna kratkog spoja u mikromreži sastoji se iz dva koraka. U prvom koraku određuju se ekscesne struje svih DER-ova. Najpre se proračunavaju naponi u čvorovima njihovog priključenja u trenutku kvara, jer ti naponi definišu veličinu struje prema Grid Code standardu.



Slika 1. *Modul kvara u generalizovanom Δ–kolu [3].*

Pretpostavlja se da invertori još nisu detektovali kvar, pa DER-ovi u tom trenutku injektiraju istu struju kao pre kvara, dok su ekscesne struje u generalizovanom Δ–kolu jednake nuli. Nakon toga se naponi svih čvorova određuju superpozicijom napona pre i tokom kvara, a ekscesne struje dobijaju kao razlika ukupne i prethodne struje DER-a.

U drugom koraku, poznate ekscesne struje se unose u model, čime vektor injektiranih struja postaje nenulti i omogućava proračun kompletnog stanja mikromreže sa kvarom. Konačno stanje dobija se superpozicijom generalizovanog Δ–kola i kola pre kvara.

Ovakav pristup precizno modeluje IBDER-ove, ne zahteva koren mreže i omogućava brze i tačne proračune za sve tipove kvarova u oba režima rada mikromreže. Upravo iz tog razloga je uzeta za analizu među ostalim metodama iz aktuelne literature.

4. PODEŠAVANJE I KOORDINACIJA PREKOSTRUJNE RELEJNE ZAŠTITE U DISTRIBUTIVNIM MREŽAMA

Relejna zaštita obezbeđuje selektivno isključenje kvara i pravilno funkcionisanje mreže. U distributivnim sistemima najčešće se primenjuju trenutna prekostrujna zaštita (I>>), prekostrujna zaštita (I>) i prekostrujna zaštita sa relejom nulte komponente (I_0>), koje štite elemente mreže od međufaznih i zemljospojnih kvarova. Releji mogu imati strujno nezavisnu ili zavisnu karakteristiku, pri čemu se selektivnost postiže podešavanjem struje i vremena delovanja [8].

Sa integracijom DER-ova, distributivne mreže postaju aktivne, a tokovi snage dvosmerni. To menja vrednosti i smerove struja kratkog spoja, što može izazvati pogrešno ili zakašnjelo delovanje releja i narušiti koordinaciju zaštite. Poseban problem javlja se između reklozera i osigurača, gde prisustvo DER-a može promeniti redosled reagovanja. Zbog toga je neophodno prilagoditi tradicionalne šeme zaštite novim uslovima rada kako bi se očuvala selektivnost i pouzdanost sistema.

4.1. Adaptivna relejna zaštita sa visokim prisustvom DER-ova

Adaptivna metoda koordinacije prekostrujne zaštite razvijena je u [5,9] radi rešavanja problema koje donosi integracija DER-ova u distributivne mreže. Za razliku od tradicionalnih pristupa, ova metoda uvodi vremenske intervale između trenutka nastanka kvara i reagovanja

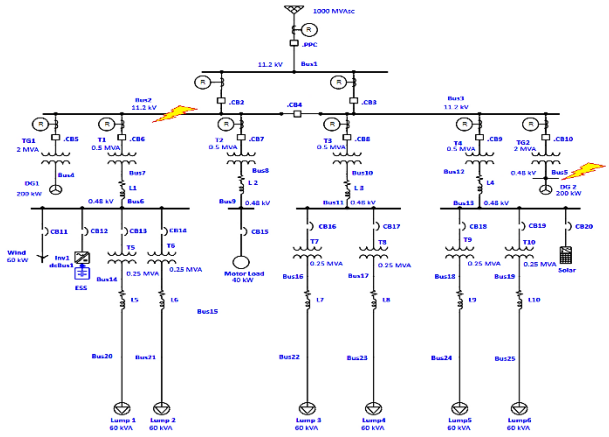
releja, koji se određuju prema vremenu isključenja DER-ova iz mreže u skladu sa FRT zahtevima.

Postupak se zasniva na analizi parova glavni–rezervni relej. Nakon pojave kvara, svi DER-ovi ostaju priključeni određeno vreme (u radu se koristio FRT zahtev Nemačke, u kom je ovo vreme jednako 150 ms), tokom kojeg se proračunavaju struje kratkog spoja i vremena reagovanja oba releja. Ako glavni relej reaguje pre isteka tog perioda, proračun se završava. Ukoliko ne, prelazi se u sledeći interval u kojem se uzima u obzir postepeno isključenje DER-ova u zavisnosti od pada napona. Za svaki novi interval ponovo se izračunavaju struje kratkog spoja i vremena delovanja releja, uz korekciju prethodnih vrednosti.

Postupak se ponavlja sve dok nijedan DER ne ostane priključen pre reakcije glavnog releja, čime se obezbeđuje tačna koordinacija i selektivnost zaštite. Ova metoda omogućava dinamičko prilagođavanje podešavanja releja promenljivom broju aktivnih DER-ova i predstavlja pouzdano rešenje za mreže sa visokim udelom distribuiranih izvora, uključujući i mikromreže.

5. NUMERIČKA ANALIZA REZULTATA

Na slici 2 prikazana je jednopolna šema mikromreže univerzitetskog kampusa *Case Western Reserve (CWRU)* iz Klivlenda, Ohajo, modelovana u softveru ETAP. Mikromreža obuhvata 28 trofaznih čvorova sa više distribuiranih izvora energije: dva dizel-generatora po 200 kW , vetrogenerator od 60 kVA , sistem za skladištenje energije od od 40 kVA i solarni izvor od 40 kVA, kao i više potrošača snage od 60 kVA po čvoru.



Slika 2. *Jednopolna šema CWRU mikromreže.*

Simulacije kratkih spojeva sprovedene su u čvorovima 2 i 3 (dve žute munjice na slici 2). Simulirani su jednopolni i tropolni kratak spoj, u povezanom i ostrvskom režimu rada, radi procene ponašanja mikromreže u različitim uslovima.

U naredna dva potpoglavlja prikazane su analize rezultata kratkih spojeva i koordinacije relejne zaštite.

5.1. Simulacija kratkih spojeva u čvorovima 2 i 5

Simulacije kratkih spojeva sprovedene su u čvorovima 2 i 5 mikromreže CWRU, kako bi se procenilo ponašanje sistema u povezanom i ostrvskom režimu rada. Na slici 2 prikazana je jednopolna šema mikromreže modelovane u ETAP-u, dok su rezultati kratkih spojeva dati u tabelama 1–4. U čvoru 2, koji je najbliži tački zajedničkog priključenja *(PCC)*, izvedene su simulacije tropolnog i jednopolnog kratkog spoja. Kod tropolnog kratkog spoja, struja kratkog spoja u povezanom režimu iznosila je oko 52 kA, dok je u ostrvskom bila svega 260 A, što predstavlja razliku od gotovo 200 puta (tabela 1). Slično, kod jednopolnog kratkog spoja struja je pala sa 25 kA u povezanom na 380 A u ostrvskom režimu (tabela 2). Ovi rezultati jasno pokazuju da u ovom delu sistema gotovo celokupnu struju kratkog spoja obezbeđuje Utility grid, dok je doprinos DER-ova zanemarljiv.

Tabela 1. *Rezultati za tropolni kratak spoj u čvoru 2.*

	TROPOLNI KRATAK SPOJ			
Režim rada	**Povezan sa mrežom**		**Ostrvski**	
Veličine	I_f[kA]	V_f[%]	I_f[kA]	V_f[%]
Bus 2	51.807	0	0.262	0
Bus 5	1.776	4.17	1.776	4.17
Bus 6	1.097	12.33	1.097	12.33
Bus 13	0.62	7.47	0.62	7.47

Tabela 2. *Rezultati za jednopolni kratak spoj u čvoru 2.*

	JEDNOPOLNI KRATAK SPOJ			
Režim rada	**Povezan sa mrežom**		**Ostrvski**	
Veličine	I_f[kA]	V_f[%]	I_f[kA]	V_f[%]
Bus 2	25.529	0	0.384	0
Bus 5	0.489	50.21	1.513	32.29
Bus 6	0	88.26	0.035	56.87
Bus 13	0.138	87.42	0.051	55.76

Analiza čvora 5, na kojem je priključen dizel-generator DG2, pokazuje veći doprinos lokalne proizvodnje. Kod tropolnog kratkog spoja struja kratkog spoja u povezanom režimu iznosila je oko 45 kA, dok je u ostrvskom bila 5 kA (tabela 3). Za jednopolni kratki spoj vrednosti su bile približno 11 kA i 5 kA (tabela 4). Razlika između režima je manja nego u čvoru 2, jer lokalni DER doprinosi napajanju kratkog spoja u ostrvskom radu.

Tabela 3. *Rezultati za tropolni kratak spoj u čvoru 5.*

	TROPOLNI KRATAK SPOJ			
Režim rada	**Povezan sa mrežom**		**Ostrvski**	
Veličine	I_f[kA]	V_f[%]	I_f[kA]	V_f[%]
Bus 5	45.568	0	5.564	0
Bus 4	0.064	101.43	1.554	8.84
Bus 6	0.038	101.47	0.506	19.79
Bus 13	0.066	101.51	0.549	15.42

Tabela 4. *Rezultati za jednopolni kratak spoj u čvoru 5.*

	JEDNOPOLNI KRATAK SPOJ			
Režim rada	**Povezan sa mrežom**		**Ostrvski**	
Veličine	I_f[kA]	V_f[%]	I_f[kA]	V_f[%]
Bus 5	11.768	0	5.283	0
Bus 4	0.011	104.74	1	38.75
Bus 6	0.007	104.39	0.579	51.07
Bus 13	0.05	104.58	0.371	48.96

Zaključno, rezultati potvrđuju da tip kratkog spoja, lokacija i režim rada značajno utiču na vrednost struje kratkog spoja. Tropolni kratki spojevi izazivaju najveće struje, dok su one najmanje u udaljenim tačkama tokom ostrvskog rada. Primenjena metoda proračuna pokazala je visoku tačnost i pouzdanost u svim analiziranim slučajevima, čime je potvrđena njena primenljivost u realnim mikromrežama.

5.2. Koordinacija relejne zaštite za kratke spojeve u čvorovima 2 i 5

Studija koordinacije relejne zaštite sprovedena je u softveru ETAP korišćenjem modula *Star – Protection and Coordination*, namenjenog analizi i podešavanju zaštitnih uređaja. Simuliran je tropolni kratki spoj u čvorovima 2 i 5, kao i u prethodnim analizama, ali samo u povezanom režimu rada, zbog ograničenja standardne metode koja ne obuhvata ostrvski rad mikromreže. Bitno je napomenuti da *Star – Protection and Coordination* modul ne uvažava implementiranje matematičkih funkcija, već da koristi standard IEC kao referencu. Upravo zato, u narednom pasusu kada se bude govorilo o "korigovanim vrednostima", odnosiće se na upotrebu opisane adaptivne metode za koordinaciju relejne zaštite za korigovanje vremena reagovanja dobijenih u softveru ETAP.

U čvoru 2 relej je reagovao nakon 20 ms, što je unutar prvog FRT intervala dok su svi DER-ovi još priključeni na mrežu, pa dalji proračun nije bio potreban. U čvoru 5 vreme reagovanja releja iznosilo je 390 ms, što prema FRT zahtevima prelazi prvi interval od 150 ms, te je analiza nastavljena u sledećem vremenskom koraku. U drugom intervalu, kada se deo DER-ova isključuje zbog pada napona, proračun je korigovan i dobijena su nova vremena delovanja releja – za glavni relej 10 vreme je povećano na 508 ms, dok je za rezervni relej 3 smanjeno na 1280 ms. Ovi rezultati potvrđuju da adaptivna metoda pruža veću preciznost jer dinamički prati promene u mreži i usklađuje podešavanja prema stvarnim uslovima rada.

Iako metoda uspešno modeluje ponašanje IBDER sistema i ispunjava FRT zahteve, njeno ograničenje je primena isključivo u povezanom režimu mikromreže. U ostrvskom režimu, gde su struje kratkog spoja znatno manje, potrebna su dodatna istraživanja i razvoj naprednijih rešenja koja bi omogućila pouzdano delovanje zaštite u svim režimima rada mikromreže. Ovo predstavlja osnovu za zaključke i preporuke iz narednog poglavlja.

6. ZAKLJUČAK

U ovom radu prikazan je pregled i analiza metoda za proračun kratkih spojeva i nadstrujnu relejnu zaštitu u mikromrežama, sa fokusom na njihove mogućnosti i ograničenja. Pokazano je da konvencionalne metode često koriste pojednostavljene modele DER-ova, zavise od postojanja korena mreže i ne opisuju precizno ostrvski režim rada, što dovodi do grešaka u proračunima i nepouzdanog funkcionisanja zaštite.

Za analizu su odabrane po jedna reprezentativna metoda iz obe oblasti. Simulacije na mikromreži Univerziteta Case Western Reserve pokazale su da metoda zasnovana na generalizovanom Δ-kolu, usklađena sa FRT i RCI zahtevima, obezbeđuje visoku tačnost, dok adaptivna relejna zaštita pokazuje ograničenja u ostrvskim uslovima sa malim strujama kratkog spoja.

Rezultati ukazuju na potrebu razvoja naprednih, adaptivnih metoda zaštite koje dinamički prate promene u radu mikromreže. Buduća istraživanja treba da budu usmerena na razvoj robustne, ekonomične i pouzdane nadstrujne zaštite, koja bi:

- uvažavala FRT i RCI standarde,
- bila primenljiva u oba režima rada,
- bila nezavisna od postojanja korena mreže,
- adaptivno menjala podešavanja u zavisnosti od režima,
- radila stabilno i tokom prelaznih stanja.

Razvoj takve metode biće predmet daljih istraživanja autora i mentora.

7. LITERATURA

[1] [1] Л. Стрезоски, „Моделовање и фундаментални прорачуни активних дистрибутивних мрежа“, Факултет техничких наука, Нови Сад, 2021.

[2] L. Mariam, M. Basu, M.F. Colon "Microgrid: Architecture, policy and future trends", vol 64, 2016, pp 477-489. https://doi.org/10.1016/j.rser.2016.06.037

[3] Strezoski, L., Prica, M., Loparo, K. A. "Generalized Δ-Circuit Concept for Integration of Distributed Generation in Real-Time Short-Circuit Calculations." *IEEE Transactions on Power Systems*, vol. 32, no. 4, 2017, pp. 3237–3245. doi:10.1109/TPWRS.2016.2617158

[4] Uddin, M., Mo, H., Dong, D., Elsawah, S., Zhu, J., Guerrero, J. M. "Microgrids: A Review, Outstanding Issues and Future Trends." *Energy Strategy Reviews*, vol. 49, 2023, 101127. https://doi.org/10.1016/j.esr.2023.101127.

[5] Luka Strezoski, Izabela Stefani, Dusko Bekut, Novel method for adaptive relay protection in distribution systems with electronically-coupled DERs, International Journal of Electrical Power & Energy Systems, Volume 116, 2020, 105551, ISSN 0142-0615, https://doi.org/10.1016/j.ijepes.2019.105551.

[6] L. V. Strezoski, N. G. Simic and K. A. Loparo, "A Robust Short-circuit Calculation Method for Islanded, Grid-connected, and Utility Microgrids," in *Journal of Modern Power Systems and Clean Energy*, vol. 13, no. 1, pp. 325-337, January 2025, doi: 10.35833/MPCE.2023.001041

[7] Strezoski, V., Bekut, D., "A canonical model for the study of faults in power systems", *IEEE*, vol. 6, no. 4, 1991, pp. 1493-1499. doi: 10.1109/59.116995

[8] Поповић, Д., Бекут, Д., Тресканица, В. „Специјализовани ДМС алгоритми“, Нови Сад, 2004.

[9] И.Стефани,"Прорачун подешавања и координације релејне заштите у дистрибутивним системима са дистрибуираним енергетским ресурсима заснованим на уређајима енергетске електронике“, Факултет техничких наука, Нови Сад, 2021.

Kratka biografija:

Aleksej Žilović rođen u Novom Sadu 2001. god. Osnovne studije upisuje 2020. god. i iste završava 2024. Odmah nakon toka upisuje master akademske studije, smer Elektroenergetski sistemi. Kontakt: aleksej.zilovic@uns.ac.rs

Prof. Dr Luka strezoski rođen je 1976. god. Redovni je profesor, dekan i šef katedre za Energetsku elektroniku i pretvarače.

Зборник радова Факултета техничких наука, Нови Сад

УДК: 004.383.5
ДОИ: https://doi.org/10.24867/34BE11Krunic

Аутоматска детекција и класификација патологија на гастроскопским и колоноскопским снимцима

Automatic detection and classification of pathology in gastroscopic and colonoscopic images

Светлана Крунић, *Факултет техничких наука, Нови Сад*

Студијски програм – ОБРАДА СИГНАЛА

Кратак садржај – *Циљ рада је пројектовање и обука аутоматског система за анализу гастроскопских и колоноскопских снимака у видљивом спектру ради детекције присуства патоморфолошких промена и њихове категоризације. Систем је заснован на савременим методама дубоког учења и способан да самостално, на основу снимака насталих током стандардне дијагностичке ендоскопске процедуре, процени да ли у снимцима постоје патоморфолошке промене, које категорије, и представи резултате у облику вероватноће присуства патологије (абнормалан налаз) и вероватноће различитих категорија болести. Употребни циљ је дијагностичка помоћ лекарима приликом дијагностике.*

Кључне речи: ***класификација, ендоскопске слике, машинско учење***

Abstract – *The aim of this work is to design and train an automatic system for the analysis of gastroscopic and colonoscopic images in the visible spectrum for the detection of the presence of pathomorphological changes and their categorization. The system is based on modern deep learning methods and is capable of autonomously assessing, based on images obtained during standard diagnostic endoscopic procedures, whether pathomorphological changes are present, to which category they belong, and presenting the results as probabilities of pathology presence (abnormal findings) and probabilities of different disease categories. The practical goal was to provide diagnostic support to physicians during the diagnostic process.*

Keywords: *classification, endoscopic images, machine learning*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Владимир Петровић, ред. проф.

1. УВОД

Развој метода дубоког учења у последњој деценији значајно је унапредио анализу медицинских слика и отворио могућност за примену аутоматизованих система у клиничкој дијагностици. Једна од области у којој ови системи имају велики потенцијал јесте гастроентерологија, где ендоскопске процедуре, попут гастроскопије и колоноскопије, представљају основни дијагностички алат за визуелну процену слузнице дигестивног тракта. Иако ендоскопија омогућава рано откривање полипа, упалних процеса и других патолошких стања, анализа снимака је захтевна и подложна субјективним грешкама, што указује на потребу за развојем интелигентних система који би подржали лекаре у процесу дијагнозе, скраћујући време дијагностике, лечења, смањујући шансе могућих компликација и побољшавајући квалитет живота пацијената.

У досадашњим истраживањима класификације ендоскопских снимака, посебно на скуповима података HyperKvasir и KvasirV2, доминирају приступи засновани на дубоким конволутивним неуронским мрежама и њиховим ансамблима. Рад *EndoNet* [6] представља један од напредних приступа, заснован на вишестепеној фузији карактеристика добијених из више CNN архитектура (Inception, Xception и ResNet101), уз примену техника редукције и селекције карактеристика као што су NNMF и mRMR. На основу експеримената на HyperKvasir скупу (10 уравнотежених класа), аутори су постигли укупну тачност од 98%.

У раду енгл. "*A triple-pronged approach for ulcerative colitis severity classification using multimodal, meta, and transformer-based learning*" [7], предложен је свеобухватан модел за класификацију степена тежине улцерозног колитиса, који комбинује мултимодалне моделе, енгл. few-shot meta learning и енгл. Vision Transformer (ViT) архитектуре. Овај приступ је, применом ансамбла више ViT модела, постигао 93% тачности и F1 скор од 93%, уз висок ниво интерпретабилности постигнут анализом SHAP метода.

Рад енгл. "*A New Approach for Gastrointestinal Tract Findings Detection and Classification Deep Learning-Based Hybrid Stacking Ensemble Models"* [8] представио је хибридни приступ заснован на енгл. stacking ансамблу дубоких неуронских мрежа за детекцију и класификацију налаза у гастроинтестиналном тракту. Аутори су применили статистички валидиран метод са стратификованом поделом података и свеобухватном евалуацијом уз примену више метрика (ACC, F1, MCC, ROC-AUC), при чему је постигнута тачност од 98% на HyperKvasir скупу.

Ипак, већина наведених радова ослања се на спајање више класа ради побољшања квантитативних резултата, што смањује клиничку применљивост и интерпретабилност.
За разлику од њих, у овом истраживању примењен је модел DINOv2 [2], на бази ендоскопским слика отвореног кода HyperKvasir [1], који омогућава учење репрезентација без надзора и показује већу робусност на варијације у осветљењу и текстури. Истраживање је организовано у два нивоа сложености: трокласна класификација (здраво, болесно, проблематично) и проширена класификација на 22 класе анатомских и патолошких структура.
Поред тога, евалуација је извршена и на сликама из другог извора тј. гастроскопским снимцима са Клиничко болничког центра Војводине (КБЦВ), чиме је испитана примењивост модела ван јавних скупова података и модел приближен реалним клиничким условима.

2. БАЗА ПОДАТАКА

За реализацију рада коришћен је база отвореног кода HyperKvasir [1] која садржи више од 110.000 слика, видеа и маски лабелираних/нелабелираних патологија и анатомских структура дигестивног тракта. Из скупа је изабран део са лабелираним сликама у видљивом спектру, а након уклањања недовољно заступљених класа, лат. *ileum* и енгл. *hemorrhoids,* формиран је уравнотежен скуп од 11.619 слика распоређених у 22 класе, Табела 1. Подела података извршена је стратификовано у односу 60:15:25 на скупове за обуку, валидацију и тестирање. Прва фаза представљала је класификацију слика у здраво, болесно и проблематично ткиво. Трећа класа је неопходна јер представља „остале" класе које нису ни патологије ни анатомске структуре, већ класе које представљају оцену квалитета припреме пацијента за преглед. Ове оцене су важне и неопходне, јер сам квалитет припреме значајно утиче на квалитет дијагностике. Тј. са техничке стране, у присуству артефаката услед лоше припреме пацијента, откривање и класификација патологије није толико поуздана. У другом кораку класификација се фокусира само на релевантне инстанце унутар сваке групе, чиме се постиже прецизнија детекција специфичних ентитета.

Табела 1: Списак класа и број узорака датим класама

Класа	Број слика
Barretts	41
Barretts-short-segment	53
BBPS-0-1	646
BBPS-2-3	1148
Cecum	1009
Dyed-lifted-polyps	1002
Dyed-resection-margins	989
Esophagitis-a	403
Esophagitis-b-d	260
Impacted-stool	131
Polyps	1000
Polyps-masks	1000
Pylorus	999
Retroflex rectum	391
Retroflex stomach	764
Ulcerative colitis grade-0-1	35
Ulcerative-colitis-grade-1	201
Ulcerative-colitis-grade-1-2	11
Ulcerative-colitis-grade-2	443
Ulcerative-colitis-grade-2-3	28
Ulcerative-colitis-grade-3	133
Z-line	932

3. МЕТОД

За решавање задатка примењен је енгл. transfer learning приступ са DINOv2-Base Vision Transformer (ViT) [2] моделом, који садржи 86 милиона параметара, као основом. Модел је коришћен као екстрактор карактеристика, при чему су финални вектори ембединга на CLS токену улаз у класификаторску главу. У првом моделу класификатор је обучен за три класе, док је у другом моделу извршено фино подешавање за 22 класе.
DINOv2 је визуелни трансформер (ViT), који уместо класичних конволуција користи механизам енгл. self-attention. Слика се дели на енгл. patch-еве величине 16×16 пиксела, који се линеарно пројектују у вектор димензије 768. Секвенца вектора се пропушта кроз 12 трансформер блокова са по 12 глава пажње и скривеним слојем величине 3072, а CLS токен представља глобалну репрезентацију слике која се прослеђује класификаторској глави.
Класификаторска глава модела за класификацију патологија је имплементирана као енгл. fully connected network са следећом структуром: улазни слој 768 неурона, скривени слој 256 неурона са ReLU активацијом, енгл. Dropout слој [4] вредности 0.5 и излазни слој са бројем неурона једнаким броју класа. Класификациона глава трокласног модела садржала је слој за нормализацију и линеарни слој.
Обрада података за оба модела изведена је применом техника обраде слике, као и аугментације ради побољшања робусности модела. Слике су стандардизоване према статистикама ImageNet скупа и промењене на резолуцију 224×224 пиксела. Употребљен је енгл. WeightedRandomSampler како би се компензовала неуравнотеженост између класа.
Сви експерименти реализовани су у окружењу енгл. PyTorch, а перформансе оба модела праћене су дискутованим метрикама, што је омогућило детаљну анализу тачности по класама.
Трокласни модел је тренирана оптимизатором енгл. AdamW [3] са почетном кораком учења 1×10^{-5}, енгл. weight decay параметром 10^{-4} и функцијом губитка енгл. CrossEntropyLoss. Тренинг је изведен током 20 епоха уз енгл. early stopping стратегију након пет епоха без побољшања F1 скор на валидационом скупу.
Тренинг модела за класификацију патологија тренирана је такође оптимизатором енгл. AdamW са почетном стопом учења 3×10^{-5} и енгл. weight decay параметром 5×10^{-3}. Класификатор је тренирана током 12 епоха, док је функција губитка и овде била CrossEntropyLoss.

4. ЕВАЛУАЦИОНЕ МЕТРИКЕ

Квалитет развијеног модела за класификацију ендоскопских слика оцењен је коришћењем стандардних метрика за вишекласну класификацију. Све метрике су рачунате по класама, а затим приказане и као тежински просек у односу на број узорака сваке класе.

Тачност представља удео исправно класификованих узорака у односу на укупан број узорака:

$$\text{ТАЧНОСТ} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

где су:
TP – број исправних позитивних класификација (енгл. true positives)
TN – број исправних негативних класификација (енгл. true negatives)
FP – број лажно позитивних класификација (енгл. false positives)
FN – број лажно негативних класификација (енгл. false negatives)

Прецизност мери колико су од свих узорака које је модел означио као позитивне заиста позитивни:

$$\text{ПРЕЦИЗНОСТ} = \frac{TP}{TP+FP} \quad (2)$$

Одзив (енгл. Sensitivity или енгл. True Positive Rate) показује колики део стварно позитивних узорака модел успешно препознаје:

$$\text{ОДЗИВ} = \frac{TP}{TP+FN} \quad (3)$$

F1 скор представља хармонијску средину између прецизности и одзива и користи се као уравнотежена мера перформанси модела:

$$\text{F1 \_СКОР} = \frac{\text{ПРЕЦИЗНОСТ}\times\text{ОЗИВ}}{\text{ПРЕЦИЗНОСТ}+\text{ОДЗИВ}} \times 2 \quad (4)$$

Конфузиона матрица приказује дистрибуцију предикција модела по класама и омогућава идентификацију међукласних грешака. За вишекласну класификацију матрица димензија K × K садржи вредности:

$$C_{ij} - \text{„број слика класе } i \text{ класификованих као класа } j$$

5. РЕЗУЛТАТИ

У првој фази, у којој је циљ био разликовање здравог, болесног и проблематичног ткива, модел је постигао високу стабилност и тачност класификације. На тест скупу је остварена укупна тачност од 98% и макро F1 мера од 98%, што указује на високу способност генерализације. Највећи број погрешних класификација јављао се између класа „болесно“ и „проблематично“, што је очекивано због морфолошке сличности и присуства артефаката у појединим снимцима.

У другој фази, извршена је класификација на 22 класе анатомских и патолошких региона. Модел је постигао тачност од 91% и тежински F1 скор од 91% на тест скупу. Највећи број мешања класа дешава се у класама степена улцерозног колитиса, где прелазне класе *ulcerative-colitis-grade-0-1, ulcerative-colitis-grade-1-2* и *ulcerative-colitis-grade-2-3* често буду класификоване као „пуне класе“ *ulcerative-colitis-grade-1, ulcerative-colitis-grade-2* и *ulcerative-colitis-grade-3*. Ово може бити обашњено тиме што је порекло „прелазних класа“ компромис немогућности консензуса од стране стручњака.

Примена модела спроведена је на снимцима добијеним у сарадњи са Клиничко болничким центром Војводине (КБЦВ), који нису били део скупа за обуку, Слике 1 и 2. За евалуацију коришћене су четири излабелиране класе (укупно девет слика). У енгл. *zero-shot* тестирању, трокласни модел је успешно препознао све примере у првој фази са 100% тачношћу, док је у другој фази остварио високу сагласност између предвиђених и стварних класа, нарочито код колитиса и ретрофлексираног желуца, Табела 2. Ови резултати потврђују добру генерализацију система и његову применљивост на податке из различитих извора.

Слика 1: Пример слике класе улцерозни колитис 3 из КБЦВ, класификоване у класу улцерозни колитис 2

Слика 2: Пример слике класе полип из КБЦВ, успешно класификоване

Табела 2:Резултати примене модела на сликама КБЦВ

Истинита класа	Први модел	Други модел
Ulcerative-colitis-grade-3	болесно	Ulcerative-colitis-grade-3
Ulcerative-colitis-grade-3	болесно	Ulcerative-colitis-grade-2
Ulcerative-colitis-grade-2	болесно	Ulcerative-colitis-grade-2
Retroflex-stomach	здраво	Retroflex-stomach
Retroflex-stomach	здраво	Retroflex-stomach
Polyps	болесно	Pylorus
Polyps	болесно	Dyed-resection-margins

Polyps/retroflex-stomach	болесно	Retroflex-stomach
Polyps	болесно	Polyps

6. ЗАКЉУЧАК

У овом раду представљен је систем за аутоматску класификацију ендоскопских слика гастроинтестиналног тракта заснован на дотредирању DINOv2 [2] модела дубоког учења. Постигнути резултати показују да DINOv2 [2] архитектура, иако првобитно развијена за општу визуелну анализу, уз примену енгл. transfer learning-а може бити веома ефикасна и у медицинском домену. У поређењу са класичним конволутивним мрежама, као што су ResNet и EfficientNet, DINOv2 [2] показује већу осетљивост на фине текстуралне и морфолошке разлике, што је посебно значајно код гастроентеролошких снимака где су промене често суптилне. Високе вредности тачности и F1 мере у трокласној класификацији потврђују стабилност модела, док резултати у проширеној класификацији показују обећавајуће резултате на којима има места за даље истраживање. Ипак, упркос ограничењима услед неуравнотежености класа и недовољног броја узорака за поједине категорије, систем је задржао робусност и способност да правилно разликује морфолошки сличне класе. Практична примена на стварним узорцима из КБЦВ додатно потврђује потенцијал овог приступа у клиничкој пракси. Добри zero-shot резултати могу се приписати чињеници да су снимци из обе базе настали на сличним ендоскопским уређајима произвођача медицинске опреме Olympus, али и способности DINOv2 [2] модела да препозна глобалне визуелне структуре, а не само локалне шаблоне. Истраживање је показало да је комбинација енгл. self-supervised визуелних репрезентација и енгл. transfer learning приступа ефикасна стратегија за анализу медицинских слика у условима ограниченог броја означених података. Постигнути резултати, са тачношћу до 98% у трокласној и 91% у вишекласној класификацији, потврђују применљивост предложеног модела у клиничком контексту, при чему систем показује способност прецизног препознавања различитих анатомских региона и патолошких промена, као и отпорност на варијације у осветљењу, углу и контрасту снимака. Планирани наставак истраживања укључује увођење DINOv3 [5] архитектуре, проширење скупа података у сарадњи са Клиником за гастроентерологију и хепатологију и развој енгл. multitask модела који би истовремено вршили класификацију и сегментацију лезија, што би додатно повећало клиничку вредност система. Будући рад биће усмерен на проширење скупа података, како у смислу броја слика, тако и у погледу обухватања већег броја патологија и анатомских обележја које систем треба да класификује. Планира се и примена енгл. explainable AI техника, како би се крајњем кориснику обезбедила већа поузданост и транспарентност нашег производа. Такође, биће размотрена интеграција сегментационих метода које ће омогућити просторну локализацију лезија и/или региона од интереса. Развијени модел представља корак ка практичној примени система вештачке интелигенције у ендоскопској дијагностици, доприносећи унапређењу квалитета и ефикасности клиничке праксе.

7. ЛИТЕРАТУРА

[1] Borgli, H., Thambawita, V., Smedsrud, P.H. *et al. HyperKvasir*, a comprehensive multi-class image and video dataset for gastrointestinal endoscopy. *Sci Data* **7**, 283 (2020). https://doi.org/10.1038/s41597-020-00622-y

[2] Oquab, Maxime, et al. "Dinov2: Learning robust visual features without supervision." *arXiv preprint arXiv:2304.07193* (2023).

[3] Loshchilov, Ilya, and Frank Hutter. "Decoupled weight decay regularization." *arXiv preprint arXiv:1711.05101* (2017).

[4] Srivastava, Nitish, et al. "Dropout: A Simple Way to Prevent Neural Networks from Overfitting." Journal of Machine Learning Research 15.1 (2014): 1929–1958.

[5] Siméoni, Oriane & Vo, Van Huy & Seitzer, Maximilian & Baldassarre, Federico & Oquab, Maxime & Jose, Cijo & Khalidov, Vasil & Szafraniec, Marc & Yi, Seungeun & Ramamonjisoa, Michaël & Massa, Francisco & Haziza, Daniel & Wehrstedt, Luca & Wang, Jianyuan & Darcet, Timothée & Moutakanni, Théo & Sentana, Leonel & Roberts, Claire & Vedaldi, Andrea & Bojanowski, Piotr. (2025). DINOv3. 10.48550/arXiv.2508.10104.

DOI: https://doi.org/10.24867/34BE11Krunic

DOI: https://doi.org/10.24867/34BE11Krunic

DOI: https://doi.org/10.24867/34BE11Krunic

Кратка биографија:

Светлана Крунић рођен је у Врбасу 2001. год. Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства – Обрада сигнала одбранила је 2025.год.
Контакт: skrunic43@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.85
ДОИ: https://doi.org/10.24867/34BE13Davinic

Алгоритамски модел хемијских реакција и његова примена у едукативној видео игри

Algorithmic model of chemical reactions and its application in an educational video game

Богдан Давинић, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *Овај рад представља развој алгоритамског модела за валидирање хемијских реакција у реалном времену у оквиру едукативне видео-игре. Модел формализује правила комбиновања елемената на основу валентности и електронегативности, уз аутоматизовано генерисање формуле и визуелног приказа једињења. Систем је имплементиран у окружењу Unreal Engine и омогућава интерактивну проверу реакција кроз повратну информацију кориснику. Рад повезује алгоритамску логику са визуелним и педагошким принципима у циљу подршке учењу кроз игру.*

Кључне речи (три до пет): *алгоритам, хемијске реакције, валидација, едукативна игра, визуелизација*

Abstract – *This paper presents the development of an algorithmic model for real-time validation of chemical reactions within an educational video game. The model formalizes the rules of element combination based on valence and electronegativity, including automated formula generation and visual compound rendering. Implemented in the Unreal Engine environment, the system enables interactive reaction validation through user feedback. The work integrates algorithmic logic with visual and pedagogical principles to support learning through gameplay.*

Keywords: (three to five): *algorithm, chemical reactions, validation, educational game, visualization*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Драган Иветић, ред. проф.

1. УВОД

Постојећа дигитална решења за подучавање хемије најчешће су конципирана као квизови, једноставне симулације лабораторијских експеримената или визуелни прикази елемената. Код таквих система изостаје формално дефинисана логика међусобне интеракције хемијских елемената. У тим система правила хемијских реакција често нису формално моделована, већ представљају илустративне или наративне примере. Услед непостојања адекватног алата јавља се потреба за прецизним дефинисањем хемијских процеса и увођењем јасних правила интеракције у игри, како би корисник кроз игру усвојио логику хемијских реакција.

Основни проблем којим се овај рад бави јесте недостатак формализованог модела за валидацију хемијских реакција у реалном времену унутар едукативне видео-игре. Било је потребно дефинисати начин на који се комбиновањем унетих елемената и њихових валенци, електронегативности и других особина може генерисати резултат који је у складу са хемијским принципима. На визуелном нивоу требало је приказати ток реакције и формирање једињења у облику који је интерактиван и разумљив кориснику.

Са аспекта техничке реализације, проблем обраде подразумева пројектовање структура података и алгоритама који могу да опишу елементе, њихове особине и правила њихових интеракција. Стога је било потребно развити механизам који ће, у складу са хемијским принципима, генерисати исправан резултат реакције и паралелно обезбедити прегледан визуелни приказ тока реакције и формирања једињења.

Овај рад се фокусира на бинарне реакције између два елемента, при чему је развијен модел који омогућава њихову валидацију и визуелизацију унутар окружења „Unreal Engine“. У оквиру тог модела испитује се начин на који се логика хемијске реакције може интегрисати у механику игре, а да се не наруши њена интерактивна или визуелна структура. Резултати рада треба да омогуће основу за проширење система на сложеније типове реакција и повезивање са педагошким приступима учења кроз игру.

Идеја рада није да се створи образовни алат у педагошком смислу, већ да се технички испита могућност алгоритамске валидације хемијских процеса и њиховог обједињавања са визуелним приказом унутар једног интегрисаног система. да се развије и имплементира алгоритамски модел који формално дефинише и проверава исправност хемијских реакција у реалном времену, заснован на валентним правилима и електронегативности елемената, и да се тај модел интегрише у интерактивно окружење образовне видео-игре. На тај начин, рад

повезује техничку тачност хемијских процеса са визуелним и интерактивним приказом у едукативном контексту.

2. МЕТОД

Да би се тај циљ остварио, неопходно је формулисати јасне техничке задатке и међуциљеве. Први корак обухвата дефинисање структура података за представљање хемијских елемената и једињења, при чему те структуре морају омогућити једноставно проширење и аутоматизовану проверу односа између елемената. Следећи корак је развој алгоритма за валидацију реакција који проверава комбинације на основу валентних правила, електронегативности и хемијске стабилности. Резултат валидације представља улаз за визуелни модул који генерише приказ формираног једињења и обезбеђује повратну информацију кориснику.

Трећи задатак односи се на интеграцију ових компонената у јединствену архитектуру у оквиру окружења „Unreal Engine“. Тиме се омогућава да систем функционише у реалном времену, при чему свака корисничка интеракција активира логичку проверу и одговарајућу визуелну реакцију. Посебна пажња посвећује се модуларности како би се систем могао проширити додавањем нових типова реакција, сложенијих једињења или различитих механизама визуелизације.

Модел података у систему представља основу техничке архитектуре и дефинише начин на који су хемијски ентитети записани, обрађени и приказани кориснику. Његова функција је да обезбеди конзистентан формат за размену информација између модула задужених за валидацију реакција, генерисање назива и визуелну презентацију резултата. Све структуре имплементиране су као „USTRUCT“ типови у окружењу „Unreal Engine“, чиме се постиже интеграција са „Blueprint“ системом и омогућава проширење функционалности без нарушавања постојећег кода.

„FElement“ је основна јединица модела података и описује појединачне хемијске елементе. Његови атрибути укључују симбол и назив елемента, листу могућих валентних стања, припадност хемијској групи и боју која се користи у визуелном интерфејсу. Ова структура омогућава систему да сваки елемент тумачи као самосталан ентитет са јасно дефинисаним особинама које се могу анализирати, комбиновати и приказивати. Тако се успоставља веза између хемијских својстава и њиховог визуелног приказа, што доприноси транспарентности интеракције.

„FCompound“ моделује резултат комбиновања два или више елемената. Садржи податке о укљученим елементима, њиховом односу, типу везе, формули једињења и визуелним карактеристикама. Однос између елемената изражава се помоћу најмањег заједничког садржалаца њихових валенци, а атрибути као што су тип везе (јонска или ковалентна). Боја добијена пондерисањем компоненти омогућавају повезивање хемијског значења са визуелном репрезентацијом. „FCompound“ функционише као веза између алгоритма валидације и приказа резултата.

„FReactionResult“ обједињује исход реакције и служи као мост између логичког и интерактивног слоја система. Садржи показатеље успешности, формирано једињење када је реакција валидна, текстуалну поруку и додатне параметре попут енергије или стабилности. Ова структура обезбеђује стандардизован формат за све повратне информације, што омогућава да се сваки исход прецизно забележи и да корисник добије јасну повратну поруку.

Повезаност између ових структура обезбеђује јасан ток података: елементи описани у „FElement“ улазе у процес комбиновања, алгоритам на основу њихових особина креира „FCompound“, а резултат валидације се приказује преко „FReactionResult“. Оваква организација омогућава модуларност, јер сваки део система има дефинисану функцију и може се самостално проширити. Модел података тиме чини језгро техничке архитектуре и обезбеђује стабилну основу за алгоритме валидације, именовања и визуелне презентације.

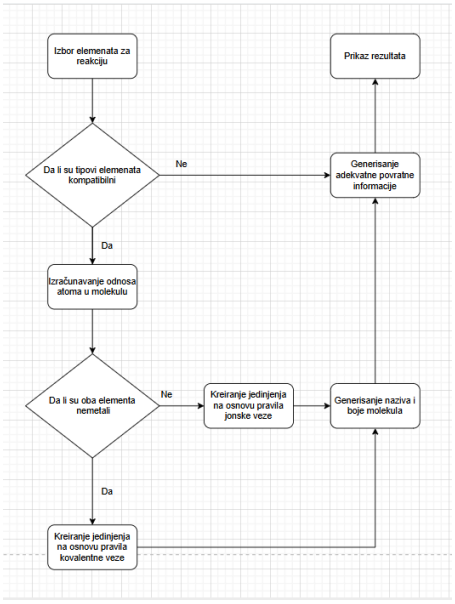
Алгоритам валидације представља функционално језгро система и проверава исправност сваке реакције. На основу параметара елемената, валенци, припадности хемијским групама и електронегативности, он утврђује да ли се може формирати стабилно једињење и како се дефинише однос између атома у формули. Тиме се обезбеђује доследно понашање и усклађеност са хемијским принципима, а корисник добија непосредну повратну информацију.

Валидација започиње преузимањем података из структура „FElement“ које корисник изабере. На основу типа елемената одређује се врста везе: комбинација метала и неметала резултује јонском везом, док комбинација два неметала даје ковалентну везу. Електронегативност се користи за дефинисање редоследа симбола у формули, елемент са мањом електронегативношћу налази се на првом месту. Следећа фаза валидације укључује анализу валентних стања учесника. Алгоритам пореди могуће вредности и рачуна најмањи заједнички садржалац како би одредио однос броја атома у једињењу; овај стехиометријски однос формира нумерички баланс реакције. Када се однос утврди, алгоритам конструише структуру „FCompound“ са свим потребним информацијама о формираном једињењу, укључујући тип везе, хемијску формулу и визуелне параметре.

У случају неуспешне реакције, када комбинација елемената не задовољава услове, систем генерише негативан резултат и поруку која објашњава узрок. Ови исходи се бележе у оквиру структуре „FReactionResult“, која служи као стандардизован излаз за све повратне информације. Тако процес валидације обезбеђује техничку конзистентност и јасну дидактичку структуру, јер сваки исход има функцију информисања и усмеравања корисника.

Алгоритам обухвата и специјалне случајеве: племените гасове и друге елементе без доступних

валентних стања, водоник и амонијак са специфичним везама или нереактивне комбинације. Имплементација алгоритма у „C++ “-у унутар окружења „Unreal Engine“ омогућава високу перформансу и јасну интеграцију са интерфејсом. Структуре података из модела обезбеђују ефикасну комуникацију између модула, док модуларна архитектура омогућава додавање нових правила без измене постојећег кода.



Слика 1. *Дијаграм тока валидације реакције*

Алгоритам именовања пролази кроз неколико фаза. Најпре анализира формулу и тип везе утврђену валидацијом. За јонска једињења примењују се правила по којима је први елемент метал, а други неметал; назив метала остаје непромењен, док назив неметала добија суфикс „-ид“. Ако метал има више валентних стања, његова валенца се приказује римским бројем у загради ради прецизности.

За ковалентна једињења, где учествују два неметална елемента, систем користи префиксе за означавање броја атома. Први елемент добија префикс само ако се појављује више пута, док други увек добија префикс, а завршава се суфиксом „-ид“ (нпр. CO_2 → угљен-диоксид). Редослед елемената у формули одређује се на основу електронегативности; елемент са већом електронегативношћу наводи се на другом месту. Овим приступом генерисани назив одражава хемијску структуру и логику реакције.

Систем такође садржи табелу изузетака за устаљене називе који не прате општа правила, као што су H_2O или NH_3. Ове вредности се проверавају пре примене алгоритма, чиме се обезбеђује усклађеност са научном праксом, уз задржавање флексибилности за образовни контекст. Формирање назива остварује се путем функција које препознају шаблон у хемијској формули и аутоматски додају одговарајуће префиксе и суфиксе. Функције попут „GetCovalentPrefix“ и „GetCovalentRootName“ обезбеђују стандардизацију и смањују могућност грешке. Резултат ових функција повезује се са структуром „FCompound“ и приказује кориснику одмах након валидације.

Имплементација је изведена у окружењу „Unreal Engine“ уз комбинацију „C++“ језика и „Blueprint“ скрипти. Такав приступ омогућава баланс између нисконивојске контроле над логиком и високог степена флексибилности у експериментима са визуелним сегментима система. Подаци о елементима и једињењима чувају се у „JSON“ формату, што обезбеђује ефикасно учитавање и једноставно проширивање базе. Радни ток вођен је алатом „Visual Studio“.

3. РЕЗУЛТАТИ

Интеграција визуелног и логичког слоја реализована је кроз систем догађаја „Unreal Engine“-а: свака акција корисника покреће проверу реакције и ажурира визуелни приказ у реалном времену. Функционалност система проверавана је кроз мануелна тестирања и анализу понашања током интерактивног играња. Иако формална евалуација ефикасности система није спроведена, систем је тестиран на стабилност и тачност, а уочене грешке и потешкоће исправљане су итеративно. На основу резултата тестирања дате су препоруке за будућа истраживања.[7]

Алгоритам валидације повезује основне хемијске параметре у логички ток који одређује исход реакције. Он функционише без спољашњих база и користи једноставне релације како би одржао равнотежу између тачности и брзине обраде. Тиме систем задржава научну конзистентност, а истовремено остаје довољно ефикасан за интерактивни рад. Током тестирања, алгоритам је показао стабилан одзив и тачне резултате при свакој поновљеној валидацији.

Интерфејс користи „event-driven“ приступ, где се елементи освежавају само када дође до промене стања. Овај принцип смањује број операција и обезбеђује одзивност без прекида тока. Време између корисничке акције и приказа резултата остало је у границама које омогућавају континуирану интеракцију. Ефикасно коришћење меморије додатно доприноси стабилности и предвидивом понашању система.

4. ДИСКУСИЈА

Структурна модуларност представља додатну предност. Модел података, алгоритам и визуелни слој функционишу као одвојене, али повезане целине, што омогућава проширење функционалности без нарушавања постојећег система. Ова флексибилност обезбеђује одрживост и олакшава примену система у будућим истраживањима или образовним контекстима.

Технички аспекти оптимизације усмерени су на постепено повећање изражајне моћи алгоритма без губитка детерминистичког понашања. Уместо потпуног редизајна, могу се увести параметарски слојеви који би омогућили реакције са додатним условима (нпр. температура или притисак) кроз ограничене нумеричке опсеге. Такав приступ би задржао стабилност основног модела, а омогућио

приказ ширег спектра хемијских појава. Паралелно с тим, архитектура система већ омогућава модуларно проширење ка вишекомпонентним реакцијама, где би свака нова компонента била засебан модул уместо део монолитне формуле. Тиме би се постигла скалабилност уз контролу перформанси.

Дакле, иако тренутни модел успешно валидира хемијске везе у формалном смислу, његова статичка природа представља ограничење у односу на реалне хемијске процесе. Кроз планирано увођење кинетичких принципа, брзине, енергије активације и каталитичких ефеката, систем би могао да постане динамички едукативни алат који објашњава не само „шта се дешава“, већ и „како и зашто се то дешава“ током хемијске реакције.

5. ЗАКЉУЧАК

Техничка структура система показује да је могуће остварити едукативни модел који у реалном времену спаја прецизност, стабилност и одзивност. Поуздан модел података, ефикасан алгоритам и кохерентан визуелни слој заједно чине основу за даљи развој система и његову педагошку примену, где техничка тачност постаје алат за разумевање, а не препрека учењу.

6. ЛИТЕРАТУРА

[1] P. Atkins, J. D. Paula, and J. Keeler, *Atkins' Physical Chemistry*, 12th ed. Oxford University Press, 2022. doi: 10.1093/hesc/9780198847816.001.0001.

[2] C. Ware, *Information visualization: perception for design*. in The Morgan Kaufmann series in interactive technologies. San Francisco, CA: Morgan Kaufman, 2004.

[3] B. Shneiderman and C. Plaisant, *Designing the user interface: strategies for effective human-computer interaction*, 4. ed. Boston, Mass. Munich: Pearson/Addison-Wesley, 2005.

[4] D. E. Knuth, “The art of computer programming. 1: Fundamental algorithms,” 2. ed., 34. [print.]., Reading, Mass: Addison-Wesley, 1995.

[5] R. C. Martin, J. Grenning, S. Brown, and K. Henney, *Clean Architecture: a craftsman's guide to software structure and design*. in Robert C. Martin series. Boston Columbus Indianapolis New York San Francisco Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo: Prentice Hall, 2018.

[6] R. E. Mayer, “TABLE I DEFINITIONSOF KEY TERMS Term Definition Example”.

[7] R. K. Yin, *Case study research and applications: design and methods*, Sixth edition. Los Angeles London New Delhi Singapore Washington DC Melbourne: SAGE, 2018.

Кратка биографија:

Богдан Давинић рођен је 2000. године у Крагујевцу. Основне студије завршио је на Факултету техничких наука Универзитета у Новом Саду, на смеру Рачунарство и аутоматика. Мастер студије наставио је на истом факултету, на смеру Мултимедија и развој игара.
Од 2023. године ангажован је као сарадник у настави, где доприноси практичној настави и раду са студентима.
Контакт: davinicbogdan@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.4
ДОИ: https://doi.org/10.24867/34BE15Dragicevic

Имплементација система за Over-the-Air ажурирање IoT уређаја

Implementation of an Over-the-Air update system for IoT devices

Марко Драгићевић, *Факултет техничких наука, Нови Сад*

Студијски програм – СОФТВЕРСКО ИНЖЕЊЕРСТВО И ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

Кратак садржај – *Рад се бави дизајном, архитектуром и имплементацијом система за сигурно и скалабилно Over-the-Air (OTA) ажурирање фирмвера, са фокусом на IoT уређаје базиране на ESP32 микроконтролеру. За реализацију серверског дела система користи се serverless приступ на Amazon Web Services (AWS) платформи, уз употребу сервиса као што су Lambda, S3, DynamoDB и IoT Core. Клијентска апликација на уређају имплементира робустан механизам за верификацију дигиталног потписа и сигуран процес инсталације. Администраторски кориснички интерфејс, који омогућава управљање верзијама и покретање процеса ажурирања, развијен је коришћењем React библиотеке.*
Кључне речи: *OTA, ESP32, AWS, Serverless, бежично ажурирање микроконтролера*

Abstract – *This thesis presents the design, architecture, and implementation of a comprehensive framework for secure and scalable Over-the-Air (OTA) firmware updates, focusing on IoT devices based on the ESP32 microcontroller. The server-side portion of the system leverages a serverless paradigm on the Amazon Web Services (AWS) platform, utilizing services such as Lambda, S3, DynamoDB, and IoT Core. The client-side application implements a robust mechanism for digital signature verification and a secure installation process. The administrative user interface, for managing versions and initiating the update process, is developed using the React framework.*

Keywords: *OTA, ESP32, AWS, Serverless, wireless updating microcontrollers*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Милан Видаковић, ред. проф.

1. УВОД

Експанзија Internet of Thing (IoT) донела је фундаментални изазов управљања софтвером на милионима географски дистрибуираних уређаја [1]. Једном распоређени, ови уређаји захтевају континуирано ажурирање ради додавања нових функционалности, побољшања перформанси, а пре свега, ради затварања критичних безбедносних пропуста. Без ефикасног механизма за даљинско ажурирање, IoT екосистеми постају рањиви, тешки за одржавање и брзо застаревају.

Рад се бави овим проблемом кроз дизајн и имплементацију комплетног система за сигурно и скалабилно Over-the-Air (OTA) [2,3] ажурирање фирмвера. Приступ је заснован на cloud-native принципима, где је целокупна серверска (backend) инфраструктура реализована на Amazon Web Services (AWS) платформи, пратећи serverless парадигму. Овакав приступ омогућава високу доступност и аутоматско скалирање, док истовремено минимизира оперативне трошкове.

Кључни фокус система је на вишеслојној безбедности. Решење имплементира сигурносни модел који укључује дигитално потписивање фирмвера на серверу и криптографску верификацију на самом уређају, чиме се гарантује аутентичност и интегритет софтвера. Рад такође истражује и демонстрира еволуцију комуникационог модела, од иницијалног приступа са периодичном провером (енгл. *polling*) до финалног, ефикаснијег решења које користи MQTT pub/sub протокол за нотификације у реалном времену. Циљ је да се прикаже целовит и практичан модел за развој робусног OTA система, применљив на реалне сценарије употребе, са ESP32 микроконтролером као циљном хардверском платформом.

2. АРХИТЕКТУРА СИСТЕМА

Развијени систем је пројектован као дистрибуирана, cloud-native апликација са јасно дефинисаним компонентама и одговорностима. Архитектура је осмишљена тако да задовољи кључне нефункционалне захтеве: скалабилност, сигурност, поузданост и ефикасност. У овом поглављу биће представљен дизајн сваке од кључних целина: backend инфраструктуре, модела података, комуникационог модела и софтверске архитектуре на самом уређају.

2.1. Cloud архитектура

За серверску инфраструктуру усвојена је serverless парадигма на Amazon Web Services (AWS) платформи. Овај избор елиминише потребу за традиционалним управљањем серверима, омогућавајући систему да

аутоматски скалира ресурсе у складу са тренутним оптерећењем, док се трошкови генеришу искључиво по потрошњи [4]. Архитектура обједињује неколико кључних AWS сервиса који раде у синергији како би пружили комплетну функционалност. Amazon API Gateway служи као сигурна улазна тачка за све HTTP захтеве; AWS Lambda функције садрже сву пословну логику; Amazon S3 се користи као издржљиво складиште за бинарне фајлове фирмвера; Amazon DynamoDB је NoSQL база података за метаподатке; док AWS IoT Core функционише као MQTT брокер за комуникацију у реалном времену.

2.2. Архитектура података

Моделирање података је кључан аспект система, директно утичући на његове перформансе и скалабилност. Уместо традиционалног релационог модела, за DynamoDB је примењен Single-Table Design. Овај напредни NoSQL приступ подразумева складиштење свих типова података у једној табели, користећи композитни примарни кључ (партициони кључ PK и сортирајући кључ SK) за ефикасно организовање и дохватање. Табела је дизајнирана да ефикасно одговори на кључне обрасце приступа (енгл. *access patterns*) и садржи два типа ставки: VERSION#... ставке, које су историјски записи о свакој верзији фирмвера, и GROUP#... ставке, које служе као „показивачи“ на тренутно активну верзију за одређену deployment групу. Ради оптимизације, GROUP ставке садрже денормализоване (дуплиране) податке, што омогућава да уређај добије све потребне информације у једном упиту, елиминишући потребу за операцијама налик на JOIN.

2.3. Архитектура комуникације

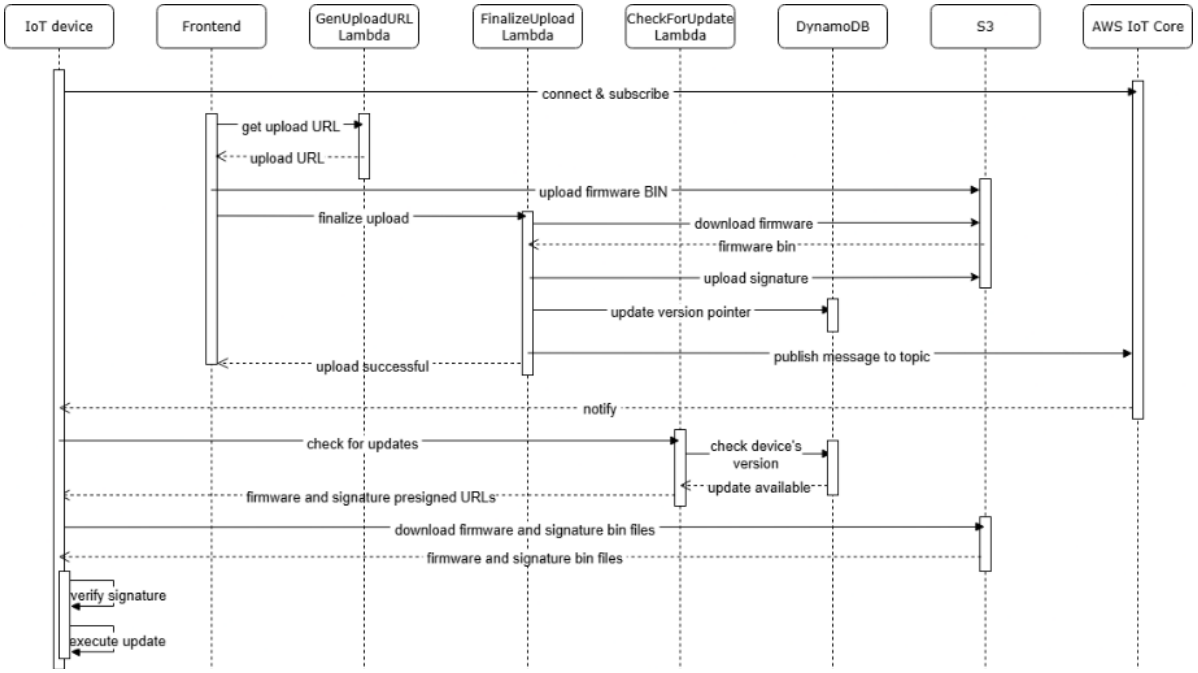
Архитектура комуникације је еволуирала током развоја. Иницијални polling модел [5], где уређај периодично шаље HTTP захтев серверу, показао је значајне недостатке: уносио је кашњење у детекцији ажурирања и генерисао велики број сувишних захтева. Због тога је финална архитектура усвојила MQTT pub/sub модел. Овај приступ, реализован преко AWS IoT Core сервиса, фундаментално мења динамику. Уређај успоставља једну дуготрајну, сигурну конекцију и претплаћује се на специфичну тему (енгл. *topic*). Backend систем објављује кратку нотификациону поруку само онда када је ново ажурирање заиста доступно. Ова архитектура вођена догађајима (event-driven architecture) је значајно ефикаснија и омогућава ажурирања у реалном времену.

2.4. Архитектура на уређају (Embedded)

Софтвер на ESP32 уређају је дизајниран са циљем да буде модуларан и робустан. Комплексност OTA процеса је енкапсулирана унутар самосталне Arduino библиотеке (SecureOtaUpdater), чиме се главна апликација поједностављује. Примењен је принцип инјекције зависности, где се кључни објекти (као WiFiClientSecure) креирају ван библиотеке и прослеђују јој, што повећава флексибилност. Архитектура се ослања на уграђени A/B партициони систем ESP32 меморије, који гарантује да уређај може да се опорави и врати на претходну верзију у случају неуспешног ажурирања.

3. ИМПЛЕМЕНТАЦИЈА СИСТЕМА

Ово поглавље детаљно описује техничку реализацију најважнијих делова система, са фокусом на имплементацију на серверском и клијентском делу.



Слика 1 - *Дијаграм секвенце*

На слици 1 је приказан обједињен дијаграм секвенце који илуструје комплетан животни циклус Over-the-Air (OTA) процеса, од иницијализације уређаја до финалне инсталације новог фирмвера.

3.1. Имплементација backend-а

Backend је реализован кроз комбинацију AWS CDK-а за дефинисање инфраструктуре и Python кода за пословну логику у Lambda функцијама. Коришћењем AWS CDK, целокупна инфраструктура је дефинисана у Python програмском језику. Ово омогућава аутоматизовано, поновљиво и верзионисано постављање свих cloud ресурса, укључујући S3 bucket, DynamoDB табелу, Lambda функције са прецизним IAM дозволама, и API Gateway ендпоинте. Овај приступ је у складу са модерним DevOps праксама и значајно смањује могућност људске грешке.

Процес објаве нове верзије фирмвера је оркестриран унутар FinalizeUpload Lambda функције. Кључни корак је дигитално потписивање. Да би се максимално заштитио приватни кључ, он се чува у AWS Secrets Manager сервису и дохвата се у тренутку извршавања. Lambda функција затим користи cryptography библиотеку за израчунавање ECDSA потписа [6], који уписује назад на S3. Након тога, ажурира DynamoDB табелу и објављује MQTT поруку на AWS IoT Core, чиме се процес завршава.

CheckForUpdate Lambda функција је оптимизована за брзину. Њен најважнији задатак је генерисање сигурних S3 Pre-signed URL-ова. Након што једним упитом ка DynamoDB-у утврди да је ажурирање потребно, она користи boto3 SDK да генерише временски ограничене URL-ове. Овај механизам омогућава уређају привремен приступ иначе потпуно приватним фајловима на S3, што је кључни сигурносни елемент.

3.2. Имплементација на ESP32 уређају

Имплементација на уређају је реализована у C++ језику кроз развијену Arduino библиотеку.

За сигурну конекцију са AWS IoT Core, уређај користи TLS протокол са аутентификацијом заснованом на X.509 сертификатима. WiFiClientSecure објекат се у тренутку повезивања конфигурише са Root CA сертификатом, сертификатом уређаја и приватним кључем уређаја. Овај процес гарантује да само ауторизовани уређаји могу да се повежу на систем и да је комуникација заштићена од прислушкивања. Имплементиран је и робустан механизам за аутоматско поновно повезивање у случају губитка везе.

Након пријема MQTT нотификације, уређај покреће процес ажурирања. Да би се уштедела RAM меморија, фирмвер се не преузима цео у меморију, већ се користи „streaming“ приступ. Преузима се у малим деловима (енгл. *chunks*), док се истовремено рачуна његов SHA-256 хеш и уписује у неактивну OTA партицију. Најважнији корак је верификација дигиталног потписа, која се врши помоћу mbedtls библиотеке. Уколико је потпис исправан, позива се Update.end(true) да би се ажурирање потврдило и променио показивач у otadata партицији; у супротном, позива се Update.end(false) и процес се сигурно прекида, остављајући уређај у претходном, функционалном стању.

3.3. Имплементација администраторског веб интерфејса

Да би се омогућило ефикасно и интуитивно управљање целокупним OTA системом, развијен је и администраторски веб интерфејс. Ова апликација представља централну контролну таблу и служи као „људски интерфејс“ за комплексну позадинску инфраструктуру, омогућавајући администратору да извршава све кључне операције без потребе за директним познавањем AWS сервиса или API-ја.

Frontend апликација је развијена као модерна Single-Page Application (SPA) коришћењем React библиотеке. Овај избор је направљен због React-ове архитектуре засноване на компонентама, која омогућава креирање комплексног корисничког интерфејса од малих, изолованих и поново употребљивих делова кода. Као SPA, апликација пружа брзо и флуидно корисничко искуство, где се све интеракције одвијају динамички, без поновног учитавања странице.

За хостовање и испоруку апликације примењена је стандардна, високо скалабилна пракса за статичке веб сајтове на AWS-у. Након процеса изградње (енгл. *build*), оптимизовани статички фајлови (HTML, CSS, JavaScript) се постављају у Amazon S3 bucket који је конфигурисан за хостовање статичких веб сајтова. Испред овог bucket-а постављен је Amazon CloudFront, глобална мрежа за испоруку садржаја (CDN). Оваква архитектура доноси две кључне предности: перформансе – кешира се садржај на локацијама широм света, што смањује време учитавања апликације за крајње кориснике, и безбедност – интеграцијом са AWS Certificate Manager (ACM), CloudFront омогућава да апликација буде доступна преко сигурне HTTPS везе, што је стандард за све модерне веб апликације.

Администраторски интерфејс омогућава извршавање свих неопходних радњи за управљање OTA процесом: преглед и управљање типовима уређаја, преглед верзија фирмвера, објављивање новог фирмвера.

4. ЗАКЉУЧАК

У раду је успешно пројектован и имплементиран комплетан систем за сигурно и скалабилно Over-the-Air (OTA) ажурирање фирмвера за IoT уређаје. Коришћењем serverless архитектуре на Amazon Web Services платформи, креирано је робусно решење које је ефикасно, скалабилно и лако за одржавање. Кључни допринос рада лежи у имплементацији вишеслојног сигурносног модела, са дигиталним потписивањем фирмвера (ECDSA) на серверу и криптографском верификацијом на ESP32 уређају, чиме је осигуран интегритет и аутентичност софтвера. Демонстрацијом преласка са традиционалног polling механизма на реактивни MQTT pub/sub модел, показана је супериорност архитектуре вођене догађајима у погледу ефикасности и брзине одзива. Развојем модуларне Arduino библиотеке и администраторског интерфејса, систем је заокружен као целовит производ

спреман за практичну примену. Могућности за даљи развој укључују увођење система за управљање корисницима (енгл. *multi-tenancy*) помоћу AWS Cognito сервиса, оптимизацију перформанси на уређају коришћењем двојезгарне обраде, као и имплементацију сигурносног „provisioning“ процеса за аутоматско додељивање јединствених идентитета уређајима.

5. ЛИТЕРАТУРА

[1] O. Mazhelis, E. Luoma и H. Warma, „Defining an internet-of-things ecosystem“, Conference on internet of things and smart spaces, 2012.

[2] S. Halder, A. Ghosal, M. Conti, „Secure over-the-air software updates in connected vehicles: A survey“, Computer Networks, 2020.

[3] M. Kubaščík, „OTA firmware updates on ESP32 based microcontrolers“, 2024 IEEE 17th International Scientific Conference on Informatics (Informatics), 2024

[4] I. Baldini, „Serverless computing: Current trends and open problems“, Research advances in cloud computing, 2017

[5] H. Takagi, „Queuing analysis of polling models“, ACM Computing Surveys (CSUR), 1988

[6] D. Toradmalle, „Prominence of ECDSA over RSA digital signature algorithm“, 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018

Кратка биографија:

Марко Драгићевић, рођен 10.02.2001. године у Лозници. Средње образовање стекао 2019. године, и исте године уписао Факултет техничких наука, смер Софтверско инжењерство и информационе технологије. Након завршених основних студија уписао је мастер студије на истом факултету, смер Софтверско инжењерство и информационе технологије. Положио је све испите предвиђене планом и програмом.
Контакт: mdragicevic58@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.738
ДОИ: https://doi.org/10.24867/34BE16Malinovic

Развој OCR модула за форензички алат Autopsy

Developing OCR Module for Autopsy Forensics Tool

Немања Малиновић, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У оквиру овог рада развијен је OCR модул интегрисан у форензички алат Autopsy ради аутоматске екстракције текста из слика током дигиталне форензичке истраге.*
Кључне речи (три до пет): *OCR, индексирање, препроцесирање, модул, Autopsy*

Abstract – *Within this thesis, an OCR module integrated into the forensic tool Autopsy was developed for automatic text extraction from images during digital forensics investigation.*
Keywords: (three to five): *OCR, indexing, preprocessing, module, Autopsy*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Стеван Гостојић, ред. проф.

1. УВОД

Савремене дигиталне истраге подразумевају анализу великих количина података различитих формата. Један од изазова је идентификација и екстракција текстуалних информација из слика, које нису у машински читљивом облику. У пракси, то отежава претрагу и повезивање релевантних информација, што може довести до споријег и мање ефикасног форензичког процеса. Недостатак модерних уграђених алата за препознавање текста у оквиру Autopsy окружења представља значајан изазов у свакодневном раду форензичара.

У овом раду проблем је решен развојем посебног модула за Autopsy који користи технологију оптичког препознавања карактера (OCR). Као основа примењен је Tesseract OCR, у комбинацији са техникама препроцесирања слике ради побољшања тачности препознавања. Развијени модул омогућава аутоматизовано извлачење текста, његово индексирање и интеграцију са постојећим системом за претрагу (keyword search) и анализу података унутар Autopsy окружења. Мотивација за овакав приступ произилази из потребе да се унапреди ефикасност дигиталних форензичких истрага. Екстракција текста из слика омогућава бржу идентификацију релевантних информација, смањује ризик од превиђања доказа и проширује могућност анализе. На тај начин, овај рад доприноси не само практичној примени у истражним процесима, већ и даљем развоју алата отвореног кода који се користе у дигиталној форензици.

Структура рада организована је на следећи начин. У другом поглављу описан је софтвер Autopsy и могућност његовог проширења кроз Java и Python модуле. Треће поглавље бави се технологијом оптичког препознавања карактера, индексирањем текста и прегледом других форензичких алата који обављају сличне функције. Четврто поглавље садржи спецификацију функционалних и нефункционалних захтева, као и дизајна развијеног софтвера. Пето поглавље обухвата кључне елементе његове имплементације. Шесто поглавље демонстрира примену модула у пракси, анализира резултате и пружа техничке коментаре о раду софтвера. На крају, закључно поглавље даје резиме извршених активности, упоређује предности и мане развијеног решења у односу на претходно описане методе и предлаже могућности за даље унапређење.

2. СТАЊЕ У ОБЛАСТИ

Autopsy [1] је један од најраспрострањенијих алата отвореног кода за дигиталну форензику. Првобитно развијен као графички интерфејс за The Sleuth Kit (TSK) библиотеку, а данас се користи као самосталан систем за анализу дигиталних доказа. Подржава анализу система датотека, преглед метаподатака, екстракцију артефаката из оперативних система, имејл клијената и интернет прегледача. Захваљујући архитектури заснованој на модуларности, Autopsy омогућава проширивање функционалности кроз додатке писане у Java и Python програмским језицима. Врсте модула у Autopsy алату су Ingest, Report и General модули.

2.1. Autopsy – Ingest модули

Ово су најважнији модули јер се извршавају током увоза и анализе података у случај. Постоје две подврсте. Data Source Ingest модули, раде над читавим извором података (нпр. Hash Lookup – упоређује све фајлове са познатим hash сетовима, keyword search – индексира цео извор ради претраге итд). Углавном се покрећу једном по додавању извора података у случај. File ingest модули, раде над појединачним фајловима (нпр. EXIF парсер – извлачи метаподатке из слика итд.) извршавају се појединачно у оквиру процеса учитавања. OCR модул који је тема овог рада је типа

File ingest модул. Анализира сваку слику, врши претпроцесирање и затим екстрахује текст и индексира их у бази података.

2.2. Java и Python модули

Једна од најважнијих предности Autopsy алата у контексту дигиталне форензике је његова висока проширивост. Java модули интегришу нове форензичке анализе директно у платформу, док Python модули омогућавају експерименталну или скриптовану обраду података, што је идеално за тестирање.

Java модули додају се одабиром опције Plugins унутар Autopsy алата где је потребно одабрати и инсталирати .nbm фајл модула који је претходно развијен.

Python модули [2] пружају већу флексибилност и брзину развоја софтвера, што их чини идеалним за истраживаче и академске пројекте. Лако их је написати за аутоматизацију одређених задатака као што су претрага, филтрирање, претварање или нормализација, извлачење метаподатака и интеграција са другим форензичким алатима. Autopsy платформа користи тзв. „Jython“ имплементацију Python програмског језика на Java виртуелној машини. То значи да Python код није изворно извршен од стране класичног Python интерпретера, већ се преводи у Java бајт-код унутар Autopsy платформе. Предности развијања ове врсте модула су брзина развијања и једноставност интеграције у окружење. Развијање је могуће у било ком текст едитору. Мане развијања ове врсте модула су ограничена подршка за Python библиотеке (максимално Python верзија 2.7.18) и потреба за познавањем Autopsy Java API-а.

2.3. Поређење са сличним алатима

У области дигиталне форензике постоји више алата који се користе за анализу података са компјутера, мобилних уређаја и других дигиталних медија. Сваки од ових алата има своје предности и мане, а избор зависи од потреба корисника, буџета и типа истраге.

EnCase је комерцијалан алат који представља индустријски стандард у дигиталној форензици. Омогућава дубинску анализу података, анализу имејлова, као и подршку за оптичко препознавање карактера из слика и докумената. Највећа предност је његова широко прихваћена употреба у судским процесима.

FTK (Forensic Toolkit) је још један комерцијални алат, познат по снажним могућностима за претрагу кључних речи и анализу дигиталних доказа са компјутера, мобилних уређаја и cloud извора. Издваја се по брзини индексирања и кориснички пријатељском интерфејсу, што омогућава ефикасно претраживање великих скупова података.

3. OCR И ИНДЕКСИРАЊЕ ТЕКСТА

3.1. Примена OCR технологија

Оптичко препознавање знакова (енг. optical character recognition – OCR) [3] представља технологију која омогућава претварање текста са слика или скенираних докумената у машински читљив и обрадив формат. Основна идеја јесте да се визуелни приказ знакова, који човек може да прочита, преведе у дигиталну репрезентацију погодну за даљу обраду, претраживање и чување у базама података. Овај процес је од кључне важности у контексту дигитализације докумената, јер омогућава елиминацију ручног прекуцавања и значајно убрзава приступ великој количини информација.

Иако је OCR данас изузетно напредовао, остају бројни изазови. Слаба резолуција, искошени документи, рукопис или текстови на језицима са сложеним писмима и даље представљају препреку. Међутим, трендови показују да интеграција OCR технологије са модерним техникама вештачке интелигенције [4] отварају нове могућности за високо прецизну, брзу и скалабилну обраду текста из визуелних извора.

Основни кораци у OCR процесу су претпроцесирање (нпр. припрема слике да буде погодна за даље анализе применом метода претпроцесирања као што су бинаризација, филтрирање шума, исправљање искошења, нормализација резолуције итд.), сегментација (подразумева раздвајање текста на мање целине, редове, речи и појединачне знакове и представља најизазовнији корак), препознавање знакова (шаблонско препознавање, статички модели, неуронске мреже и технике дубоког учења), постпроцесирање (циљ је исправљање грешака и унапређење квалитета добијеног текста користећи речнике како би се извршило упоређивање препознате речи са базом података познатих речи). Све наведене фазе заједно чине један логички ланац који омогућава да се визуелни садржај претвори у дигитални текст. Уколико једна од фаза не функционише како треба, коначни резултат ће бити значајно мање употребљив. Зато је OCR често посматран као интеграција више дисциплина као што су обрада слике, машинско учење и обраде природног језика.

Примене OCR технологија се проналази у дигитализацији књига и архива где се скениране књиге или новински чланци или историјски документи претварају у дигитални текст који се може претраживати. Претрага текста у административним системима налази примену OCR технологија за аутоматско извлачење релевантних података (нпр. број фактуре, датум, ПИБ компаније). Препознавање регистрационих таблица, банкарство, медицинска документација су још неки од области у којима се OCR користи.

Савремени системи за оптичко препознавање карактера значајно су напредовали последњих деценија и данас представљају један од кључних елемената у процесима дигитализације докумената, обраде текста и аутоматизације административних послова.

Tesseract OCR је један од најпознатијих OCR алата отвореног кода, развијен од стране компаније Google. Овај систем подржава велики број језика, укључујући и ћирилицу, што га чини погодним за примену у различитим културним и језичким контекстима. Једна од највећих предности је могућност тренирања сопствених модела, односно прилагођавање систему специфичним фонтовима или рукописима. Иако је у

прошлости био ограничен по питању тачности, интеграција са техникама дубоког учења и употребом вештачке интелигенције донела је значајно побољшање у прецизности препознавања знакова и карактера. Предност је што је алат бесплатан и отвореног кода.
Handwriting OCR (ICR – интелигентно препознавање карактера) је алат који је високо специјализован у препознавању рукописа. За разлику од штампаног текста, рукописи се карактеришу великом варијабилношћу у облику слова, неуједначеном величином и нагибом, као и честим спајањем карактера. Савремене технике дубоког учења и вештачке интелигенције омогућавају овом алату да буде међу бољима у области препознавања текста писаног рукописа. Мана је скупа лиценца.
Cloud OCR решења последњих година нуде такође висок ниво квалитета услуга. Најпознатији представници су Google Vision API, Microsoft Azure OCR и Amazon Textract. Ове услуге заснивају се на инфраструктури великих cloud провајдера, што им омогућава високу скалабилност, константно унапређивање модела и интеграцију са другим сервисима који користе вештачку интелигенцију. Ова решења елиминишу потребу за локалним хардверским ресурсима, што их чини погодним за организације које желе брзо и флексибилно увођење OCR-а без значајних почетних инвестиција.

3.2. Индексирање у форензичким алатима

Модерни форензички софтвери препознају да велики део доказа није у класичном текстуалном облику, већ унутар слика, PDF докумената и скенираних прилога. Управо због тога су у своје оквире интегрисали модуле за оптичко препознавање карактера, као и механизме за индексирање текста, чиме истражитељима и корисницима омогућавају брзо претраживање и анализу.
Инвертовани индекс је најчешће коришћена техника за индексирање и представља процес креирања помоћних структура података које омогућавају да се одређена реч или фраза пронађе унутар великог скупа докумената у врло кратком року.
Индексирање обухвата кораке као што су токенизација (раздвајање текста на токене или речи), нормализација (претварање свих речи у мали регистар), стеминг и лематизација (свођење речи на њихов корен или инфинитив), уклањање стоп речи (елиминација честих и мање значајних речи), генерисање мапе (креирање инвертованог индекса у форми: реч – [документ1,позиција1]).
Autopsy алат користи Apache Solr алат за претрагу који се надограђује на алат Lucene за индексирање и претрагу. Тиме је омогућена претрага по тексту који је претходно извучен из датотека.

4. СПЕЦИФИКАЦИЈА

4.1. Функционални захтеви

Функционални захтеви дефинишу шта систем треба да ради. Развијени модул омогућава корисницима одабир конфигурације модула (постављање параметара за подржане формате слика, језик и опције претпроцесирања), покретање OCR-а над сликама (извлачење текста из подржаних фајлова и складиштење резултата), преглед OCR логова (праћење статуса обраде и грешака приликом извршења модула) и претрагу извученог текста (брзо пронаћи конкретан текст или кључне речи).

4.2. Нефункционални захтеви

У контексту развијеног модула, ови захтеви се односе на перформансе, стабилност, употребљивост и интеграцију у постојећи софтверски оквир. Од модула се очекује да може ефикасно да обради велики број датотека у разумном времену, као и да пружи брзе и тачне резултате претраге над индексираним текстом. Интерфејс мора бити довољно једноставан да га форензичари могу користити без потребе за додатним техничким знањем, док интеграција у саму платформу мора бити без нарушавања других функционалности. Безбедност података је важна. Сав извучени текст мора се чувати унутар Autopsy база података како би се очувао интегритет доказа. Модул треба да буде развијен тако да омогући лако одржавање и проширивање, како би се накнадно могли додати нови алгоритми или технике без већих измена постојеће структуре.

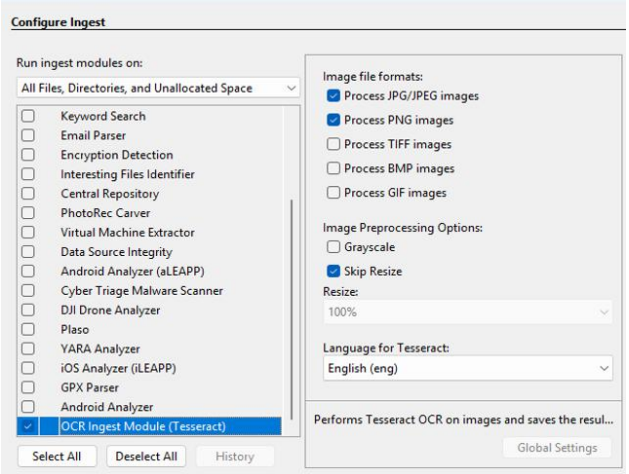
5. ИМПЛЕМЕНТАЦИЈА

Основна структура модула обухвата тзв. фабрику (енг. factory pattern) која је одговорна за креирање инстанце главне класе модула и његово повезивање са Autopsy платформом. Платформа захтева овај образац ради регистрације сваког новог модула. Главна класа модула садржи функционалности чувања подешавања, иницијализацију контекста и одређивање типова фајлова које модул обрађује на основу корисничког избора. Метода startup се позива пре обраде било ког фајла и служи за филтрирање по типу слике. Подржани формати слике су JPEG/JPG, PNG, TIFF, BMP и GIF.
ImageMagick алат отвореног кода се користи за технике претпроцесирања пре OCR процеса. Подржане технике су претварање слике у црно-белу слику (енг. grayscale) ради изоштравања читљивости текста и опција промене резолуције слике (енг. resize). Након обраде слика, модул покреће Tesseract OCR као спољашњи процес на процесираној слици. Излазни ток процеса садржи текст са слике. Уколико извршење није успешно, програм евидентира упозорење у логовима, али наставља са обрадом других фајлова, како би се обезбедила робусност целог модула. Након успешног извршења, излазни текст се декодира у стринг и резултат се анализира. Ако је пронађен текст, креира се артефакт који ће бити сачуван у Autopsy бази података ради касније индексирања.
Структура кода модула је организована у складу са принципима модуларности. Фабрика је одговорна за креирање инстанци модула и његово повезивање са Autopsy окружењем, главна класа управља логиком обраде, док је панел за подешавања издвојен као

засебна компонента која омогућава кориснику да конфигурише начин рада.

6. ДЕМОНСТРАЦИЈА

У овом одељку је кроз пример приказана употреба модула. На слици 1 приказан је изглед корисничког интерфејса који представља подешавања за модул.

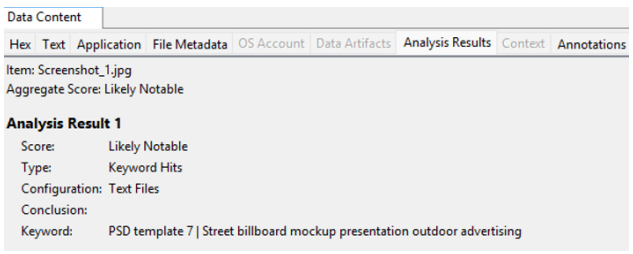


Слика 1. Кориснички интерфејс

Корисници бирају формат слика, опције претпроцесирања као и језик у којем је текст на слици описан. На слици 2 налази се слика жутог билборда са црним текстом на сивој металној конструкцији, са замућеном позадином. Из слике 2 ће бити извучен текст.

Слика 2. Слика из које се извлачи текст

Корисничка подешавања модула у овом примеру су одабир формата JPG и PNG, за језик је одабран енглески и коришћена је операција претварање слике у црно-белу. На слици 3 приказан је резултат извлачења текста.



Слика 3. Резултат анализе – Жути билборд

У овом случају извлачење текста је изузетно тачно. Сви читљиви текстуални елементи, осим стрелице (која није текст) и броја „7“ (који није на слици), су правилно препознати и спојени у један низ. Осим тих грешака, текст је изузетно тачно препознат и спојен, при чему су све речи правилно извучене упркос различитим фонтовима и позицијама.

7. ЗАКЉУЧАК

У овом раду анализирана је потреба за аутоматизованом обрадом и препознавањем текста из дигиталних слика у контексту форензичких истрага. Специфицирано решење и реализовани модул, доносе значајне предности у односу на слична постојећа решења. Пре свега, интеграција у Autopsy платформу омогућава да корисник из једног окружења управља целокупним процесом обраде и анализе слика, без потребе за додатним алатима. Ипак, имплементирани модул има и своја ограничења. OCR резултати могу бити непоуздани у случајевима када су слике ниске резолуције, имају сложену позадину или текст не одговара изабраном језику. Алат такође не може сам да изабере параметре за претходну обраду. Обрада великих или бројних слика захтева значајне хардверске ресурсе, посебно када су укључене операције претпроцесирања. Ово представља простор за побољшање у наредним верзијама. Ове надоградње учиниле би модул још кориснијим у форензичким истрагама и истраживању дигиталних доказа.

8. ЛИТЕРАТУРА

[1] Autopsy User Documentation [Online]. Доступно: https://sleuthkit.org/autopsy/docs/user-docs/4.18.0/ (приступљено септембар 2025.)

[2] Python module development [Online]. Доступно: https://sleuthkit.org/autopsy/docs/api-docs/4.19.3/mod_dev_page.html (приступљено септембар 2025.)

[3] OCR and Indexing [Online]. Доступно: https://support.filevine.com/hc/en-us/articles/360034968272-OCR-and-Indexing (приступљено септембар 2025.)

[4] C.M. Bishop, Pattern recognition and machine learning. New York, NY, USA: Springer, 2006.

Кратка биографија:

Немања Малиновић рођен је у Новом Саду 2000. год. Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства – дигитална форензика одбранио је 2025.год.
Контакт: malinovicnemanja6@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

UDK: 621.38
DOI: https://doi.org/10.24867/34BE17Tesic

УПРАВЉАЊЕ ТРОФАЗНОГ АСИНХРОНОГ МОТОРА ПРЕКО ПРОГРАМАБИЛНОГ ЛОГИЧКОГ КОНТРОЛЕРА ПУТЕМ *PROFINET* КОМУНИКАЦИЈЕ

CONTROLLING A THREE-PHASE ASYNCHRONOUS MOTOR VIA PROGRAMMABLE LOGIC CONTROLLER AND PROFINET COMMUNICATION

Владимир Тешић *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду приказана је симулација рада лифта. Комуникација између PLC-а, фреквентног регулатора и HMI панела. Приказана је и PID регулација за прецизно одређивање позиције лифта.*

Кључне речи: *Асинхрони електо мотор, програмабилни логички контролер, profinet комуникација, фреквентни регулатор, pid регулација, HMI панел.*

Abstract: *This paper presents a simulation of the operation of an elevator. Communication between the PLC, frequency converter and HMI panel. PID regulation for precise determination of the elevator position is also presented.*

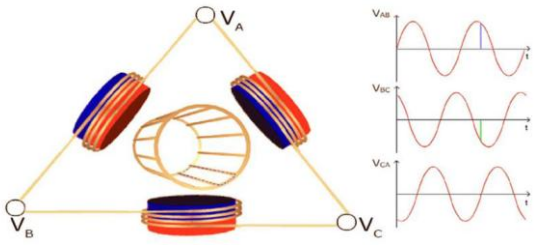
Keywords: *Asynchronous electric motor, programmable logic controller, Profinet communication, frequency regulator, PID regulation, HMI panel*

1. УВОД

Електро мотори су кључни део многих индустријских и свакодневних апликација широм света. За оптимално управљање асинхроних мотора, користе се фреквентни претварачи. У зависности од начина употребе, фреквентни претварач комуницира са програмабилним логичким контролером *PLC*-ом . *PLC* је индустријски рачунар који је дизајниран да поуздано управља аутоматизованим процесима. Комуникација између фреквентног регулатора и *PLC*-а је остварена преко *profineta*, индустријсог *etherneta.* Да би могли да видимо или мењамо одређене параметре, користи се *Human Machine Interface (HMI*).

2. АСИНХРОНИ ЕЛЕКТРО МОТОРИ

Трофазне асинхроне машине су најчешће коришћене електричне машине у многим гранама индустрије. Асинхроне машине имају 2 групе делова: статор и ротор. Статор (слика 1.) се састоји од: статорског намотаја, магнетног кола и кућишта. Када се на статор поставе три намотаја сваки са више навојака просторно померена за по 120° и када се кроз њих пропусте синусоидне струје истих амплитуда и фреквенција али временски померене за по трећину периоде (фазни померај је по 120°), магнетопобудне силе ових намотаја ће оформити обртно магнетно поље. Ротор се састоји од: роторског намотаја, вратила и вентилатора за хлађење. Обртно магнетно поље је (у идеалном случају) по унутрашњем обиму статора (а тиме и по обиму зазора и по спољашњем обиму ротора) просторно расподељено по синусном закону тако да формира магнетне полове.



Слика 1. Структура статора [2]

3. ФРЕКВЕНТНИ ПРЕТВАРАЧИ

Фреквентни претварачи играју кључну улогу у претварању једносмерне струје (*DC*) у наизменичну струју (*AC*). Фреквентни претварачи *VFD* (енг. *Variable frequency drive*) је врста контролера, који покреће електро мотор мењањем фреквенције. Фреквенција је директно повезана са брзином мотора (обртаји у минуту). Што је фреквенција већа, већи су и обртаји.

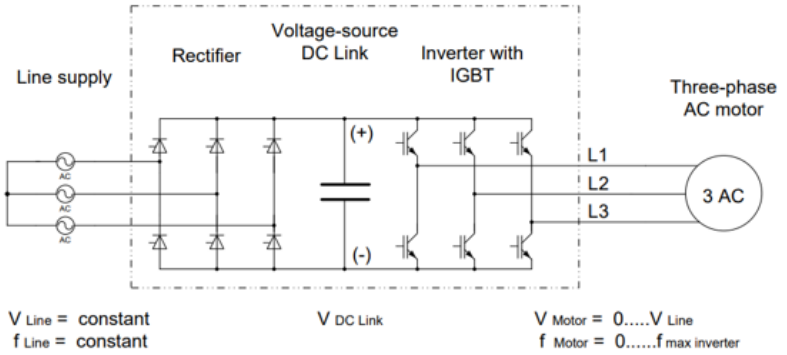
3.1. *Принцип рада*

Исправљач производи константни једносмерни напон *VDCLink*, тј. напон *DC* линка, који се исправља кондензаторима (слика 2.). Двостепени *IGBT* (енг. *IGBT = Insulated Gate Bipolar Transistor*) инвертор на излазној страни претвара напон *DC* линка у трофазни систем са променљивим напоном и променљивом фреквенцијом. Овај процес функционише по принципу S*PWM (енг. Sine Pulse Width Modulation*) модулације ширине импулса.

.

НАПОМЕНА:

Овај рад проистекао је из мастер рада чији ментор је био др Владимир Рајс, ванр. проф.



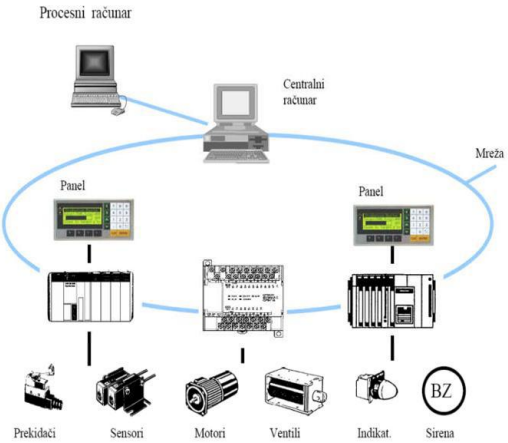
Слика 2. *Унутрашња шема претварача [2]*

4. ПРОГРАМАБИЛНИ ЛОГИЧКИ КОНТРОЛЕРИ

Програмабилни логички контролери су индустријски рачунари, са различитим улазима и излазима, који се користе за контролу и надгледање индустријске опреме на основу прилагођеног програмирања.

4.1. Улазни и излазни уређаји

Улазни уређаји чије сигнале прихвата *PLC*, могу бити аналогни или дигитални. Дигитални сигнали могу имати само стање укључено или искључено. Аналогни сигнали дају вредност од 0 до 10*V* или од 4 до 20 *mA*. Излазни уређаји на основу програма и стања на улазима, могу бити релеји, контактори, електромагнетни вентили, и други уређаји (слика 3).



Слика 3. *Улазни и излазни уређаји [2]*

5. *HUMAN-MACHINE INTERFACE HMI*

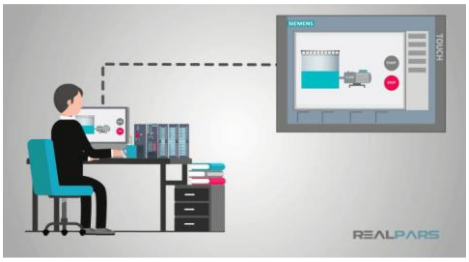
Human-Machine Interface HMI (eng. Интерфејс, комуникација између човека и машине) је контролна табла која повезује човека са машином.

У индустрији, HMI се могу користити за:

- Визуелно приказивање података
- Праћење времена производње
- Надгледање учинка у производњи
- Праћење улаза и излаза машина и још много тога.

5.1. Уобичајена употреба *HMI* уређаја

HMI комуницирају са *PLC* -овима и са улазно/излазним сензорима (слика 4.), како би се приказало стање сензора на екрану. *HMI* се могу користити за праћење и надгледање индустријских операција, као што су: искључивање машина, повећање/смањење брзине, мењање параметара машине и други



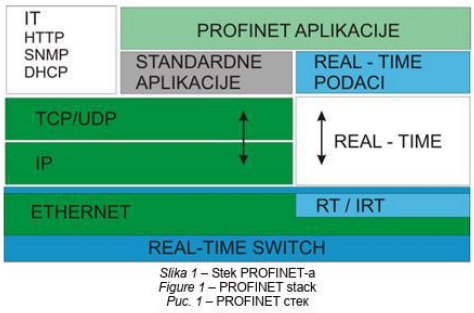
Слика 4. *HMI уређај [3].*

6. *PROFINET*

PROFINET је отворено индустријско *Ethernet* решење засновано на међународним стандардима. То је комуникациони протокол дизајниран за размену података између контролера и уређаја у аутоматизованом окружењу. Представљен је почетком 2000-их и најприхваћеније је индустријско *Ethernet* решење.

6.1. *Profinet* стандард

Profinet је стандардизован *IEC 61158* и *IEC 61784* стандардима. Карактеристика овог протокола омогућава коришћење *UDP/IP* (слика 5) протокола као протокола вишег нивоа за захтеве размене података. Паралелно са *UDP/IP* (*UDP– USER DATAGRAM PROTOCOL*) комуникацијом, циклична измена података у *profinet*-у базирана је на флексибилношћу и брзини у концепту реалног времена. Комуникација у реалном времену се одвија преко истог кабла за све апликације



Slika 1 – Stek PROFINET-a
Figure 1 – PROFINET stack
Рис. 1 – PROFINET стек

Слика 5. *Profinet* апликације [1]

Постоје 2 верзије *PROFINET-a*

- *Component Based Automation (PROFINET CBA)*
- *Input / Output (PROFINET IO)*

Док се *PROFINET IO* фокусира на размену података програмабилних контролера, *PROFINET CBA* се фокусира на дистрибуиране системе аутоматизације. *PROFINET IO* је веома сличан *PROFIBUS®-y* на *Ethernet*-у. Док *PROFIBUS* користи цикличну комуникацију за размену података са програмабилним контролерима максималном брзином од 12*Mbps*, *PROFINET IO* користи циклични пренос података за размену података са програмабилним контролерима преко *Ethernet-a*.

6.2. *Profinet* умрежавање

Пре него што *PROFINET IO* крену комуницирати са *PROFINET IO* контролером, имена морају бити додељена свим партнерима. *PROFINET* контролер може да приступи уређају само када му се дода име и *IP (Ipv4)* адреса које ће се налазити на уређају.

7. *SIEMENS STARTER*

Програмски пакет *Starter* се користи за параметризацију и пуштање у погон претварача *Siemens.*

7.1 Садржај програма *Starter*

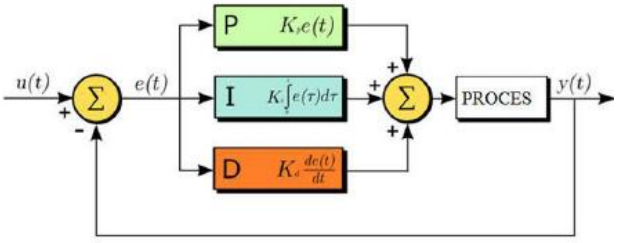
Starter се састоји од: Пројектног навигатора, радне површине, *toolbar-a,* контролни панел и експертне листе. Комуникација између рачунара и фреквентног регулатора, одвија се преко *usb*. Да би фреквентни регулатор могао да функционише, потребно је да се унесу основни параметри мотора: струја, напон, фактор, снага, брзина обртаја. Након успешно унетих параметара мотора, потребно је урадити стационарана и ротациона снимања, како би изачунали отпор ротора, индуктивност и роторову позицију.

7.2 *Profinet* комуникација

Да бисмо лакше управљали мотором, користимо *profinet* комуникацију. Тиме можемо доста брже и ефикасније да управљамо мотором. Подаци се шаљу од *drive-a* до *PLC-a* и обратно у пакетима. Сваки пакет је 16 бита, тј један *word*. Први пакет за примање је увек контролна реч, односно команде од *PLC-a,* остале речи су задата брзина, рампе, обртни моменти и слично. Први пакет за слање порука је статусна реч, затим иду стварна брзина, струја, обртни моменат и слично.

8. *PID* РЕГУЛАТОР

Пропорционално-интегрално-деривативно (*PID*) (слика 6.) управљање је најчешћи алгоритам управљања који се користи у индустрији и универзално је прихваћен у индустријској контроли. *PID* регулатор има три подесива параметра: појачање *Kp*, интегралну временску константу *Ti* и диференцијалну константу *Td*. Присуство пропорционалног, интегралног и диференцијалног дејства у овом регулатору омогућава добијање добрих перформанси система као што су: стабилност, брзина реаговања и тачност рада (Формула 1).



Слика 6. *PID регулатор [2]*

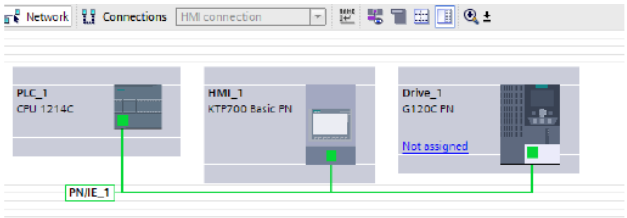
$$u(t) = Kp + Ki\int_0^t e(t)dt + Kd\frac{de(t)}{dt} = Kp\left(e(t) + \frac{1}{Ti}\int_0^t e(t)dt + Td\frac{de(t)}{dt}\right) \quad (1)$$

9. *ПРОГРАМИРАЊЕ SIEMENS TIA PORTAL*

Програмско окружење за рад са *Siemens*-овим *PLC*-овима серије *S7-1200* зове се *Totally Integrated Automation Portal (TIA) Portal*. То је апликација која служи за писање, измену и надгледање програма.

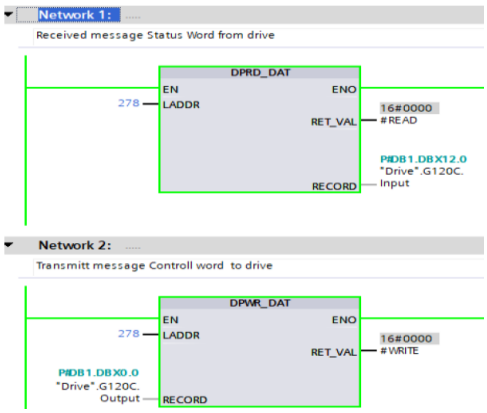
9.1. Хардверска конфигурација

У хардверској конфигурацији (слика 7) се додаје адреса и име уређајима. Сваки уређај треба да има јединствено име и адресу на истом *subnet-u.*



Слика 7. *Хардверска конфигурација*

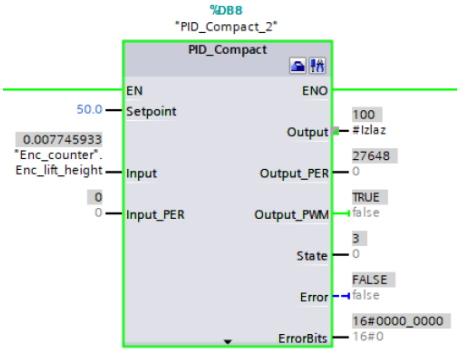
9.2. Слање и примање података



Слика 8. *Слање и примање података*

У поље *LADDR* (слика 8.) додајемо адресу. Правимо 2 типа *word* са називима *READ и WRITE* и додајемо их у *RET_VAL*. У поље *RECORD* уносимо податке са "*Drive db*". У писање уносимо *input*. У читање уносимо *output*. *Output* структура се шаље ка фреквентном регулатору. *Input* структура се шаље од фреквентног регулатора ка *plc-y*.

9.3. *PID* регулација



Слика 9. *PID регулатор*

PID се извршава у организационом блоку *Cyclic interrupt ob30. OB30* је организациони блок који се позива и извршава у одређеним и тачним временским интервалима. *Setpoint* је вредност која треба да се достигне. *Input* је повратна информација са енкодера. *Output* је излаз, који се шаље на фреквентни претварач (слика 9.).

10. ТЕСТИРАЊЕ

На поље *Start* на *HMI* покрећемо систем. Имамо могућност позивања лифта споља и изнутра. Приликом позивања лифта на жељени спрат. Мотор позелени и лифт креће. Мотор преко конопчића и котураче подиже/спушта лифт на жељени спрат (слика 10). Позицију лифта чита преко ласерског сензора. При доласку на жељени спрат, врата на панелу на симулацији се отварају.

Слика 10. *Изглед макете*

11. ЗАКЉУЧАК

У овом раду реализација комуникације profinet између *PLC*-а, *HMI*-а и фреквентног регулатора. На *HMI* панелу имамо могућност гледања параметара мотора и симулацију лифта. Са панела пуштамо мотор у рад, дајемо му *preset*. Када је мотор спреман за рад, добијемо потврду од фреквентног регулатора *preset_confirm*. Тиме иконица мотора постаје плаве боје.

12. LITERATURA

[1] https://us.profinet.com/profinet-explained/ (приступљено у септембру 2025.)

[2] extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.elektronika.ftn.uns.ac.rs/et-industrijska-elektronika/wp-content/uploads/sites/137/2018/03/Industrijska-elektronika-20-mart-2018.pdf (приступљено у септембру 2025.)

[3] https://library.automationdirect.com/hmis-and-multi-platform-communication/ (приступљено у септембру 2025.)

Кратка биографија:

Владимир Тешић родом из Крупња, рођен 1999. god. Дипломски рад на Факултету техничких наука из области Електротехнике и рачунарства – Примењена електроника одбранио је 2023.god.
контакт:
vladimirtesic27@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 007:004.056
ДОИ: https://doi.org/10.24867/34BE18Mijailovic

Имплементација аутентификације применом FIDO2 стандарда

Implementation of Authentication Using the FIDO2 Standard

Давид Мијаиловић, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *Рад се бави дизајном, имплементацијом и анализом веб апликације која користи FIDO2 стандард као замену за традиционалне лозинке. Кроз теоријски преглед, развој функционалног прототипа и симулацију напада, рад демонстрира практичну примену и безбедносну отпорност система аутентификације без лозинки, нудећи увид у његову супериорност у односу на системе засноване на лозинкама.*

Кључне речи (три до пет): *Аутентификација, FIDO2, WebAuthn, аутентификација без лозинке, криптографија јавног кључа*

Abstract – *This paper addresses the design, implementation, and analysis of a web application that utilizes the FIDO2 standard as a replacement for traditional passwords. Through a theoretical overview, prototype development, and attack simulations, the work demonstrates the practical application and security resilience of a passwordless authentication system, offering insight into its superiority over password-based systems.*

Keywords: (three to five): *Authentication, FIDO2, WebAuthn, Passwordless Authentication, Public key cryptography*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Горан Сладић, ред. проф.

1. УВОД

Дигитална трансформација је у средиште безбедносних изазова поставила концепт дигиталног идентитета, чија је верификација деценијама била готово синоним за употребу лозинки. Иако једноставне за имплементацију, лозинке су се показале као системски несигурне у модерном окружењу претњи. Истраживања су показала да корисници, оптерећени захтевима за дугим и сложеним лозинкама, усвајају небезбедне стратегије, као што је поновна употреба истих или сличних лозинки на више различитих сервиса [1]. Ова пракса, позната као „повезана судбина креденцијала“, значи да безбедносни пропуст на једном, мање битном сајту директно угрожава безбедност корисника на критичним сервисима попут имејла или интернет банкарства. Нападачи ово системски искоришћавају кроз нападе “попуњавањем креденцијала” (енгл. *credential stuffing*), где аутоматизовано тестирају процурене парове корисничких имена и лозинки на хиљадама других сајтова [2].

Поред напада на сервере, корисници су директно изложени нападима социјалног инжењеринга, пре свега „пецању“ (енгл. *phishing*). *Phishing* напади манипулишу корисницима како би их навели да добровољно унесу своје креденцијале на лажне веб странице које визуелно имитирају легитимне, што представља један од најраспрострањенијих и најефикаснијих проблема електронске крађе идентитета [3].

Као одговор на ове системске слабости, *FIDO* Алијанса (*Fast Identity Online Alliance*) и Конзорцијум за светску мрежу (*W3C*) развили су скуп стандарда познат као *FIDO2*. *FIDO2*, који се састоји од *Web Authentication* (*WebAuthn*) *API*-ја и *Client to Authenticator Protocol*-а (*CTAP2*), уводи отворену, скалабилну и интероперабилну архитектуру за аутентификацију без лозинки [4]. Коришћењем асиметричне криптографије, *WebAuthn* омогућава корисницима да се пријаве на онлајн сервисе користећи биометријске податке, мобилне уређаје или хардверске сигурносне кључеве на начин који је фундаментално отпоран на *phishing* и цурење база података са сервера [5].

Мотивација за овај рад произилази из препознавања да су инкрементална побољшања система заснованих на лозинкама достигла своје границе. Потребна је фундаментална промена парадигме. Примарни циљ овог рада је дизајнирати, имплементирати и анализирати функционални прототип веб апликације који у потпуности замењује традиционалну аутентификацију са *WebAuthn* стандардом, како би се демонстрирала његова практична применљивост и безбедносна отпорност.

2. НЕДОСТАЦИ ТРАДИЦИОНАЛНЕ АУТЕНТИФИКАЦИЈЕ

Традиционална аутентификација заснована на лозинкама рањива је на различите врсте напада који произилазе из комбинације техничких недостатака и

лоших навика корисника [6]. Упркос повећаној свести о важности сложености лозинки, многи корисници и даље примењују несигурне технике, као што су поновна употреба лозинки, одабир слабих комбинација и њихово записивање [6].

2.1. Phishing напади

Једна од најефикаснијих метода за крађу лозинки је *phishing* [7]. Нападачи креирају веб-сајтове који су готово идентични легитимним, а преваре су толико уверљиве да чак и искусни корисници могу бити преварени [8]. Основна рањивост лозинки на *phishing* произилази из њихове природе као дељене тајне.

2.2. Напади понављањем

Напад понављањем (енгл. *replay attack*) представља облик мрежног напада у којем се ваљан пренос података злонамерно понавља или одлаже [8]. Нападач може пасивно прислушкивати комуникацију, пресрести креденцијале за пријаву, а затим их поново послати да би остварио неовлашћен приступ. Да би се спречили овакви напади, неопходно је обезбедити „свежину“ сваке трансакције, што се постиже употребом механизама као што су једнократне лозинке или временске ознаке [9].

2.3. Man-in-the-Middle напади

Напад посредника (енгл. *Man-in-the-Middle*) је врста напада у којој нападач тајно пресреће и мења комуникацију између две стране које верују да комуницирају директно. У контексту лозинки, циљ је пресрести акредитиве током њиховог преноса. Иако се протоколи попут *HTTPS*-а користе за шифровање, нападачи и даље могу искористити рањивости [10]. Када се лозинка пресретне, она остаје важећа за пријаву и може се поново користити [11].

3. FIDO2 И WEBAUTHN СТАНДАРД

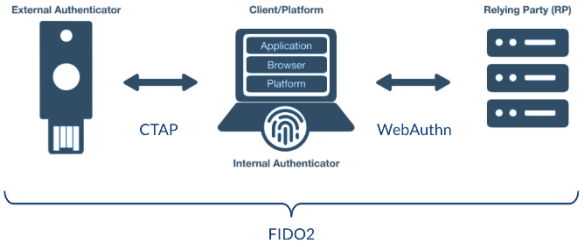
Стандард *FIDO2* представља комбинацију две међусобно повезане компоненте: *WebAuthn* и *CTAP2*. *WebAuthn* је спецификација коју је развио *W3C* и дефинише начин на који веб-апликације комуницирају са клијентским окружењем (прегледачем). *CTAP2* је спецификација под управом *FIDO* Алијансе и одређује како клијент комуницира са аутентификатором (нпр. *USB* токен, сигурносни кључ) [12].

Архитектура система укључује три кључна ентитета (слика 1) [12]:

1. *Relying Party* (*RP*) – Веб сервис (сервер) који жели да аутентификује корисника. *RP* иницира регистрацију, валидира криптографске потписе и чува јавне кључеве.

2. *WebAuthn* клијент / прегледач – Посредује између *RP*-а и аутентификатора користећи *JavaScript API* дефинисан у *WebAuthn* спецификацији.

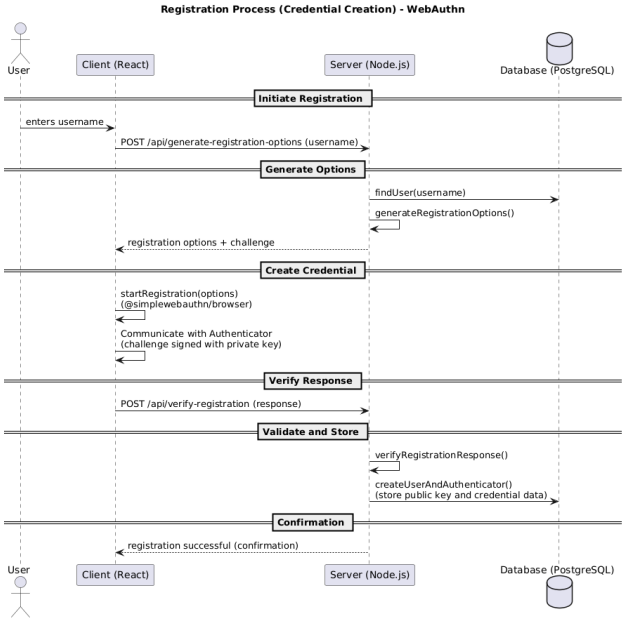
3. Аутентификатор – Компонента која безбедно чува приватни кључ и омогућава корисничку верификацију (нпр. биометрија, *PIN*). Може бити уграђен у уређај (*platform*) или бити спољни (*roaming*).



Слика 1. *Архитектура FIDO2 стандарда [13]*

4. ИМПЛЕМЕНТАЦИЈА И АНАЛИЗА СИСТЕМА

За потребе овог рада, развијен је функционални прототип веб апликације по клијент-сервер архитектури. Клијентска апликација је реализована као *Single Page Application* (*SPA*) коришћењем *React* библиотеке, док је серверска апликација изграђена на *Node.js* платформи уз *Express.js* окружење. За чување података коришћена је база података *PostgreSQL*. Архитектура система приказана је кроз секвенцијални дијаграм (слика 2) који илуструје ток комуникације између клијента, сервера и аутентификатора. На тај начин је обезбеђена јасна подела одговорности између слојева система и омогућена лакша надоградња и тестирање компонената.



Слика 1. *Секвенцијални дијаграм процеса регистрације корисника*

4.1. Клијентска и серверска имплементација

Клијентска апликација је реализована као *Single Page Application* коришћењем *React* библиотеке и *TypeScript*-а, при чему је кориснички интерфејс изграђен уз помоћ *Material-UI* компонентне библиотеке ради постизања визуелне конзистентности

и приступачности. Навигација унутар апликације имплементирана је помоћу *React Router*-а, који омогућава раздвајање јавних и заштићених рута [14]. Централизовано управљање статусом аутентификације спроведено је помоћу *AuthProvider* модула заснованог на *React Context API*-ју, који врши проверу активне сесије и одржава пријављено стање корисника.

На клијентској страни, коришћена је *@simplewebauthn/browser* библиотека која олакшава интеракцију са нативним *WebAuthn API*-јем прегледача. Процес аутентификације или регистрације одвија се у три корака:

1. Добијање опција са сервера: Клијент прво шаље *POST* захтев серверу са корисничким именом. Сервер враћа *JSON* објекат са опцијама, укључујући и криптографски изазов (енгл. *challenge*).

2. Покретање WebAuthn церемоније: Добијене опције се прослеђују функцији *startRegistration()* или *startAuthentication()*. Ове функције позивају нативни *WebAuthn API* прегледача (*navigator.credentials.create()* или *get()*), који преузима интеракцију са корисником и аутентификатором (нпр. *Windows Hello*, *YubiKey*).

3. Слање одговора на верификацију: Резултат добијен од аутентификатора (који садржи потписани изазов и друге податке) шаље се назад серверу на верификациону руту.

На серверској страни, коришћена је *@simplewebauthn/server* библиотека за генерисање изазова и верификацију криптографских одговора. Приликом регистрације, функција *generateRegistrationOptions()* се позива са параметрима као што су *rpName* (име апликације) и *rpID* (домен апликације). Посебно су важне опције унутар *authenticatorSelection* објекта: *userVerification: 'preferred'*, која сигнализира да треба захтевати верификацију корисника (PIN, биометрија), и *residentKey: 'required'*, која захтева од аутентификатора да сачува кључ на самом уређају, што омогућава аутентификацију без претходног уноса корисничког имена (*passkey*).

Функције *verifyRegistrationResponse* и *verifyAuthenticationResponse* врше криптографску проверу одговора добијеног од клијента. Оне упоређују изазов сачуван у сесији, проверавају да ли се *origin* и *rpID* поклапају са очекиваним вредностима дефинисаним у конфигурацији, и валидирају потпис користећи сачувани јавни кључ. За аутентификацију, функција такође проверава да ли је бројач (енгл. *counter*) у одговору већи од последњег сачуваног бројача у бази, што је кључна мера против клонирања аутентификатора.

Middleware ланац на серверу интегрише заштитне механизме као што су *rate limiting* и сесијско управљање изазовима, чиме се спречавају *brute-force* и *replay* напади. Логика је модуларно организована у контролере, руте и сервисе, што омогућава лако тестирање и одржавање кода.

4.2. Емпиријска анализа отпорности

Да би се практично потврдиле теоријске безбедносне гаранције, извршена је симулација три кључна вектора напада на имплементирани систем. Сваки напад је симулиран у контролисаном окружењу, користећи реалне услове комуникације између клијента и сервера. Резултати показују да комбинација механизама као што су *origin-binding*, јединствени криптографски изазов и бројач потписа обезбеђује вишеслојну заштиту против најчешћих типова напада.

Отпорност на Phishing
Симулиран је *phishing* напад подешавањем идентичне копије клијентске апликације на другом домену (порту). Покушај пријаве са лажне странице је био неуспешан. Заштита функционише на два нивоа [15]:

1. *CORS* политика: Серверска конфигурација је спречила комуникацију са неовлашћеног домена.

2. *Origin-binding*: Чак и након привременог онемогућавања *CORS* заштите, напад је заустављен на нивоу протокола. Потписани одговор који је аутентификатор генерисао на *phishing* сајту садржао је *origin* лажног сајта. Када је сервер верификовао овај одговор, одбио је аутентификацију јер се *origin* из потписа није поклапао са очекиваним, легитимним *origin*-ом апликације. Ово доказује да је заштита уграђена у технологију и не зависи од пажње корисника.

Отпорност на *Replay* нападе
Симулација је изведена пресретањем валидног аутентификационог одговора и његовим поновним слањем. Напад је био неуспешан захваљујући комбинацији два механизма:

1. Једнократни изазов: Сервер за сваки покушај пријаве генерише нови, јединствени изазов који се чува у сесији. Потписани одговор је валидан само за тај изазов.
2. Бројач потписа: Сваки *FIDO2* аутентификатор одржава интерни бројач који се инкрементира при свакој употреби. Сервер проверава да ли је бројач у примљеном одговору строго већи од последњег забележеног. Пошто поновљени захтев садржи исту вредност бројача, сервер га одбија [16].

Отпорност на *Man-in-the-Middle* нападе
WebAuthn архитектура је суштински отпорна на *MITM* нападе. Прво, спецификација захтева коришћење *HTTPS*-а, чиме се целокупна комуникација енкриптује. Друго, чак и у хипотетичком сценарију где нападач

успе да дешифрује саобраћај, напад је обесмишљен. За разлику од лозинке, у *WebAuthn* протоколу се не преносе осетљиви подаци које би нападач могао искористити. Приватни кључ никада не напушта сигурно окружење аутентификатора. Пресретнути потписани одговор је неупотребљив јер је једнократан и криптографски везан за оригиналну сесију и домен. Тиме је напад суштински обесмишљен јер нема тајне која се може украсти [17].

5. ЗАКЉУЧАК

Овај рад је демонстрирао дизајн, имплементацију и безбедносну ефикасност система аутентификације без лозинки заснованог на *FIDO2* стандарду. Кроз развој функционалног прототипа и емпиријску анализу, недвосмислено је потврђено да је имплементирано решење отпорно на кључне векторе напада који представљају системску претњу за традиционалне системе базиране на лозинкама, као што су *phishing*, *replay* и *Man-in-the-Middle* напади.

Показано је да је решење отпорно на *phishing* захваљујући криптографском везивању креденцијала за веб домен (енгл. *origin-binding*), што спречава злоупотребу на лажним сајтовима. Отпорност на *replay* нападе је осигурана комбинацијом једнократних криптографских изазова и бројача потписа. Коначно, анализа је показала да су *MITM* напади значајно отежани, јер приватни кључ никада не напушта сигурно окружење корисниковог уређаја. Резултати овог рада јасно потврђују да *WebAuthn* представља значајан искорак у дигиталној аутентификацији.

ЛИТЕРАТУРА

[1] D. R. Pilar, A. Jaeger, C. F. Gomes и L. M. Stein, „Passwords usage and human memory limitations: A survey across age and educational background," PloS one, т. 7, бр. 12, p. e51067, 2012.

[2] A. Das, J. Bonneau, M. Caesar, N. Borisov и X. Wang, „The tangled web of password reuse," у NDSS, 2014.

[3] M. Jakobsson и S. Myers, Phishing and countermeasures: understanding the increasing problem of electronic identity theft, John Wiley & Sons, 2007.

[4] FIDO Alliance, „FIDO Client to Authenticator Protocol (CTAP)," 2019.

[5] M. Weir, S. Aggarwal, B. De Medeiros и B. Glodek, „Password cracking using probabilistic context-free grammars," у 2009 30th IEEE Symposium on Security and Privacy, 2009.

[6] K. Chanda, „Password security: an analysis of password strengths and vulnerabilities," *International Journal of Computer Network and Information Security,* 2016.

[7] J. Owens и J. Matthews, „A study of passwords and methods used in brute-force SSH attacks," у USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008.

[8] RocketMeUpCybersecurity, „How WebAuthn is Changing the Future of Passwordless Security," 21 September 2023. Available: https://medium.com/@RocketMeUpCybersecurity/how-webauthn-is-changing-the-future-of-passwordless-security-71f71185fa42 (приступљено октобар 2025.)

[9] Y. Mo и B. Sinopoli, „Secure control against replay attacks," у 2009 47th annual Allerton conference on communication, control, and computing (Allerton), 2009.

[10] A. Mallik, „Man-in-the-middle-attack: Understanding in simple words," Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2018.

[11] M. Conti, N. Dragoni и V. Lesyk, „A survey of man in the middle attacks," IEEE communications surveys & tutorials, 2016.

[12] M. Barbosa, A. Boldyreva, S. Chen, K. Cheng и L. Esquível, „Privacy and Security of FIDO2 Revisited," Proceedings on Privacy Enhancing Technologies, 2025.

[13] A. Sinitsyna, „Beyond Passwords: FIDO2 AND WebAuthn in practice,". Available: https://www.inovex.de/de/blog/fido2-webauthn-in-practice/ (приступљено октобар 2025.)

[14] Remix, „React Router," 2025. Available: https://reactrouter.com/home. (приступљено октобар 2025.)

[15] L. S. Huang, Z. Weinberg, C. Evans и C. Jackson, „Protecting browsers from cross-origin CSS attacks," у Proceedings of the 17th ACM conference on Computer and communications security, 2010.

[16] G. Dua, N. Gautam, D. Sharma и A. Arora, „Replay attack prevention in Kerberos authentication protocol using triple password", 2013.

[17] M. Al-Sinani и A. A. Zaidan, „A review on man-in-the-middle attacks in cloud computing and their detection and prevention," ACM Computing Surveys (CSUR), 2021.

Кратка биографија:

Давид Мијаиловић рођен је 2000. године у Лозници. Основне академске студије је завршио 2023. године на Факултету техничких наука у Новом Саду. **Контакт**: mijailovicd00@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

UDK: 007:004.056
DOI: https://doi.org/10.24867/34BE19Popovic

Имплементација мултифакторске аутентификације за Open SSH сервер

Implementation of Multifactor Authentication for the Open SSH Server

Петар Поповић, *Факултет техничких наука, Нови Сад*

Студијски програм– ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Рад реализује имплементацију мултифакторске аутентикације за OpenSSH сервер, уз коришћење TOTP кодова као другог фактора. Приказани су кораци конфигурације, тестирања и анализа безбедносних аспеката током пријаве корисника на сервер.*

Кључне речи: *мултифакторска аутентификација, Open SSH сервер, MS аутентификатор, TOTP код*

Abstract – *In this paper, the implementation of multi-factor authentication for the OpenSSH server is presented, using TOTP codes as the second authentication factor. The configuration steps and security analysis during user login to the server are described.*

Keywords: *Multifactor authentication, Open SSH server, MS authenticator, TOTP code*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Горан Сладић, ред. проф.

1. УВОД

Дигитална инфраструктура постала је критична за готово све сфере савременог друштва, од комуникација и образовања до финансијских трансакција и управљања индустријским процесима [1]. Са растом комплексности система и међусобне повезаности сервиса, површина напада се континуирано шири, а последице инцидената све су скупље и видљивије [2]. Зато превенција, рано откривање рањивости и увођење вишеслојних механизама заштите представљају темељ одрживе сајбер безбедности. Традиционална аутентификација подразумева аутентификацију лозинкама. Она се у данашњем времену показала недовољном услед поновне појаве *phishing*-а , крађе база и *Brute-force* напада. Чак и уз политичке сложености и ротације лозинки, компромитација једног фактора често доводи до неовлашћеног приступа подацима [3,4]. Додавање додатног другог фактора значајно умањује ризик од преузимања корисничког налога. Мултифакторска аутентификација заснована на временски ограниченим једнократним кодовима *TOTP* (енг. *Time-based One-Time Password)* уравнотежује безбедност и употребљивост [5].
Код се генерише локално на уређају корисника, важи кратко и безбедно се упоређује на серверу [6]. Овај модел не захтева сталну повезаност ка спољним сервисима и добро се уклапа у оперативне услове серверских окружења [7].
Циљ рада је да се пројектује, имплементира и оцени прилагођени модул за *TOTP*, те интегрише у *OpenSSH* сервер тако да се обезбеди ток „Лозинка + *TOTP*“ без нарушавања постојећих оперативних навика администратора. Интеграцијом *TOTP* у *SSH* (енг. Secure shell) очекује се смањена вероватноћа успешног неовлашћеног приступа у сценаријима компромитације лозинке.

2. *OPENSSH* СЕРВЕР И АУТЕНТИФИКАЦИЈА

*SSH (*енг. *Secure Shell)* представља криптографски мрежни протокол намењен безбедној комуникацији између клијента и удаљеног сервера. Развијен је као замена за небезбедне протоколе као што су *Telnet* и *rlogin*, који су слали податке у отвореном тексту и били изложени пресретању и злоупотреби [7]. *SSH* обезбеђује три кључна својства комуникације: поверљивост, интегритет и аутентичност учесника у комуникацији [8]. Архитектура OpenSSH се временом развијала да укључује модуларни *PAM* слој, подршку за аутентификацију базирану на сертификатима, доношење одлуке о приступу на основу више фактора и могућност интеграције са системима за централизовану контролу идентитета. Ова еволуција резултирала је тиме да данашњи *OpenSSH* омогућава сегментацију корисничких сесија, анализу логова и динамичко управљање приступом.

2.1 Архитектура *OpenSSH* и слојеви безбедности

SSH протокол се састоји од три логичка слоја. Први слој је транспортни који обезбеђује енкрипцију и интегритет саме комуникације. Други слој протокола је слој аутентификације и он омогућава серверу да потврди идентитет клијента који успоставља везу са сервером. Последњи је слој канала и он служи за управљање више логичких сесија унутар једне SSH конекције. Током успостављања везе, клијент и сервер размењују јавне кључеве и договарају се о симетричним сесијским кључевима који ће бити коришћени за енкрипцију података [9]. Додатни PAM (енг. Pluggable Authentication Modules) слој, представља флексибилан и проширив механизам за управљање процесом аутентификације. Основна предност овог слоја је могућност да раздвоји апликациону логику од механизама за проверу идентитета [10].

3. *MFA* И ИМПЛЕМЕНТАЦИЈА У OPENSSH

Мултифакторска аутентификација (*MFA*) подразумева употребу два или више независних фактора приликом провере идентитета корисника. Основна идеја је да компромитација једног фактора не доведе аутоматски до компромитације налога корисника. Фактори додатне провере се обично сврставају у три категорије. Прва категорија су нешто што корисник зна, као лозинка, безбедносно питање или пин код. Други могући фактор јесте нешто што корисник поседује као мобилни уређај, паметни токен, одвојени дигитални кључ или нешто друго. Као последњи могући фактор додатне провере је нешто што сам корисник јесте. Ту спадају сви биометријски подаци корисника, отисак прста, лице или зеница ока.
Оваква комбинација значајно смањује ризик од неовлашћеног приступа и усклађује систем са безбедносним стандардима.

3.1 Интеграција *MFA* у *OpenSSH*

OpenSSH омогућава интеграцију *MFA* преко *PAM* слоја који се налази између механизма за пријаву и система за проверу идентитета. Конкретна имплементација може се постићи додавањем *TOTP* модула у конфигурацију [11]. Цео процес пријаве корисника на систем започиње уносом корисничког имена и лозинке у конзолу. Уколико је први фактор аутентификације био успешан, сервер од корисника тражи унос *TOTP* кода. У следећем кораку након уноса кода, код се верификује путем библиотеке која генерише исти алгоритам. Тек успешна верификација овог кода омогућава кориснику потпуни приступ систему.
Овај приступ не захтева екстерне сервисе и задржава све предности *OpenSSH* укључујући безбедност, отворени код и једноставну конфигурацију.

4. СПЕЦИФИКАЦИЈА СИСТЕМА

Ово поглавље описује захтеве, архитектуру и дизајн система за имплементацију мултифакторске аутентификације у OpenSSH серверу. Систем је развијен са циљем да обезбеди додатни ниво безбедности у SSH окружењу применом другог фактора аутентификације заснованог на *TOTP* алгоритму.

4.1 Архитектура система

У овом поглављу приказана је архитектура и основна логика решења за интеграцију мултифакторске аутентификације у SSH окружењу.
Систем се састоји од три главне компоненте:

- Клијентска апликација - представља интерфејс преко ког корисник иницира конекцију са сервером;
- Серверска инфраструктура - прихвата захтев, управља фазама пријаве и преусмерава процес ка *PAM* систему;
- Безбедносни слој - имплементира додатни фактор аутентификације и валидацију једнократних кодова;

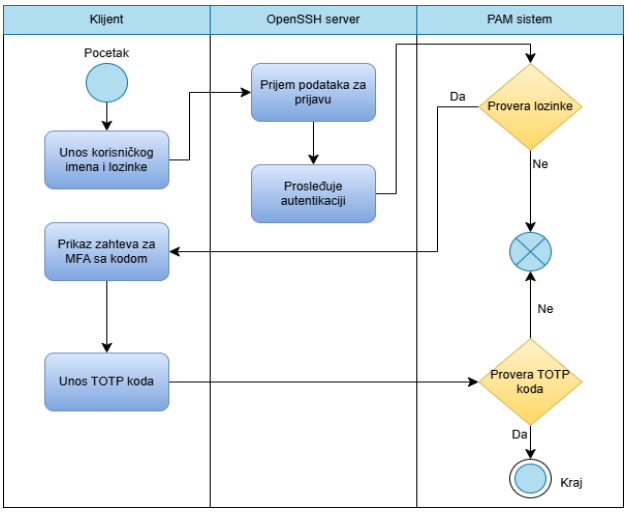
Клијент систему приступа преко терминала који шаље корисничко име и лозинку серверу. Сервер, раније конфигурисан да користи *PAM* систем као посредни слој, прослеђује податке *PAM*-у. Даље се иницира мултифакторска аутентификација и позива се *TOTP* модул ради верификације временски ограниченог кода генерисаног на уређају.
PAM механизам је од централног значаја у овој архитектури јер омогућава додавање нових метода аутентификације без измене кода *OpenSSH* сервера. На овај начин обезбеђује се проширивост и одрживост система у различитим инфраструктурама. Овај модел значајно унапређује безбедност јер минимизује ризик од компромитације налога и онемогућава приступ са само једним фактором аутентификације [11].

4.2 Процес аутентификације

Процес корисничке аутентификације у OpenSSH систему са интегрисаним мултифакторским механизмом може се описати кроз следеће кораке:

- Иницијализација конекције - клијент покреће SSH сесију и шаље серверу своје корисничко име.
- Унос лозинке - корисник уноси лозинку која се прослеђује серверу ради провере.
- Валидација лозинке - сервер позива *PAM* механизам да провери лозинку.
- Генерисање и унос *TOTP* кода - корисник користи апликацију која генерише код на основу тајног кључа и времена.
- Провера кода преко *TOTP* модула - *PAM* верификује унети код.
- Доношење одлуке - ако су оба фактора исправна, приступ је дозвољен; у супротном, сесија се прекида.

Овако дефинисан процес повећава безбедност и обезбеђује виши степен поузданости и контроле приступа у мрежним окружењима (слика 1).



Слика 1. *Дијаграм активности*

5. ИМПЛЕМЕНТАЦИЈА СИСТЕМА

За интеграцију мултифакторске аутентификације у *OpenSSH* сервер имплементиран је нови *TOTP* модул. Његова функција је да прихвати, обрађује и исправно

одговори на захтев клијента за аутентификацију. Представља проширење постојећег *PAM* модула.

5.1 Структура и интерфејси модула

У оквиру имплементације мултифакторске аутентификације, развијен је посебан *PAM* модул који омогућава интеграцију *TOTP* другог фактора у OpenSSH аутентификациони процес. Овај модул је кључни слој који омогућава проверу корисничког *TOTP* кода, који се генерише синхронизовано у односу на тајни кључ корисника и системско време.
Основни PAM модул развијен је у језику C и ослања се на стандардне интерфејсе. Најважнија тачка комуникације са стеком јесте функција за аутентификацију у којој почиње ток *MFA*.
Развој модула био је вођен циљем минималне интервенције у постојећи *OpenSSH* код тако што се користе механизми који су део *PAM* архитектуре и њених интерфејса, а која постоји као слој за аутентификацију у Linux систему. *PAM* модул неприметно интегрише нову *MFA* логику, а корисници настављају да користе већ познате клијентске алате као што је мобилна апликација за генерисање *TOTP* кодова.

5.2 Конфигурација система

За интеграцију развијеног *PAM* модула у системску аутентификацију *OpenSSH* сервера потребно је извршити суштинске измене у два конфигурациона фајла. Један је конфигурациони фајл *OpenSSH* а други *PAM*.
У конфигурационом фајлу *OpenSSH*, за активирање мултифакторске аутентификације, мора да се омогући *ChallengeResponseAuthentication*, што омогућава интеракцију корисника путем *keyboard-interactive* механизма. Поред тога, *AuthenticationMethods* се конфигурише тако да захтева почетни унос лозинке и потом *TOTP* кроз *keyboard-interactive*. Ово осигурава да корисник мора успешно проћи оба корака да би се пријавио. Ове измене представљају основни предуслов за успешан рад тока мултифакторске аутентификације засноване на привременим токенима у *OpenSSH* окружењу. Измењен конфигурациони фајл је приказан на листингу 1.

```
Port 2222
UsePAM yes
KbdInteractiveAuthentication yes
PasswordAuthentication no
AuthenticationMethods keyboard-interactive
```

Листинг 1. Конфигурациони *OpenSSH* фајл

5.3 Функције аутентификације *TOTP* модула

Главна функција сваког PAM аутентификационог модула је функција за обраду аутентификације. Она интегрише све алгоритамске и безбедносне кораке који воде од покретања сесије, преко прикупљања и провере података корисника, до коначне одлуке о дозвољавању или ускраћивању приступа систему.
На самом почетку функција преузима параметре и корисничке податке преко PAM модула. Користећи помоћну функцију, она идентификује корисника који покушава пријаву. Потом, приступа се фајлу који садржи тајни бинарни кључ у главном директоријуму тог корисника.
Функција за декодирање служи да тај кључ безбедно претвори у облик погодан за криптографску обраду. После успешног декодирања кључа, ток се наставља ка делу за интеракцију са самим корисником. Ту се шаље прилагођени текст за испис преко prompt_code и чека се унос кода од стране корисника. Овде систем подржава напредно конфигурисање, где се преко листе аргумената може мењати име фајла, број дозвољених покушаја, временски корак, број потребних цифара и стил корисничког prompt-a.

5.4 Генерисање и валидација токена

У модулу је додатно имплементирана функција за генерисање кода (*totp*). Користи се за генерисање и валидацију токена на серверској страни. У развијеном модулу користи *HMAC-SHA1* алгоритам.
Као улаз добија тајни кључ, временско стање, временски корак и број цифара за излаз. Прво се израчунава вредност броја (*counter*) који је целобројни део тренутног времена подељеног временским интервалом.
Овај број се представља као низ од 8 бајтова и шаље заједно са кључем у *HMAC* функцију. Добијени *MAC* (*Message Authentication Code*) се затим динамички сече, а добијена вредност се модуларно скраћује на жељени број цифара — најчешће шест. Функција је приказана на слици 2.

```
static unsigned int totp(const unsigned
char *key, size_t keylen,time_t t,
int step,int digits) {
       long long counter = (long long)
              (t / step);
       unsigned char msg[8];
       for (int i = 7; i >= 0; i--) {
         msg[i] = (unsigned char)
         (counter & 0xFF);
         counter >>= 8;
       }
       unsigned char mac[EVP_MAX_MD_SIZE];
       unsigned int maclen = 0;
       HMAC(EVP_sha1(), key, (int)keylen,
       msg, sizeof(msg), mac, &maclen);
       int off = mac[maclen - 1] & 0x0F;
       unsigned int bin =
         ((mac[off] & 0x7Fu) << 24) |
         ((mac[off + 1] & 0xFFu) << 16) |
         ((mac[off + 2] & 0xFFu) << 8) |
         (mac[off + 3] & 0xFFu);
       unsigned int mod = 1;
       for (int i = 0; i < digits; i++)
         mod *= 10u;
       return bin % mod;
}
```

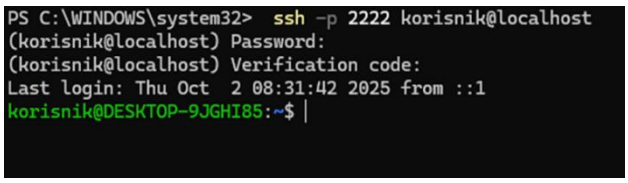
Слика 2. *Функција за генерисање* TOTP *кода*

При валидацији списак важећих кодова генерише се за неколико временских интервала чиме се умањује утицај малих десинхронизација корисника и сервера.

Ако унети код одговара неком референтном коду у датом прозору, *MFA* провера је успешно завршена.

5.5 Пријава на систем

Током процеса мултифакторске аутентификације неопходно је кориснику у сваком тренутку обезбедити јасне и прецизне поруке. *PAM* модул је по том питању потпуно модуларан и омогућава једноставно дефинисање свих исписа на терминалу. Како би се избегла непотребна сложеност, кориснику се приказују само основне поруке за унос лозинке и за унос верификационог кода. У случају исправног уноса оба параметра, систем приказује поруку о успешној пријави, док се у супротном исписује обавештење о неуспешној аутентификацији. Интеракција корисника са *OpenSSH* сервером након увођења мултифакторске аутентификације остаје једноставна и интуитивна, уз минималне измене у односу на класичан ток пријаве. Главна разлика је у додатном кораку провере идентитета. Након иницијализације *SSH* конекције, корисник уноси корисничко име и лозинку као и у стандардној сесији. Уколико је лозинка исправна, сервер активира *PAM* механизам који прослеђује процес ка *TOTP* модулу. Тада се кориснику приказује упит за унос једнократног кода који се генерише на његовом мобилном уређају у апликацији за аутентификацију. Ако је код валидан, приступ систему се одобрава и корисник је успешно улогован. У супротном, пријава се прекида уз одговарајућу поруку о грешци. Цео ток процеса од иницијализације конекције до успешне верификације једнократног кода приказан је на слици 3.



Слика 3. *Терминал приликом успешне пријаве*

6. ЗАКЉУЧАК

У оквиру овог рада изложена је имплементација мултифакторске аутентификације за OpenSSH сервере, са посебним освртом на интеграцију Microsoft Authenticator апликације као другог фактора заснованог на ТОТП механизму. Представљено решење омогућава значајно повећање безбедности приступа серверу, што је потврђено кроз серију тестирања у локалном SSH окружењу. Резултати показују да је увођење мултифакторске аутентификације практично и ефективно - додатни слој аутентикације не захтева комплексну инфраструктуру, кориснички ток није значајно успорен, а процес пријаве остаје интуитиван и лак за све кориснике.

Примена ТОТП токена и подршка кроз Microsoft Authenticator доказале су се као једноставне за интеграцију и употребу, уз минималне захтеве за додатну конфигурацију и обуку. Узимајући у обзир све изведене тестове, имплементација мултифакторске аутентификације базиране на ТОТП стандардима потврдила је своју поузданост и скалабилност. Овакав модел је посебно прикладан за окружења где је потребно брзо обезбедити критичне ресурсе, као и за све сценарије где се жели подизање отпорности на напредне претње и злоупотребе корисничких акредитација.

Имплементација оваквог решења представља препоручени корак за све организације и појединце који желе да подигну ниво заштите SSH сервера.

7. ЛИТЕРАТУРА

[1] Stallings, W. (2017). Network Security Essentials: Applications and Standards. 6th ed., Pearson.

[2] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W.W. Norton & Company.

[3] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). *The Tangled Web of Password Reuse.* NDSS Symposium.

[4] Florêncio, D., & Herley, C. (2011). *Where Do Security Policies Come From?* Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS).

[5] O'Gorman, L. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, 91(12), 2021–2040.

[6] M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time-Based One-Time Password Algorithm. RFC 6238, IETF.

[7] Ylönen, T., & Lonvick, C. (2006). The Secure Shell (SSH) Protocol Architecture. RFC 4251, IETF.

[8] Kim, H. & Smith, M. (2019). "Security comparison of Secure Shell (SSH) and predecessor protocols." Journal of Communication and Computer, 16(6), 262–270

[9] Barret, D., Silverman, R., & Byrnes, R. (2012). SSH, The Secure Shell: The Definitive Guide. O'Reilly.

[10] Samar, V., & Lai, C. (1996). Pluggable Authentication Modules. Sun Microsystems White Paper.

[11] M'Raihi, D., et al. (2011). TOTP: Time-Based One-Time Password Algorithm. RFC 6238.

Кратка биографија:

Петар Поповић рођен је 2001. године у Лозници. Основне академске студије је завршио 2023. године на Факултету техничких наука у Новом Саду. Мастер рад на Факултету техничких наука из области Рачунарство и аутоматика – Електронско пословање одбранио је 2025. године.

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.9
ДОИ: https://doi.org/10.24867/34BE20Bubnjevic

ЈЕДАН ПРИСТУП МОДЕЛОМ ВОЂЕНОГ ИНЖЕЊЕРИНГА ИНФОРМАЦИОНИХ СИСТЕМА

A MODEL-DRIVEN APPROACH TO INFORMATION SYSTEM ENGINEERING

Вељко Бубњевић, *Факултет техничких наука, Нови Сад*

Студијски програм – СОФТВЕРСКО ИНЖЕЊЕРСТВО И ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

Кратак садржај – *Циљ овог истраживања је да се, применом инжењеринга вођеног моделима, формално дефинишу и практично примене поступци трансформација који омогућавају поступни прелазак са концептуалног на имплементациони ниво. Полазећи од концептуалног модела информационог система заснованог на концепту типа форме, предложени приступ омогућава извођење релационе шеме базе података и њеног имплементационог описа за изабрану SQL (Structured Query Language) платформу. Дефинисан је методолошки оквир који обухвата проширење наменског језика FTDSL (Form Type Domain-Specific Language) развојем графичке синтаксе и имплементацију Model-to-Model и Model-to-Text трансформација, чиме се обезбеђује интегрисан и аутоматизован процес инжењеринга информационих система заснован на моделима.*

Кључне речи : *трансформације шема база података, концептуално моделовање, концепт типа форме, MDE/CASE алати*

Abstract – *The aim of this research is to formally define and practically apply transformation procedures based on model-driven engineering (MDE), enabling a gradual transition from the conceptual to the implementation level. Starting from the conceptual model of an information system (IS) based on the form type concept, the proposed approach enables the derivation of a relational database schema and its implementation description for the selected SQL (Structured Query Language) platform. A methodological framework has been defined, encompassing the extension of the domain-specific language FTDSL (Form Type Domain-Specific Language) through the development of its graphical syntax and the implementation of Model-to-Mode and Model-to-Text transformations, thereby providing an integrated and automated model-driven information system engineering process.*

Keywords: *database schema transformation, conceptual modeling, form type concept, MDE/CASE tools*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је др Славица Кордић, ванр. проф.

1. УВОД

Традиционални начин изградње *IS* полазио је од прикупљања корисничких захтева, најчешће у неформалном облику, који су касније претварани у формалне моделе система. Такви модели су неретко садржали детаље везане за конкретну имплементациону платформу, док је програмски кôд настајао углавном ручним програмирањем. Савремени приступи, засновани на моделима полазе од идеје да се развој софтвера заснива на низу формалних трансформација модела различитих нивоа апстракције, почев од рачунарски независних модела (*Computation-Independent Model – CIM*), све до модела зависних од платформе и извршивог кôда.

У том правцу, на Факултету техничких наука Универзитета у Новом Саду развијају се методе за платформски независно моделовање *IS* и алгоритми за аутоматску трансформацију таквих модела у извршиве прототипове *IS*. У оквиру ових истраживања развијен је алат под називом IIS*Case (*Integrated Information Systems CASE*), који припада класи интегрисаних *CASE* (*Computer Aided Software Engineering*) производа. Његова основна улога је да подржи што већи број активности у процесу развоја *IS*.

Иако је у алату IIS*Case већ реализован реверзни инжењеринг на основу мета-модела, презентованих у [1][2], процес *forward* инжењеринга у оквиру *MDE* окружења до сада није био у потпуности подржан. Уместо тога, IIS*Case је користио *GPL* (*General Purpose Language*) Java као засебан приступ, што је стварало одређени јаз у односу на принципе развоја софтвера вођеног моделима. У овом раду је развијена нова, унапређена верзија алата IIS*Case, у којој је процес инжењеринга *IS* у потпуности реализован применом *MDE* приступа. Реализација је спроведена, применом *Model-to-Model* (*M2M*) и *Model-to-Text* (*M2T*) трансформација у области инжењеринга *IS*, као и проширењем постојећег наменског језика *FTDSL* развојем његове графичке синтаксе, чиме се обезбеђује комплетан развој *IS* у оквиру јединственог и интегрисаног *MDE* окружења.

2. КОНЦЕПТУАЛНО МОДЕЛОВАЊЕ *IS*

Инжењеринг *IS* у алату IIS*Case започиње концептуалним моделовањем *IS*, где пројектант на основу захтева и докумената креира типове форми,

којима се описују правила употребе података у реалном систему. Тип форме се може схватити као општи облик пословних докумената и екранских форми путем којих корисник ступа у интеракцију са *IS*. Типови форми представљају основу за генерисање почетног скупа атрибута и идентификацију полазног скупа ограничења, које IIS*Case користи као улазне параметре у поступку формирања релационе шеме базе података.

2.1. Концепт типа форме

Генерализацијом анализе садржаја екранских и штампаних форми (докумената) долази се до појма типа форме [3]. Тип форме $\mathcal{F}$ је структура стабла чије чворове представљају типови компоненти. Формално, тип форме је именована петорка $\mathcal{F}(O, \varphi, Man, \mathcal{S}_S(\mathcal{F}), C_{\mathcal{F}})$, над скупом обележја $W(\mathcal{F})$, где је:

- $O = \{N_i(Q_i, C_i, Role(N_i)) \mid i = 1,\ldots, m\}$ скуп типова компоненти,
- $\varphi \subseteq O \times O$ је релација која над скупом O дефинише структуру стабла,
- Man је функција обавезности: Man: $\varphi \rightarrow \{M, O\}$, која сваком $(N_i, N_j) \in \varphi$ придружује вредност M (обавезна) или O (опциона) веза,
- $\mathcal{S}_S(\mathcal{F})$ је параметар чија вредност Y указује на то да тип форме $\mathcal{F}$ учествује, а вредност N да тип форме $\mathcal{F}$ не учествује у формирању шеме базе података,
- $C_{\mathcal{F}}$ скуп ограничења типа форме $\mathcal{F}$, при чему скуп обележја $W(\mathcal{F})$ задовољава услове (1) и (2) :

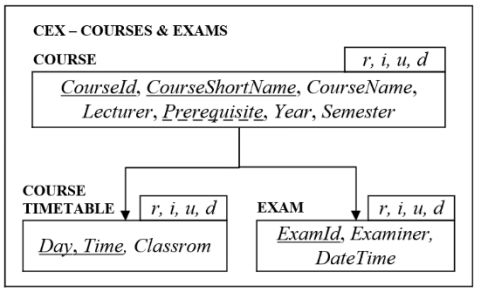
$$\bigcup_{i=1}^{m} Q_i = W(\mathcal{F}), \tag{1}$$

$$(\forall N_i, N_j \in O)(i \neq j \Leftrightarrow Q_i \cap Q_j = \varnothing). \tag{2}$$

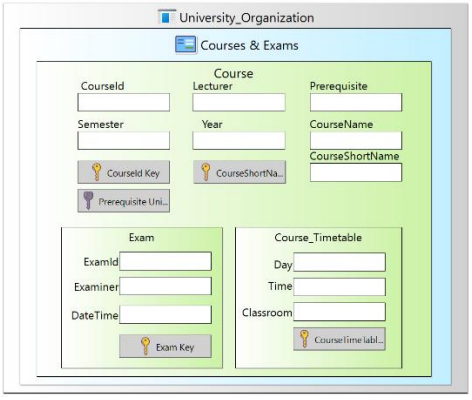
2.2. Развој графичке синтаксе језика FTDSL

Да би се могао спровести процес *forward* инжењеринга алата IIS*Case користећи приступ развоју софтвера вођеног моделима, било је неопходно обезбедити подршку за концептуално моделовање *IS* употребом наменског језика *FTDSL*, као улазног модела у ланцу *M2M* трансформација. *FTDSL* је наменски језик немењен за концептуално моделовање *IS* путем типова форми, који омогућава формалну спецификацију структура и ограничења на нивоу *PIM* (*Platform-Independent Model*) модела. У оквиру овог истраживања развијена је графичка синтакса наменског језика *FTDSL*, оригинално представљеног у [2]. Док је *FTDSL* у почетној верзији био заснован на текстуалној нотацији, која је захтевала добро познавање синтаксних правила и структура самог језика, предложено проширење у овом раду уводи графички слој који омогућава интуитивније концептуално моделовање *IS*. Графичка синтакса омогућава визуелну спецификацију типова форми, компоненти и њихових односа, што приближава процес моделовања перцепцији крајњег корисника и олакшава комуникацију између аналитичара и доменских стручњака. Истовремено, задржана је формална повезаност са апстрактном синтаксом језика *FTDSL*, што омогућава његову интеграцију у *MDE* оквир и *M2M* ланац трансформација.

На слици 1 приказан је тип форме *Courses & Exams*, док је на слици 2 приказан модел истог типа форме моделован коришћењем графичке синтаксе наменског језика *FTDSL* употребом *Eclipse Sirius* алата.



Слика 1. *Тип форме* Courses & Exams



Слика 2. *Модел типа форме* Courses & Exams *специфициран употребом графичке синтаксе језика* FTDSL

3. ТРАНСФОРМАЦИЈА КОНЦЕПАТА ПРОШИРЕНОГ IIS*CASE МЕТА-МОДЕЛА У КОНЦЕПТЕ ПРОШИРЕНОГ ГЕНЕРИЧКОГ МЕТА-МОДЕЛА

Након концептуалног моделовања, следећи корак представља пројектовање подшеме релационе базе података за изабрани апликативни систем. Подшема релационе базе података која задовољава услов *3NF* добија се поступком нормализације применом модификованог Бернштајновог алгоритма синтезе. Реализација модификованог Бернштајновог алгоритма синтезе спроведена је употребом ланца *M2M* трансформација. Као изворни модел коришћен је модел који је у складу са мета-моделом дефинисаним у оквиру апстрактне синтаксе језика *FTDSL*, док је као циљни модел коришћен модел који је у складу са Генеричким мета-моделом који је дефинисан у складу са теоријским основама релационог модела података [1]. Оба мета-модела су, у циљу подршке процесу *forward* инжењеринга, проширена новим концептима, при чему се први у наставку рада означава као Проширени IIS*Case мета-модел, а други као Проширени генерички мета-модел.

Како модификовани алгоритам синтезе обухвата више корака, који нису могли бити изражени потпуно декларативно, било је неопходно процес трансформације поделити на више целина, где сваки

излаз из претходне трансформације представља улаз у наредну. У ту сврху дефинисано је шест међусобно повезаних трансформација, које заједно омогућавају потпуну реализацију поступка *forward* инжењеринга: *FormConstraintsIdentification*, *Synthesis3NF*, *PKCandidatesIdentification*, *PKSelection*, *PKPropagation*, *InterRelationalConstraintsDefinition*.

3.1. Идентификација полазног скупа ограничења

FormConstraintsIdentification је егзогена *out-place* трансформација којом се трансформише модел који је у складу са IIS*Case мета-моделом у модел који је у складу са Проширеним генеричким мета-моделом. Ова трансформација уведена је како би се из концептуалног модела идентификовао полазни скуп ограничења који ће представљати улаз у алгоритам синтезе. Трансформацијом се идентификују следећа ограничења са типова форми: функционалне зависности, нефункционални односи, специјалне функционалне зависности са уграђеним ограничењима јединствености и уграђене зависности садржавања. Поступак идентификације полазног скупа ограничења у потпуности се заснива на формалним правилима дефинисаним у [4][5].

Пример 3.1. Посматра се тип форме са слике 2.1. Применом правила из *FormConstraintsIdentification* трансформације добија се следећи скуп функционалних зависности:

$$F(\mathcal{F}) = \{CourseId \rightarrow CourseShortName,\ CourseId \rightarrow CourseName,\ CourseId \rightarrow Lecturer,\ CourseId \rightarrow Prerequisite,\ CourseId \rightarrow Year,\ CourseId \rightarrow Semester,\ CourseId + Day + Time \rightarrow Classroom,\ CourseId + ExamId \rightarrow Examiner,\ CourseId + ExamId \rightarrow DateTime,\ CourseShortName \rightarrow CourseId,\ Prerequisite \underline{\rightarrow} CourseId\},$$

при чему је знаком $\underline{\rightarrow}$ означена специјална функционална зависност. Применом правила за идентификацију нефункционалих односа добија се следећи скуп нефункционалних односа:

$$NF(\mathcal{F}) = \{CourseId + Day + Time \rightarrow \theta_1,\ CourseId + ExamId \rightarrow \theta_2\}.$$

3.2. Алгоритам синтезе

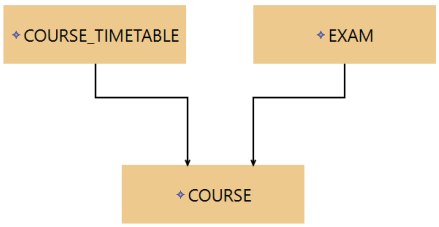
Након идентификације полазног скупа ограничења следећи корак представља примена алгоритма синтезе. Алгоритам синтезе је специјално унапређен за практичне примене потреба алата IIS*Case, па се из тог разлога назива модификованим. Трансформација којом се спроводи алгоритам синтезе јесте *Synthesis3NF*. Улаз у ову трансформацију представљају два модела, један који је излаз из претходне трансформације, и други који је полазни концептуални модел у складу са IIS*Case проширеним мета-моделом. Потреба за концептуалним моделом у оквиру ове трансформације произилази из чињенице да се поједина ограничења, дефинисана унутар генерисане релационе шеме, могу закључити само на основу информација које су доступне у концептуалном моделу. Концептуални модел, представља неопходан извор семантичког контекста који омогућава правилну идентификацију, и формирање ограничења у релационој шеми базе података. По изласку из ове трансформације добија се скуп шема релација који задовољава услов *3NF*.

Пример 3.2. Посматра се полазни скуп ограничења из примера 3.1. Применом алгоритма синтезе у оквиру *Synthesis3NF* трансформације добија се следећи скуп шема релација подшеме:

- *Course*({*CourseId*, *CourseName*, *CourseShortName*, *Lecturer*, *Year*, *Semester*, *Prerequisite*}, {*CourseId*, *CourseName*, *CourseShortName*}, {*Prerequisite*}),
- *Course_Timetable*({*Day*, *Classroom*, *CourseId, Time*}, {*Day+Time+CourseId*}}) и
- *Exam*({*ExamId*, *CourseId*, *Examiner*, *DateTime*}, {*ExamId+CourseId*}}).

У оквиру ове трансформације врши се генерисање и графа затварања [4][5]. Граф затварања представља погодну дијаграмску технику за представљање структуре шеме релационе базе података. Сваки чвор у графу затварања представља једну шему релације у шеми базе података, док свака грана између чворова означава да скуп обележја надређеног чвора функционално одређује, тј. затвара, скуп обележја подређеног чвора.

Пример 3.3. На слици 3 приказан је граф затварања у *Eclipse Sirius* едитору који је добијем *Synthesis3NF* трансформацијом на скуп ограничења из примера 3.1.



Слика 3. *Генерисани граф затварања*

3.3. Избор кандидата за примарни кључ

По изласку из алгоритма синтезе свака шема релације добија скуп еквивалентних кључева. Један од тих еквивалентних кључева пројектант треба да одабере за примарни кључ. У контексту модификованог алгоритма синтезе не може сваки еквивалентни кључ да испуњава услов да буде кандидат за примарни кључ. Ова тема детаљно је разрађена у [5]. Провера испуњености услова кандидата за примарни кључ спроведена је у оквиру трансформације *PKCandidatesIdentification*, која за сваки кључ утврђује да ли испуњава услов кандидата за примарни кључ и сходно томе га означава. Уколико ниједан кључ у појединој шеми релације не испуњава услов кандидата за примарни кључ, извршавање ланца трансформација се прекида и корисник се обавештава о томе. Након тога се извршава трансформација *PKSelection*, која насумично бира један од кандидата за примани кључ и проглашава га за примарни. Обе трансформације представљају ендогене *in-place* трансформације, а као резултат се добија модел шеме базе података у којем свака шема релације има дефинисан примарни кључ.

3.4. Трансформација скупа шема релација са некоректним простирањем кључа

По изласку из претходне трансформације свака шема релација поседује примарни кључ. Међутим, приликом одабира примарних кључева могло је да дође до њиховог некоректног простирања, односно, да се деси да су различити еквивалентни кључеви једне шеме релације изабрани за стране кључеве. Трансформација *PrimaryKeysPropagation* има за циљ да изврши трансформацију скупа шема релација са некоректним простирањем кључа у скуп шема релација са коректним простирањем кључа, поштујући алгоритам трансформације у модификованом алгоритму синтезе.

3.5. Генерисање међурелационих ограничења

InterRelationalConstraintsDefinition трансформацијом се завршава процес генерисања подшеме релационе базе података. Ова трансформација генерише следеће типове ограничења:

- основна, инверзна и проширена ограничења референцијалног интегритета,
- ограничења основних и инверзних референцијалних интегритета заснованих на нетривијалним зависностима садржавања,
- међурелациона ограничења зависног скупа шема релација и
- проширена ограничења торке.

3.6. Мапирање концепта Проширеног генеричког мета-модела у концепт РСУБП мета-модела

Завршни корак у ланцу *M2M* трансформација представља трансформацију модела који је настао као резултат претходне трансформације у модел који је у складу са РСУБП (Релациони систем за управљање базама података) мета-моделом. РСУБП мета-модел обухвата појмове неопходне за моделовање шема база података на најнижем нивоу апстракције, односно на нивоу РСУБП-а. Овај мета-модел је дефинисан у [1]. Потреба за овим мапирањем произилази из чињенице да је РСУБП мета-модел концептуално и структурно ближи изабраној *SQL* платформи, чиме се омогућава једноставнија и ефикаснија реализација *M2T* трансформација у процесу генерисања извршивог *SQL* кôда.

4. ГЕНЕРИСАЊЕ ИМПЛЕМЕНТАЦИОНОГ ОПИСА ШЕМЕ БАЗЕ ПОДАТАКА

Завршни корак поступка инжењеринга представља процес генерисања имплементационог описа подшеме базе података, који се спроводи применом *M2T* трансформација. Циљ овог корака је да се модел, који је у складу са РСУБП мета-моделом, трансформише у извршиви *SQL* кôд погодан за креирање релационе базе података у оквиру изабраног РСУБП-а. За реализацију генератора кода коришћен је *Eclipse Modeling Framework* (*EMF*) у комбинацији са *Acceleo* језиком, који представља уобичајено решење за *M2T* трансформације. Развијени генератор омогућава аутоматско генерисање имплементационог описа шеме базе података у облику *DDL* (*Data Definition Language*) скрипти за три платформе: *ANSI SQL*, *Oracle 21c* и *Oracle 23c*.

Генератор подржава генерисање процедуралних механизама за проверу очувања ограничења инверзних референцијалних интегритета. Кориснику је омогућен избор начина реализације ових ограничења — путем складиштених процедура (*stored procedures*) или погледа (*views*). Додатно, у оквиру овог решења подржнао је и аутоматско генерисање процедуралних механизама који служе за проверу и одржавање проширених ограничења торке.

5. ЗАКЉУЧАК

Спроведеним истраживањем и реализацијом ланца *M2M* и *M2T* трансформација, у овом раду омогућен је развој *IS* применом *MDE* приступа. На овај начин, концептуални модели дефинисани језиком *FTDSL* постају полазна основа за аутоматско генерисање релационе шеме базе података и имплементационог описа. Кључни доприноси рада огледају се у:

- развоју унапређене верзије алата IIS*Case у којој је реализован *MDE* процес инжењеринга *IS*,
- омогућавању интегрисаног концептуалног моделовања и генерисања релационе шеме базе података унутар јединственог *MDE* окружења,
- дефинисању и имплементацији ланца *M2M* трансформација који обезбеђује потпуно аутоматизован прелазак са концептуалног на имплементациони ниво.

Резултати овог истраживања представљају значајан корак ка успостављању потпуно интегрисаног *MDE* процеса алата IIS*Case, чиме се остварују могућности за даља истраживања, међу којима су генерисање прототипа *IS* заснованих на генерисаној шеми базе података.

6. ЛИТЕРАТУРА

[1] Aleksić S, Metode transformacija šema baza podataka u obezbeđenju reinženjeringa informacionih sistema, doktorska disertacija, Univerzitet u Novom Sadu (2013).

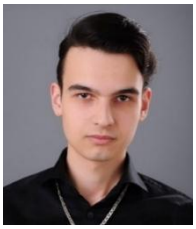
[2] Čeliković M, Pristup modelovanju specifikacija informacionog sistema putem namenskih jezika, doktorska disertacija, Univerzitet u Novom Sadu (2018).

[3] Ristić S, Istraživanje problema konsolidacije podšema baza podataka, doktorska disertacija, Univerzitet u Novom Sadu (2003).

[4] Luković I, Automatizovano generisanje podšeme relacione baze podataka putem formi, magistarski rad, Univerzitet u Beogradu (1993).

[5] Mogin, Pavle, Ivan Luković, and Miro Govedarica. Principi projektovanja baza podataka. Fakultet tehničkih nauka (2004).

Кратка биографија:



Вељко Бубњевић рођен је у Новом Саду 2001. год. Дипломски рад на Факултету техничких наука из области Електротехнике и рачунарства одбранио је 2024. год. Године 2025. изабран је у звање сарадника у настави на Факулету техничких наука.
Контакт: bubnjevic@uns.ac.rs

Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.42:004.738.12
DOI: https://doi.org/10.24867/34BE21Jocic

ПРОРАЧУН ТОКОВА СНАГА ИНТЕГРИСАНИХ ПРЕНОСНО-ДИСТРИБУТИВНИХ МРЕЖА

POWER FLOW PROCEDURE FOR INTEGRATED TRANSMISSION-DISTRIBUTION NETWORKS

Коста Јоцић, Никола Војновић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду предложена је процедура за прорачун токова снага интегрисано преносно-дистрибутивних мрежа. Представљени су модели различитих типова мрежа и проблема токова снага и поступци за њихово решавање, као вид одвојеног приступа при анализи стаационарног стања мреже. Дат је предлог заједничког, јединственог поступка над интегрисаном мрежом уз приложене резултате прорачуна над конкретним примером мреже и дискусију резултата.*

Кључне речи: *интегрисана преносно-дистрибутивна мрежа, Њутн-Рафсонов поступак, поступак сумирања струја и корекција напона, токови снага*

Abstract – *This paper proposes one solution for an integrated power flow calculation procedure over an integrated transmission-distribution networks. Models of different types of network and power flow problems, as well as the methods for their solution, are introduced as a form of the separated approach to a steady-state network analysis. Building upon these foundations, an integrated, unified, procedure applicable to the integrated network is proposed. The validation of the approach is given through calculations performed on a representative test network, followed by a discussion of the obtained results.*

Keywords: *integrated transmission-distribution network, Newton-Raphson procedure, Backward/Forward Sweep, load flow*

1. УВОД

Прорачуни токова снага устаљених режима спадају у основне прорачуне у дистрибутивним и електроенергетским менаџмент системима. На њиховим резултатима се базира велики број других прорачуна, услед чега је неопходно развити погодне алгоритме који ће на што поузданији и што ефикаснији начин обезбедити резултате тих прорачуна у сваком захтеваном моменту. Услед моделовања мрежа нелинеарним моделима, поступци којима се врши анализа стања система су итеративни. У раду су представљени различити типови алгоритама, намењених за прорачуне токова снага различитих типова мрежа, као и комбинација истих за анализу стања интегрисаних мрежа. За преносне мреже представљен је Њутн-Рафсонов, а за дистрибутивне поступак сумирања струја и корекција напона. Ово решење представља најпогоднији избор, услед упетљане структуре преносних, односно радијалних структура и великих димензија дистрибутивних система. Сами модели токова снага разматраних мрежа писани су сходно методу независних напона (за пренос) и методу независних струја (за дистрибуцију). Софтверски пакет MKL, библиотеке компаније Intel [1] и Гаус-Зајделов нумерички метод употребљени су као алати за нумеричке прорачуне.

Услед раста утицаја децентрализације ЕЕС-а долази појаве реверзибилних токова снага, од дистрибутивних ка преносним деловима система, као и преношење несиметрије режима у истом смеру. Те појаве додатно усложњавају међусобни утицај ова два дела система и мотивишу потребу за развојем процедуре која би у реалном времену вршила прорачун токова снага у целокупној мрежи.

Предложени поступак се заснива на интеграцији претходно описана два поступка у један, који се примењује над јединственом преносно-дистрибутивном мрежом.

Математичка подлога, као и тестирање предложеног интегрисаног поступка изложени су у главама 2 и 6, респективно.

2. ЕЛЕМЕНТИ МАТЕМАТИКЕ

Модели проблема токова снага исказују се кроз системе нелинеарних једначина, чија се решења добијају решавањем њихове линеаризоване форме. Резултати добијени таквим приступом су само апроксимације решења почетног система. Што је околина линеаризације ужа, то су апроксимације тачније. Сходно горе наведеном, поступци за решавање таквих система су итеративни.

У наставку се, применом два поступка поменута у уводу, кроз делове 2.1 и 2.2 , решава следећи систем нелинеарних алгебарских једначина:

$$\begin{aligned} b_1 &= f_1(x_1, x_2, \dots, x_n), \\ b_2 &= f_2(x_1, x_2, \dots, x_n), \\ &\vdots \\ b_n &= f_n(x_1, x_2, \dots, x_n). \end{aligned} \tag{1}$$

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Никола Војновић, ванред. проф.

2.1. Њутн-Рафсонов поступак

Њутн-Рафсонов поступак се ослања на прва два члана развоја нелинеарне функције у Тејлоров ред, у околини разматране тачке. Тиме се добија линеарна апроксимација разматране функције. Решавање почетне нелинеарне се своди на решавање линеарне функције, чиме добијено решење није тачно, већ апроксимирано [2], [3]. На примеру система датог релацијама (1), Њутн-Рафсонов поступак се примењује кроз следеће кораке:

1. Развити све функције $f_k(\boldsymbol{X})$ у Тејлоров ред у околини h - те апроксимације решења. Након тога се врши линеарна апроксимација узимањем само прва два члана, за сваку независно променљиву, чиме се добија релација:

$$f_k^h(x_1, x_2, \dots, x_n) = f_k(x_1^h, x_2^h, \dots, x_n^h) + \frac{1}{1!}\cdot\sum_{i=1}^{n}\left.\frac{\partial f_k(x_1^h, x_2^h, \dots, x_n^h)}{\partial x_i}\right|_{\substack{x_j = x_j^h, \\ j=1,2,\dots n}} \cdot (x_i - x_i^h), \quad (2)$$
$$k = 1,2, \dots n.$$

2. С обзиром да се решава линеаризовани облик (дат претходном релацијом) почетног нелинеарног система (1), релација (2), након сређивања, добија следећу форму:

$$\Delta b_k^h = \sum_{i=1}^{n}\left.\frac{\partial f_k(x_1^h, x_2^h, \dots, x_n^h)}{\partial x_i}\right|_{\substack{x_j = x_j^h, \\ j=1,2,\dots n}} \cdot \Delta x_i^h, \quad (3)$$
$$k = 1,2, \dots n,$$

где су:

$$\Delta b_k^h = b_k - f_k(x_1^h, x_2^h, \dots, x_n^h), \quad (4)$$
$$\Delta x_i^h = x_i^{h+1} - x_i^h, \quad (5)$$
$$k = 1,2, \dots n; \quad i = 1,2, \dots n.$$

3. Ако се чланови суме из релације (3) обележе са a_{ki}^h, тада се тој релацији може дати следећа матрична форма:

$$\begin{bmatrix}\Delta b_1^h \\ \Delta b_2^h \\ \vdots \\ \Delta b_n^h\end{bmatrix} = \begin{bmatrix} a_{11}^h & a_{12}^h & \cdots & a_{1n}^h \\ a_{21}^h & a_{22}^h & \cdots & a_{2n}^h \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}^h & a_{n2}^h & \cdots & a_{nn}^h \end{bmatrix} \cdot \begin{bmatrix}\Delta x_1^h \\ \Delta x_2^h \\ \vdots \\ \Delta x_n^h\end{bmatrix}, \quad (6)$$

где је матрица из релације јакобијан функција ($\boldsymbol{J}(\boldsymbol{X}^h)$) с десних страна система, датог релацијама (1), израчунат за текућу (h - ту) апроксимацију његовог решења $\boldsymbol{X}^h$.

4. Разматрани систем линеарних једначина треба решити по вектору корекција текућих апроксимација решења система $\Delta\boldsymbol{X}^h$.
5. На основу добијеног вектора из претходне тачке, долази се до наредне апроксимације, која се узима за решење система, услед веће тачности:

$$\boldsymbol{X}^{h+1} = \boldsymbol{X}^h + \Delta\boldsymbol{X}^h. \quad (7)$$

6. Проверава се задовољење критеријума конвергенције:

$$\left|x_k^{h+1} - x_k^h\right| \le \varepsilon_x \wedge$$
$$\left|b_k - f_k(x_1^{h+1}, x_2^{h+1}, \dots, x_n^{h+1})\right| \le \varepsilon_f, \quad (8)$$
$$h = 1,2,3, \dots; \quad k = 1,2, \dots, n.$$

7. Уколико је постигнуто задовољење критеријума, рачуна се наредна апроксимација решења и она се узима као крајње решење поступка. У супротном, поступак се наставља у наредној итерацији.

2.2. Гаус-Зајделов метод

Разматрани систем нелинеарних једначина дат релацијама (1) се, за потребе примене овог метода, трансформише у погоднији облик. Ако се познаје h-та апроксимација решења, коригована $(h+1)$ -ва апроксимација решења, сходно Гаус-Зајделовом методу гласи [3], [4] :

$$\begin{aligned} x_1^{h+1} &= \Phi_1(x_1^h, x_2^h, x_3^h, \dots, x_{n-1}^h, x_n^h), \\ x_2^{h+1} &= \Phi_2(x_1^{h+1}, x_2^h, x_3^h, \dots, x_{n-1}^h, x_n^h), \\ &\vdots \\ x_n^{h+1} &= \Phi_n(x_1^{h+1}, x_2^{h+1}, x_3^{h+1}, \dots, x_{n-1}^{h+1}, x_n^h). \end{aligned} \quad (9)$$

Задовољење критеријума конвергенције се проверава следећом релацијом:

$$\left|x_k^{h+1} - x_k^h\right| \le \varepsilon_x \wedge$$
$$\left|b_k - f_k(x_1^{h+1}, x_2^{h+1}, \dots, x_n^{h+1})\right| \le \varepsilon_f, \quad (10)$$
$$h = 1,2,3, \dots; \quad k = 1,2, \dots, n.$$

3. ПРИМЕНА ЊУТН-РАФСОНОВОГ ПОСТУПКА У ПРОРАЧУНУ ТОКОВА СНАГА

Математички модел произвољне преносне мреже (приказане погонским колом на слици 1) може се исказати са две реалне релације биланса снага, написаних у складу са методом независних напона, и то у адмитантној форми (релације (11) и (12)). Тим релацијама се могу описати сви чворови система, односно њихове инјектиране снаге и снаге које од тих чворова отичу у остатак система:

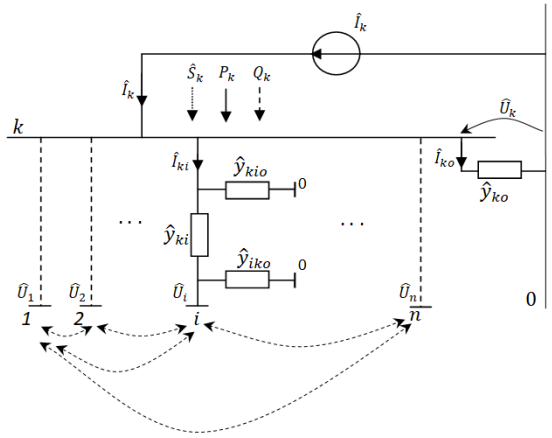
$$P_k = Re\left\{\hat{U}_k^* \sum_{i=1}^{n} \hat{Y}_{ki} \cdot \hat{U}_i\right\} \quad (11)$$

$$Q_k = -Im\left\{\hat{U}_k^* \sum_{i=1}^{n} \hat{Y}_{ki} \cdot \hat{U}_i\right\} \quad (12)$$

Сходно класичној класификацији чворова, независне променљиве овог модела су модули и углови напона (или само углови) чворова, а вредности инјкетираних снага (или бар активних) су познате вредности. Почетне апроксимације, у чијој околини се врше линеаризације, су претпостављене вредности, дате „flat-start“ приступом. Парцијалним изводима десних страна тих релација по свим (могућим) независним променљивама добијају се елементи матрице Јакобијана. Тиме се комплетира матрична форма модела токова снага, исказана релацијом (13). Неким од солвера заснованих на Гаусовој редукцији, или неком сличном нумеричком методу, се долази до решења система [3], [5].

$$\Delta \boldsymbol{S}^{h}_{(2n-2-p)\times 1} = \boldsymbol{J}^{h}_{(2n-2-p)\times(2n-2-p)} \Delta \boldsymbol{X}^{h}_{(2n-2-p)\times 1}. \qquad (13)$$

Са леве стране модела су одступања инјектираних снага, као познате вредности. Решење система чини вектор корекција апроксимација непознатих величина стања у текућој итерацији h, приказан вектор колоном на десној страни релације (13). Након задовољења критеријума, рачунају се непознате стања, на основу добијених корекција, и наредна апроксимација се проглашава решењем. Након тога је могуће реконструисати целокупни режим мреже.



Слика 1. *Опште поједностављено погонско коло дела преносне мреже*

4. ПРИМЕНА ПОСТУПКА СУМИРАЊА СТРУЈА И КОРЕКЦИЈА НАПОНА У ПРОРАЧУНУ ТОКОВА СНАГА

Дистрибутивне мреже, услед, махом, радијалне структуре и димензија модела, захтевају другачији тип алгоритма за прорачун токова снага. Дистрибутивна радијална мрежа (приказана на слици 2) моделована је „Г-сегментима“ и нумерисана по слојевима. Тиме је извршена неопходна припрема за сам поступак [5].

Поступак описан у овој глави рада заснива се на сумирању струја од последњих слојева мреже ка корену, те корекцији напона чворова, у обрнутом смеру, посредством падова напона израчунатих на основу нових апроскимација струја редних грана.

Поступак сумирања струја и корекција напона (*BFS – Backward Forward Sweep*) може се представити следећим корацима:

1. Сумирање струја:

$$\hat{I}_k^{h+1} = \frac{\hat{S}_k}{\hat{U}_k^{*h}} + \hat{y}_{ok}\hat{U}_k^h + \sum_{j\in\alpha_k} \hat{I}_j^{h+1}, \qquad (14)$$
$$k = n, n-1, \dots, 3, 2;$$

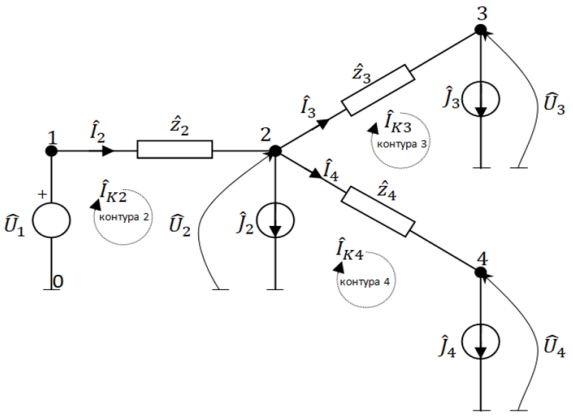
2. Корекција напона:

$$\hat{U}_k^{h+1} = \hat{U}_K^{h+1} - \hat{z}_k \hat{I}_k^{h+1} \qquad (15)$$
$$k = 2, 3, \dots, n;$$

3. Провера задовољења критеријуме конвергенције:

$$\left|\Delta\theta_k^h\right| \le \varepsilon_1 \ \wedge \ \left|\Delta U_k^h\right| \le \varepsilon_2. \qquad (16)$$

Решења модела су комплексни напони чворова, на основу којих се врши реконструкција режима мреже.



Слика 2. *„Г-сегменти“ дела радијалне мреже*

5. ТОКОВИ СНАГА ИНТЕГРИСАНИХ ПРЕНОСНО-ДИСТРИБУТИВНИХ МРЕЖА

Поступак предложен у овом раду представља једну од две различите подврсте метода раздвајања. Прва прописује да једна субпроцедура размењује резултате са другом, тек након конвергенције по својим критеријумима. Комплетан прорачун се завршава задовољењем додатног критеријума конвергенције, услед постојања још једне итеративне шеме, поред већ постојеће две. Друга подврста (којој припада предложени поступак) прописује да се размена (међу)резултата врши у току једне итерације. То значи да постоји само једна итеративна шема и истовремена провера критеријума конвергенције за обе субпроцедуре. Њутн-Рафсонов поступак (Глава 3) и „*BFS*“ поступак (Глава 4) представљају те субпроцедуре. Поступак се излаже над уопштеним примером интегрисане мреже, састављене из дела преносне мреже од n чворова у чијих су неколико чворова прикључене дистрибутивне мреже од по m чворова. Претпоставља се да је целокупна интегрисана мрежа уравнотежена и да је режим симетричан.

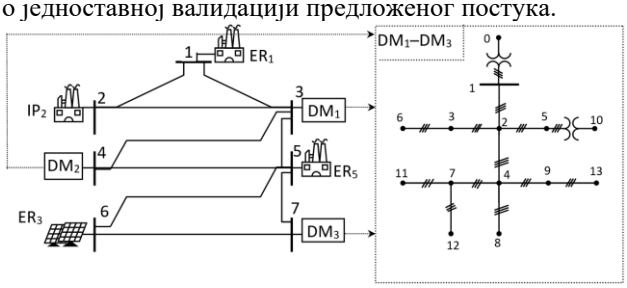
Припреме свих мрежа, као почетак поступка, су независне. Итеративни део почиње кораком сумирања струја дистрибутивних подручја. Он резултује, у вредностима снага потрошње тих подручја. Те снаге представљају улазе за Њутн-Рафсонов поступак. Након извршења целе итерације те субпроцедуре, добијају се нове апроксимације модула и углова напона чворова преносне мреже. Са тим вредностима поступак се наставља од дела намењеног дистрибуцији. Извршава се корекција напона, након које се располаже новим апроксимацијама величина стања целокупне интегрисане мреже. Следећим кораком се проверава задовољење критеријума конвергенције. Врши се за сваки део постпука независно. Када се критеријуми задовоље, врши се реконструкција режима. У супротном, прелази се наредну итерацију, те се понављају описани кораци.

Једна од кључних особина предложеног поступка јесте моменат размене (међу)резултата. Таква интеракција између два дела поступка даје чвршћу међузависност, него код метода раздвајања првог типа. Такође, битна особина овог поступка јесу ефикасности одабраних алгоритама који га сачињавају [2], [3], [4].

6. НУМЕРИЧКИ ПРИМЕР

У овој глави врши се тестирање предложеног поступка, на примеру интегрисане преносно-дистрибутивне мреже, приказане на слици 3 [9]. Подсистем преноса јесте напонског нивоа 110 [kV], док је остатак података дат у табелама 1, 2 и 3. Потрошње чворова дистрибутивних подручја јесу 200 [kW] и 67 [kVAR], редом. Режим дистрибутивне мреже је апроксимиран симетричним режимом, са једнаким потрошњама по чворовима и искључиво радијалне структуре.

Поступак је обрађен у програмском језику Фортран. Резултати прорачуна, изложени у наставку, су неке очекиване вредности и понашања, с обзиром да се ради о једноставној валидацији предложеног постука.



Слика 3. *Пример интегрисане преносно-дистрибутивне мреже*

У табели 4 приказане су вредности напона чворова преносне мреже, након конвергенције прорачуна, а на слици 4 вредности инјектираних снага по чворовима и токови снага по водовима. Процентуалне вредности снага губитака су испод 1 [%]. Чвор 2 има највећу потрошњу и активне и реактивне снаге, те је и оправдан најнижи модуо и угао напона на његовим сабирницама. Чвор 6 има највећу вредност модула напона, без обзира што се највише снаге инјектира у чвору 5, јер је чвор 6 типа PV (вредност задатог модула напона, из табеле 2). Исти закључак се може уочити и на примеру токова снага у једној од дистрибутивних мрежа (слика 5). Са графика, датог сликом 6, може се приметити да је највећи пад напона присутан између чворова 1 и 2. Разлог томе јесте што се у другом слоју налази само једна грана, тј. са ње се напаја највећа количина потрошње. Променом топологије (уз исте остале факторе: профил потрошње, радијална структура, параметри) се могу променити напонске прилике у мрежи. Сваки од тих појединачних фактора, или њихова комбинација, мења напонске прилике.

Табела 1. *Параметри преносног и дистрибутивних подсистема*

	$r^+[\Omega]$	$x^+[\Omega]$	$g^+[\text{nS}]$	$b^+[\mu\text{S}]$	l [km]
ПМ	0,01	0,336	2,6	0,33	60
ДМ	0,3465	1,0179	0,0	6,2998	0.6096

Табела 2. *Управљачке стратегије енергетских ресурса*

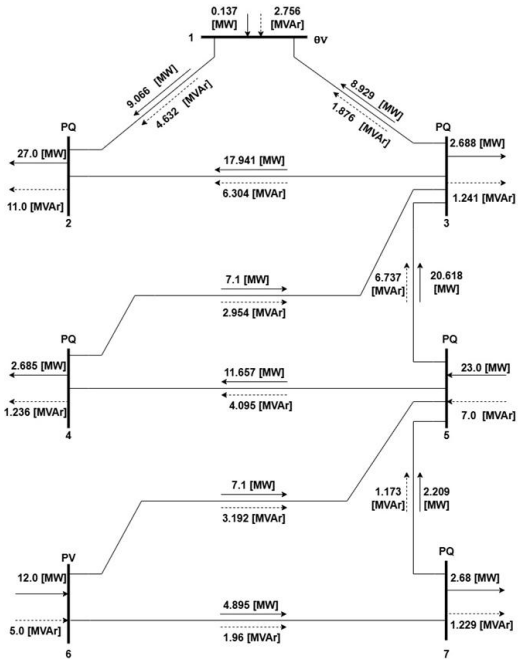
Енергетски ресурс/индустријска потрошња	$P_{inj}^{3\sim}$ [MW]	$Q_{inj}^{3\sim}$ [MVAr]	Модул напона [kV]
IP_2	-27,0	-11,0	/
ER_5	23,0	7,0	/
ER_6	12,0	/	112,364

Табела 3. *Подаци о трансформаторима*

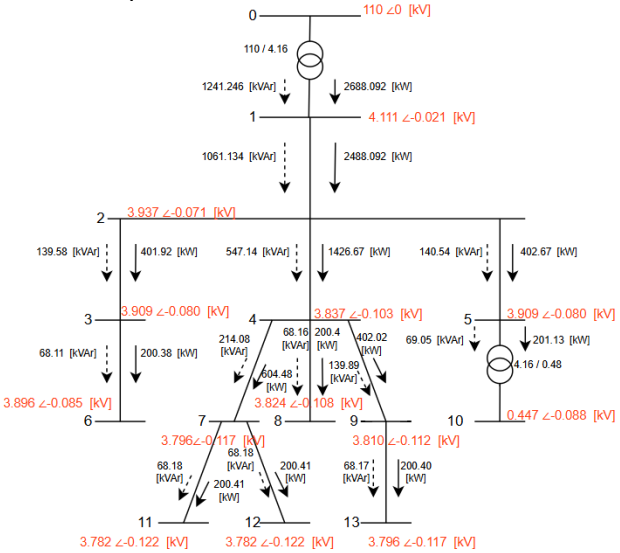
	Vn1 [kV]	*Vn2* [kV]	*R* [%]	*X* [%]	*Sn* [kVA]
TR 1	110,0	4,16	1,0	8,0	5000,0
TR 2	4,16	0,48	1,1	2,0	500,0

Табела 4. *Напонски профили чворова преносне мреже*

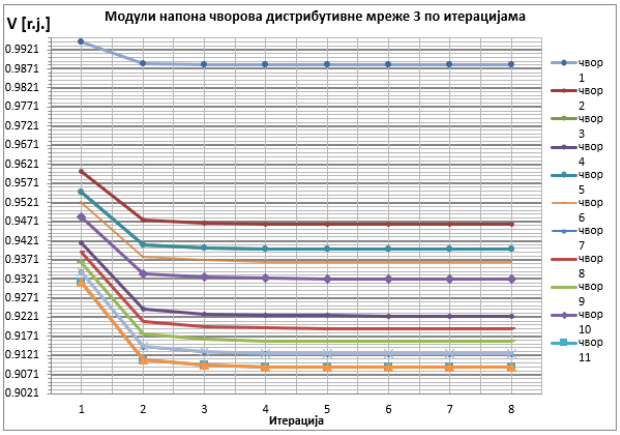
	Модуо напона		Угао
Чвор	[kV]	[r.j.]	[rad]
1	110,00000	1,00000	0,00000
2	109,09184	0,99174	-0,01499
3	110,38258	1,00347	0,01474
4	110,96073	1,00873	0,02935
5	111,76524	1,01604	0,04811
6	112,36400	1,02149	0,05937
7	111,96713	1,01788	0,05162



Слика 4. *Инјектиране снаге чворова и токови снага по водовима преносног подсистема*



Слика 5. *Напонски профили и токови снага једне дистрибутивне мреже*



Слика 6. *Модули напона чворова дистрибутивне мреже кроз итерације*

7. ЗАКЉУЧАК

Прорачуни токова снага заузимају централно место међу прорачунима у електроенергетским и дистрибутивним менаџмент системима. Неопходност поузданости и ефикасности њихових резултата је на високом нивоу, што чини њихову област истраживања стално отвореном за нове предлоге и решења.

Традиционални приступ проблему токова снага, који диктира независтан приступ анализама стања преносних и дистрибутивних мрежа, актуелан је већ деценијама. С друге стране, децентрализација електроенергетских система, у последње време, добија на значају и све више утиче на природу токова снага у мрежи. Тај утицај усложњава међузависности дистрибутивних и преносних подсистема, и тиме ствара потребу за развојем неких нових алгоритама који ће веродостојније анализирати стање мреже. Тај развој је мотивисао настанак целокупне нове области истраживања, која нуди предлоге интегрисаних поступака прорачуна токова снага над интегрисаним преносно-дистрибутивним мрежама.

У овом раду предложено је једно решење за прорачун токова снага интегрисаних преносно-дистрибутивних мрежа. Развијена процедура настала је синтезом два традиционална поступка: Њутн-Рафсоновог и поступка сумирања струја и корекција напона. Први поступак је оптималан за обраду преносних, док је други оптималан за обраду дистрибутивних мрежа.

Предложени интегрисани поступак је тестиран на једноставном примеру преносно-дистрибутивне мреже. Резултати добијени тим прорачуном осликавају очекиване вредности, с обзиром на улазне податке и пример мреже. Вредности модула и углова напона чворова, након прорачуна, налазе се у очекиваним границама. Један од мноштва могућих тема за даља истраживања би могла бити развој и тестирање овог поступка на примеру несиметричних режима у интегрисаним мрежама.

8. ЛИТЕРАТУРА

[1] https://www.intel.com/-content/www/us/en/developer/tools/oneapi/onemkl.html (приступљено у марту 2025.)

[2] Стрезоски Ц. Владимир, *Основни прорачуни електроенергетских система*, Том I. Нови Сад, Србија: ФТН издаваштво, 2017.

[3] Војновић Никола, „Прорачун токова снага неуравнотежених мрежа са енергетским ресурсима прикљученим на мрежу преко уређаја енергетске електронике“, докторска дисертација, Факултет техничких наука, Нови Сад, 2018.

[4] Стрезоски В. Реља, „Теоријска заснованост прорачуна симетричних токова снага радијалних дистрибутивних мрежа“, дипломски рад, Факултет техничких наука, Нови Сад, 2011.

[5] Стрезоски Ц. Владимир, *Основни прорачуни електроенергетских система*, Том II. Нови Сад, Србија: ФТН издаваштво, 2017.

DOI: https://doi.org/10.24867/34BE21Jocic

DOI: https://doi.org/10.24867/34BE21Jocic

DOI: https://doi.org/10.24867/34BE21Jocic

[9] IEEE Test feeder,https://cmte.ieee.org/pes-testfeeders/resources/. 13-bus feeder.(приступљено у марту 2025.)

Кратка биографија:

Коста Јоцић рођен је у Новом Саду 1996.год. Дипломирао је на Факултету техничких наука из области Електротехнике и рачунарства – Електроенергетски системи 2019. године.

Никола Војновић рођен је у Новом Саду, 1987. год. Дипломирао је, мастерирао и докторирао на Факултету техничких наука у Новом Саду из области Електротехнике и рачунарства.

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.38
DOI: https://doi.org/10.24867/34BE22Tufegdzic

NAPREDNA KONTROLA TROFAZNOG IŠM NAPONSKOG INVERTORA POVEZANOG NA MREŽU PREKO REZONANTNOG LCL FILTRA

ADVANCED CONTROL OF A THREE-PHASE VOLTAGE-SOURCE INVERTER CONNECTED TO THE GRID VIA A RESONANT LCL FILTER

Marijana Tufegdžić, Vladimir Popović, Fakultet tehničkih nauka, Novi Sad

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom master radu modeluje se i razmatra napredna kontrola trofaznog impulsno-širinski modulisanog (IŠM) naponskog invertora povezanog na krutu električnu mrežu preko rezonantnog LCL filtra. Rad obuhvata modelovanje sistema u različitim koordinatnim sistemima, analizu rezonantnih pojava u LCL filtru, kao i tehnike njihovog pasivnog i aktivnog prigušenja. Posebna pažnja posvećena je dizajnu upravljačke strukture zasnovane na kaskadnoj regulaciji sa kontrolom kvadrata napona jednosmernog kola i regulaciji vektora struje uz primenu fazno-zaključne petlje.*

Abstract – *This master thesis focuses on the modeling and advanced control of a three-phase pulse-width modulated (PWM) voltage source inverter connected to a stiff electrical grid via a resonant LCL filter. The work includes system modeling in various coordinate frames, analysis of resonant phenomena within the LCL filter, and the implementation of both passive and active damping techniques. Special attention is given to the design of a cascaded control structure based on the regulation of the square of the DC-link voltage and the vector control of the grid current using a phase-locked loop (PLL).*

Ključne reči: *rezonantni LCL filtar, pasivno i aktivno prigušenje, tokovi snaga, regulacija napona DC kola*

1. UVOD

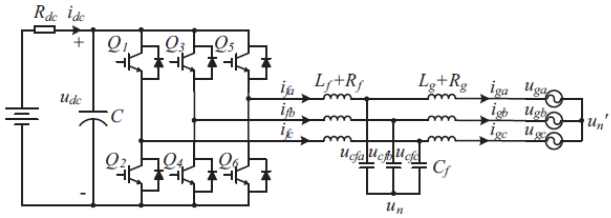
Razvoj distributivnih energetskih sistema i povećanje udela energetske elektronike u savremenim elektro-energetskim mrežama uslovljavaju sve širu primenu trofaznih naponskih pretvarača. Sve strožiji tehnički zahtevi u pogledu kvaliteta energije, elektromagnetne kompatibilnosti i stabilnosti sistema doveli su do zamene uobičajene topologije sa *L* izlaznim filtrom sa topologijom koja sada ima rezonantni *LCL* filtar. Pored sposobnosti *LCL* filtra da omogućava efikasnije potiskivanje viših harmonika, njegova upotreba uvodi kompleksnu dinamiku u sistem, uključujući pojavu rezonantnih učestanosti koje mogu ugroziti stabilnost, [1].

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Vladimir Popović, docent

U ovom radu razvijen je usrednjeni model trofaznog impulsno-širinski modulisanog (*IŠM*) naponskog pretvarača povezanog na krutu trofaznu mrežu preko *LCL* filtra. Posebna pažnja posvećena je upravljačkoj strukturi zasnovanoj na kaskadnoj regulaciji – vektorskoj regulaciji struje sa sinhronizacijom na ugao fazor mrežnog napona pomoću fazno–zaključne petlje i regulaciji kvadrata napona jednosmernog međukola.

2. MODELOVANJE TROFAZNOG *IŠM* PRETVARAČA PREMA MREŽI SA *LCL* FILTROM

Jednačine trofaznog sistema strujnog kola naponskog invertora sa *LCL* filtrom mogu se jednostavno dobiti sagledavanjem *Slike 1*, uz pretpostavke da je mreža kruta i predstavljena idealnim trofaznim naponskim izvorom, [2].



Slika 1. *Tipična struktura trofaznog naponskog invertora povezanog na krutu mrežu preko LCL filtra*

Dobijeni usrednjeni matematički model pretvarača prema mreži sa *LCL* filtrom u sinhrono-rotirajućem *dq* sistemu je najpogodniji za kontrolu, jer su sve izvedene veličine jednosmerne.

$$L_f \cdot \frac{d\boldsymbol{i_f}}{dt} + R_f \cdot \boldsymbol{i_f} = -\omega \cdot L_f \cdot \boldsymbol{J} \cdot \boldsymbol{i_f} + \frac{u_{dc}}{2} \cdot \boldsymbol{S} - \boldsymbol{u_{cf}} \quad (1)$$

$$C_f \cdot \frac{d\boldsymbol{u_{cf}}}{dt} = -\omega \cdot C_f \cdot \boldsymbol{J} \cdot \boldsymbol{u_{cf}} + \boldsymbol{i_f} - \boldsymbol{i_g} \quad (2)$$

$$L_g \cdot \frac{d\boldsymbol{i_g}}{dt} + R_g \cdot \boldsymbol{i_g} = -\omega \cdot L_g \cdot \boldsymbol{J} \cdot \boldsymbol{i_g} + \boldsymbol{u_{cf}} - \boldsymbol{u_g} \quad (3)$$

$$C \cdot \frac{du_{dc}}{dt} = i_{dc} - \frac{3}{2} \cdot \boldsymbol{S} \cdot \boldsymbol{i_f} \quad (4)$$

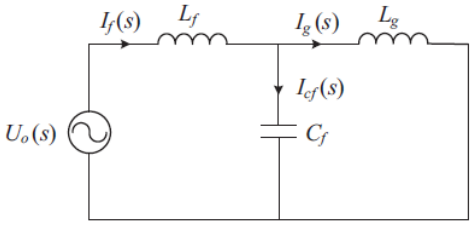
gde su:

- $\boldsymbol{i_f} = [i_{fd} \quad i_{fq}]^T$ – vektor struje mreže;
- $\boldsymbol{i_g} = [i_{gd} \quad i_{gq}]^T$ – vektor struje pretvarača;
- $\boldsymbol{i_{cf}} = [i_{cfd} \quad i_{cfq}]^T$ – vektor struje kroz granu filtarskog kondenzatora;
- $\boldsymbol{u_{cf}} = [u_{cfd} \quad u_{cfq}]^T$ – vektor napona na filtarskom kondenzatoru
- $\boldsymbol{u_g} = [u_{gd} \quad u_{gq}]^T$ – vektor napona mreže
- L_f – induktivnost rezonantnog *LCL* filtra sa strane pretvarača
- C_f – kapacitivnost rezonantnog *LCL* filtra

- L_g – induktivnost rezonantnog *LCL* filtra sa strane mreže
- C – kapacitivnost u jednosmernom kolu
- $\boldsymbol{S}$ – određuje faktore ispune digitalnog *IŠM* modulatora

3. KONFIGURACIJA *LCL* FILTRA

Kako su i pretvarač energetske elektronike i električna mreža naponski izvori, kao takvi ne mogu se neposredno spojiti. Za ublažavanje oscilacija izmedju dva ovako sučeljena naponska izvora induktivnost mreže se pojačava sprežnim elementima. Ovaj rad analizira slučaj *LCL* filtra kao sprežnog elementa, što se najčešće primenjuje u praksi, prikazano na *Slici 2*, [1].



Slika 2. *Pojednostavljeno pofazno ekvivalentno kolo LCL filtra*

U nastavku će biti opisana neželjena pojava rezonancije *LCL* filtra kao i tehnike za njeno prigušenje.

3.1. Rezonancija *LCL* filtra

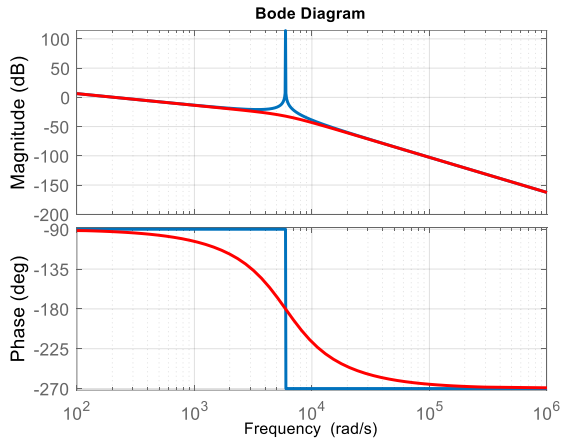
Funkcija prenosa *LCL* filtra glasi:

$$Y_{LCL}(s) = \frac{I_g(s)}{U_0(s)} = \frac{1/(L_f + L_g)}{s} \cdot \frac{\omega_{res}^2}{s^2 + \omega_{res}^2} \tag{5}$$

gde je rezonantna učestanost ω_{res}:

$$\omega_{res} = 2 \cdot \pi \cdot f_{res} = \sqrt{\frac{L_f + L_g}{L_f \cdot L_g \cdot C_f}} \tag{6}$$

Na *Slici 3* plavom bojom prikazane su amplitudska i fazna Bodeova karakteristika *LCL* filtra sa ne prigušenom rezonantnom pojavom. Izraziti pik amplitude na rezonantnoj učestanosti i brza tranzicija faze u njenoj okolini, ukazuju na probleme sa stabilnošću sistema.

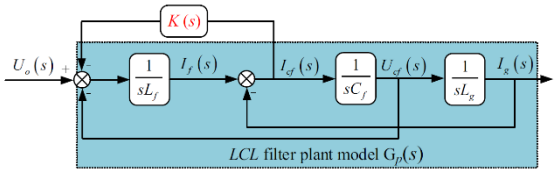


Slika 3. *Bodeov dijagram otvorene petlje VSC sa LCL filtrom sa i bez prigušenja rezonancije; parametri Tabela I, sekcija 5*

3.2. Tehnike prigušenja rezonantnih pojava

Postoje dva osnovna pristupa za prigušenje rezonantnih pojava, pasivni i aktivni pristup.

Pasivno prigušenje se ostvaruje dodavanjem otpornika na red sa kondenzatora *LCL* filtra, pri čemu se vodi računa da vrednost tog otpornika bude što manja kako bi se ograničili gubici. Ovakvom izvedbom uspešno se disipira akumulirana energija i pomera rezonantna frekvencija, [1].



Slika 4. *Blok dijagram LCL filtra sa implementacijom aktivnog prigušenja sa povratnom spregom po struji kondenzatora*

Tehnika aktivnog prigušenja koristi se kada se želi zadržati efikasnost bez dodatnih disipativnih elemenata. Kako je sama rezonansa prouzrokovana filtarskim kondenzatorom potrebno je obraditi informacije o struji i naponu grane kondenzatora i izvršiti korekciju po naponu pretvarača kao na *Slici 4*, [2].

Funkcija prenosa sa aktivnim prigušenjem, gde je K pojačanje po struji otočne grane kondenzatora, glasi:

$$Y_{LCL}(s) = \frac{I_g(s)}{U_0(s)} = \frac{1/(L_f + L_g)}{s} \cdot \frac{\omega_{res}^2}{s^2 + 2\xi\omega_{res} \cdot s + \omega_{res}^2} \tag{7}$$

Sa definisanim relativnim prigušenjem ξ:

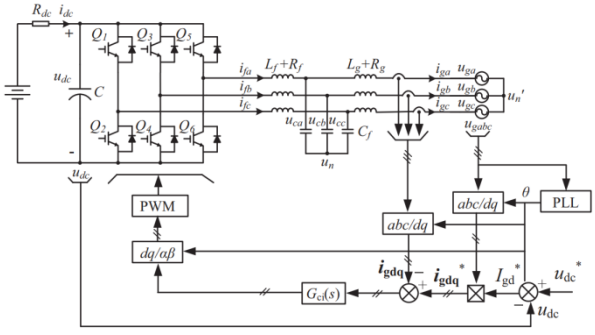
$$\xi = \frac{K\sqrt{C_f L_g}}{2\sqrt{{L_f}^2 + L_f L_g}} \tag{8}$$

Jasno je da, što je pojačanje K veće, veće je i relativno prigušenje ξ. Preporučuje se takav izbor vrednosti K da ξ bude $1/\sqrt{2}$ ili $1/2$.

Na *Slici 3*, sa crvenom linijom, prikazan je Bodeov dijagrama za slučaj uvaženog prigušenja ω_{res}. Značajno ublaženi pik i omekšana fazna tranzicija omgućavaju bolju i stabilniju kontrolu.

4. PREDLOG NAPREDNE KONTROLE TOKOVA SNAGE U KONFIGURACIJI *VSC* SA *LCL*

Stabilan i efikasan rad trofaznog *IŠM* pretvarača namenjenog za kontrolu tokova snage na mreži preko *LCL* filtra podrazumeva implementaciju kontrolera vektora struje mreže u sinhrono–rotirajućem dq koordinantom sistemu osa orijentisanim na fazor mrežnog napona u konfiguraciji kaskadnog sistema sa nadređenom petljom regulacije napona međukola, *Slika 4*, [2].

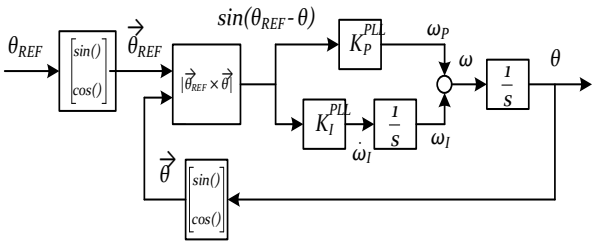


Slika 4. *Kontrola VSC u dq – koordinatnom sistemu*

4.1. Sinhronizacija sa *PLL* algoritmom i nadzor snage

Za pravilnu sihnronizaciju pretvarača energetske elektronike sa električnom mrežom na koju se on povezuje, koristi se fazno–zaključna petlja (*engl. Phase Locked Loop – PLL*), *Slika 5*.

Kada *PLL* sustigne ugao fazora mreže i kada se taj fazor poklopi sa d osom, q komponenta postaje jednaka nuli. Tako, uz pretpostavku da je mreža kruta i da je *PLL* dobro podešen, regulacijom struja po d i q osi neposredno se upravlja tokom snage (d komponenta upravlja aktivnom, a q komponenta reaktivnom snagom), [3].



Slika 5. *Nelineani PLL za sinhronizaciju ugla mreže* θ_{ref}

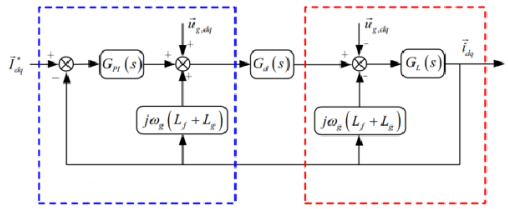
Funkcija prenosa *PLL* drugog reda sa *PI* regulatorom za kontrolu praćenja reference ugla i sinteza parametara na osnovu željenog prigušenja ζ i neprigušene prirodne učestanosti ω_n glase [3]:

$$G_{PLL}(p) = \frac{K_P^{PLL} \cdot p + K_I^{PLL}}{p^2 + K_P^{PLL} \cdot p + K_I^{PLL}} \tag{9}$$

$$\zeta = \frac{K_P^{PLL}}{2\sqrt{K_I^{PLL}}}, \omega_n = \sqrt{K_I^{PLL}} \tag{10}$$

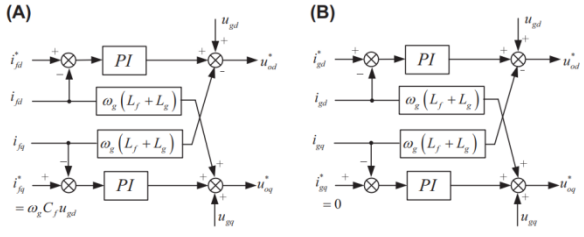
4.2. Regulacija vektora struje mreže

Preduslov za efikasno upravljanje tokovima snaga jeste da se obezbedi injekcija vektora struje pretvarača. Kod konfiguracije *VSI* pretvarača potrebno je naponsko napajanje pretvoriti u strujno regulisano, *CRVSI* (*engl. Current Regulated VSI*). Merenjem i povratnom vezom po struji može predašnje obezbediti, *Slika 6*, [2].



Slika 6. *Strujna nadzorna petlja sa prikazanim regulatorom (plava) i objektom upravljanja (crvena)*

Zavisno od trenutnih pozicija senzora struje, postoje dve varijante nadzornog sklopa, kontrola po struji pretvarača (šema sa *Slike 7A*) i kontrola po struji mreže (šema sa *Slike 7B*).



Slika 7. *Regulator vektora struje; pretvarača (levo - A); mreže (desno - B)*

Regulacija vektora struje realiovana je paralelnom akcijom dva nezavisna strujna regulatora. Iskorišćeni su *PI* regulatori u granama pod d po q osi sa rasprežućim članovima usled postojanja induktivnih padova napona. Impedansa kapacitivne grane *LCL* filtra je zanemarljivo mala na učestanosti mreže, pa je svrsishodno zanemariti njen uticaj prilikom dizajna strujnog nadzora.

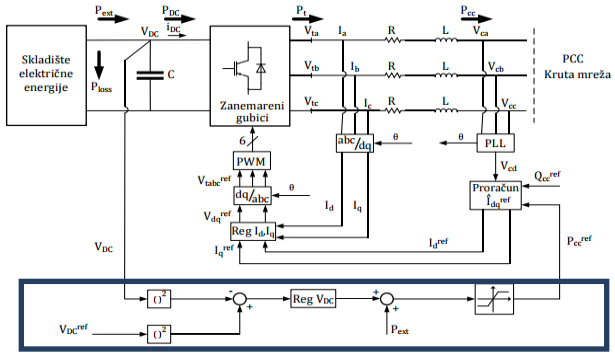
Parametri *PI* regulatora struje, K_{pI} i K_{iI} se biraju na sledeći način:

$$K_{iI} = \frac{\omega_{nI}^2}{(L_f + L_g)}, \qquad K_{pI} = \frac{2\xi_I \omega_{nI}}{(L_f + L_g)} \tag{11}$$

gde ξ_I i ω_{nI} predstavljaju faktore relativnog prigušenja i i neprigušene prirodne učestanosti petlje struje.

4.3. Nadzor napona jednosmernog kola

Nagli porast ili pad napona jednosmernog kola pretvarača može dovesti do preopterećenja ili kvarova pretvarača, kondenzatora, filtera i drugih komponenti. Ovom regulacijom obezbeđuje se pouzdana i dugotrajna upotreba pretvarača i sistema u kom je on postavljen, prikazano na *Slici 8*, [1].



Slika 8. *Nadređena kontrolna petlja napona DC kola*

Nadređena petlja za regulaciju napona *DC* međukola, V_{DC} obezbeđuje kontrolu toka aktivne snage koja se injektuje u mrežu P_{cc}^{ref}. Ukoliko je stvarna vrednost napona *DC* međukola veća od vrednosti koja je zadata tj referentna ($V_{DC} > V_{DC}^{ref}$), postoji višak uskladištene energije u *DC* međukolu. Akcija regulatora je povećanje P_{CC}. u cilju korekcija (smanjenja) napona. Pri izlasku iz regulatora dodaje se *feed–forward* član koji daje uvid u dodatnu injekciju snage P_{ext} iz izvora enegije (blok Skladište električne energije) kako bi se uklonio uticaj na direktnu granu regulacije. Reaktivna snaga Q_{cc}^{ref} može zadavati po želji, sve dok je to u granicama strujnih mogućnosti pretvarača.

Uskladnik napona jednosmernog kola projektovan je kao *PI* regulator, pri čemu se parametri biraju tako da se obezbedi stabilan odziv bez oscilacija i sa što manjim vremenskim kašnjenjem. Analiza regulacionog sklopa i sinteza parametara regulatora *DC* međukola je detaljno opisana u [1].

5. EKSPERIMENTALI REZULTATI

U nastavku se vrši eksperimentalna verifikacija algoritma za regulaciju injektovane aktivne snage ka mreži i naponskih prilika sa strane pretvarača u slučaju *LCL* filtra kao sprežnog elementa, prikazano na *Slici 4*.

Prvo se kvantifikuju parametri mreže i kontrolera, a zatim se vrše relevantni testovi tokova snaga i kontrole napona sistema.

5.1. Konfiguracija eksperimentalne postavke

U *Tabeli I* prikazani su parametri električne mreže, sprežnog *LCL* filtra i *DC* kola, dok *Tabela II* pruža informacije o pojačanjima kontrolera.

Tabela I. *Parametri električnog sistema*

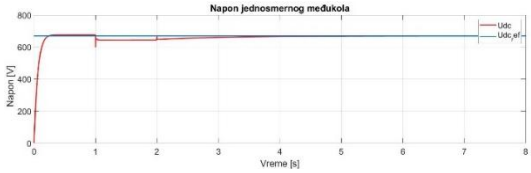
Parametar	*Vrednost[veličina]*
f_g	50[Hz]
U_l	400[V]
L_f	$3 \cdot 10^{-3}$[H]
L_g	$1.8 \cdot 10^{-3}$[H]
C_f	$25 \cdot 10^{-6}$[μF]
$R_f = R_g$	0.15[Ω]
ω_{res}	$5.96 \cdot 10^{3}$[rad/s]
U_{DC}	670[V]
R_{DC}	0.5[Ω]
E	680[V]

Tabela II. Pojačanja kontroler

Parametar	*Vrednost[veličina]*
K_{p_i}	12[V/A]
K_{i_i}	750[V/As]
K_{p_pll}	$9 \cdot 10^{3}[s^{-1}]$
K_{i_pll}	$20.25 \cdot 10^{6}[s^{-2}]$
K_d	25.3[V/A]

5.2. Eksperimentalna analiza

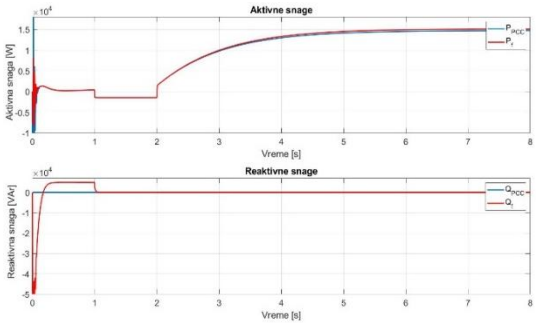
Vrši se test injektovanja aktivne snage u mrežu kontrolom napona *DC* kola. Nakon vremena potrebnog za sinhronizaciju *PLL* i uspostavljanja naponskih prilika u mreži, u vremenskoj instanci $t = 2s$ zadaje se referenca napona *DC* kola od $V_{DC}^{ref} = 670V$. Pri simetričnim uslovima u elektroenergetskoj mreži trofaznog linijskog napona $400V$, $50Hz$ sa konfiguracijom parametara iz *Tabele I* garantuje injekciju aktivne snage. Referentna vrednost reaktivne snage ka mreži je jednaka nuli.



Slika 9. *Odziv napona jednosmernog međukola pretvarača (crvena) pri zadatoj referenci (plava)*

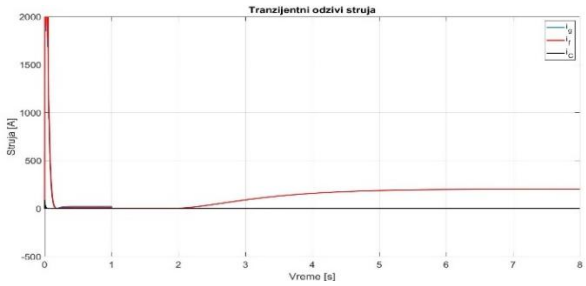
Sa *Slike 9* se jasno uočava konvergencija napona jednosmernog međukola (crvena) ka referenci (plava) nakon zadavanja iste. Tranzijentni proces traje $4s$. Posledica uvećanja naponskih prilika sa strane pretvarača rezultuje injekcijom aktivne snage ka mreži.

Na *Slici 10* prikazane su komponente aktivnih snaga pretvarača i mreže, gornji grafik. Ove snage su bliske po vrednosti, što potvrđuje da su gubici na *LCL* filtru zanemarivi. Sa iste slike, donji grafik, uočava se nenulta reaktivna snaga pretvarača koja se celokupna troši na *LCL* filtru. Posledično, reaktivna energija koja se injektuje u mrežu iznosi nula i odgovara referentnoj vrednosti nametnutoj od strane kontrolera.



Slika 10. *Prikaz aktivne i reaktivne snage pretvarača (crvena) i mreže (plava) nakon trenutka zadavanja reference; Gornji grafik-aktivne snage, donji grafik-reaktivne snage*

Odzivi sa *Slike 11* prikazuju module vektora struja pretvarača, mreže i struje kroz otočni kondenzator.



Slika 11. *Tranzijentni odziv amplitude vektora struje pretvarača (crvena), mreže (plava) i otočne struje kroz kondenzator (crna)*

6. ZAKLJUČAK

U radu je izvršeno modelovanje i analiza trofaznog naponskog pretvarača povezanog na mrežu preko *LCL* filtra, uz detaljno ispitivanje rezonantnih pojava. Predložena upravljačka struktura sa kaskadnom regulacijom i fazno-zaključanom petljom pokazala je dobru dinamiku i efikasno prigušenje harmonika. Dobijeni rezultati potvrđuju da ovakav pristup obezbeđuje stabilan rad pretvarača i zadovoljava zahteve kvaliteta energije.

7. LITERATURA

[1] Frede Blaabjerg, Control of power electronic converters and systems, Volume 3, 2021.

[1] S.G. Parker, B.P. McGrath, D.G. Holmes, Regions of active damping control for LCL filters, IEEE Trans. Ind. Appl. 50 (1) (2013) 424e432.

[3] F. Blaabjerg, R. Teodorescu, M. Liserre, A.V. Timbus, Overview of control and grid synchronization for distributed power generation systems, IEEE Trans. Ind. Electron. 53 (5) (October 2006) 1398e1409

Kratka biografija:

Marijana Tufegdžić je rođena u Sremskoj Mitrovici 2000. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Energetska elektronika i električne mašine odbranila je 2023. god.

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.75
ДОИ: https://doi.org/10.24867/34BE23Colovic

Развој од-краја-до краја шифрованог блокчејн протокола за преговоре и повраћај средстава након експлоатације на *Ethereum* мрежи

Development of an end-to-end encrypted blockchain protocol for negotiation and return of funds after an Ethereum network exploit

Алекса Чоловић, *Факултет техничких наука, Нови Сад*

Студијски програм – ПРИМЕЊЕНЕ РАЧУНАРСКЕ НАУКЕ И ИНФОРМАТИКА – ЕЛЕКТРОНСКО ПОСЛОВАЊЕ

Кратак садржај – *Овај рад представља RESET платформу децентрализовани Web3 протокол који омогућава сигурну, приватну и проверљиву комуникацију између компромитованих протокола и нападача. Рад описује архитектура система, коришћене технологије, имплементација паметних уговора и дизајн клијентске апликације.*

Кључне речи: *блокчејн, паметни уговори, Web3, Ethereum*

Abstract – *This paper presents RESET – a decentralized Web3 protocol enabling secure and verifiable post-exploit negotiations between hacked protocols and attackers. The paper describes system architecture, smart contract implementation and client application design.*

Keywords: *blockchain, smart contracts, Web3, Ethereum*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Душан Гајић, ванред. проф.

1. УВОД

Безбедност у децентрализованим финансијама (ДеФи) представља један од кључних изазова савремених блокчејн система. Упркос напретку у развоју паметних уговора и сигурносних механизама, хакерски напади на протоколе и даље су учестала појава, што доводи до значајних финансијских губитака. Према доступним подацима, само у 2022. години забележено је 231 великих сигурносних инцидената, са укупном штетом од око 3,7 милијарди долара [1]. Иако нападачи често нису мотивисани искључиво крађом, већ су спремни на преговоре и повраћај дела средстава у замену за избегавање правних последица, тренутни процес преговарања одвија се путем несигурних и неформалних канала, што отвара простор за манипулације и додатне ризике за нападаче.

RESET платформа решава овај проблем као децентрализовани *Web3* протокол који омогућава сигурну, приватну и проверљиву комуникацију између компромитованог протокола и нападача. Преговори се реализују путем енкриптованих порука чуваних на *Ethereum* мрежи, уз потпуну транспарентност трансакција. На тржишту тренутно не постоји познато решење које нуди сличан механизам, док се постојећи покушаји ослањају на *Web2* канале попут е-мејла или Телеграма, који не пружају гаранције приватности и интегритета. *RESET* уводи стандардизован процес без поверења за преговарање који је у потпуности на блокчејну, чиме се смањује ризик од манипулација и повећава вероватноћа постизања договора у безбедном окружењу.

Платформа омогућава власницима протокола да пријаве инцидент, дефинишу услове понуде за повраћај средстава, док нападачи могу да прихвате понуду или дају контрапонуду. Паметни уговори гарантују спровођење договорених услова без посредника, чиме се елиминише ризик од неиспуњених обавеза.

2. ПОЈАМ БЛОКЧЕЈН ТЕХНОЛОГИЈЕ

Блокчејн технологија је постала кључна основа за савремене дигиталне системе поверења, омогућавајући трансакције без посредника и централних ауторитета. Њена примена се посебно истиче у областима као што су финансије, управљање идентитетима и дигитална имовина, где су сигурност и транспарентност од пресудног значаја.

2.1. Дистрибуирани системи

Дистрибуирани систем чини скуп независних рачунарских елемената који кориснику делују као јединствена целина. Карактеришу га независност компоненти, њихова међусобна комуникација и кохерентност из угла корисника. У пракси, дистрибуирани системи често обухватају физички удаљене чворове ради веће доступности и отпорности на грешке.

2.2. Дистрибуирана главна књига

Дистрибуирана главна књига (енгл. *Distributed Ledger Technology* ДЛТ) представља специфичан тип дистрибуираног система без централног ауторитета, где учесници не морају веровати једни другима. Интегритет се обезбеђује криптографским механизмима и консензусним алгоритмима, што

омогућава децентрализацију, транспарентност и отпорност на манипулације. ДЛТ је основа за иновације попут ДеФи-а или НФТ-а.

2.3. Блокчејн

Блокчејн је најпознатија имплементација ДЛТ-а, заснована на линеарном ланцу криптографски повезаних блокова. Сваки блок садржи валидиране трансакције и хеш претходног блока, чиме се обезбеђује непроменљивост и сигурност података. Једном уписани подаци практично се не могу изменити без контроле над већином мреже, што блокчејн чини отпорним на цензуру и фалсификовање. Ова архитектура омогућава транспарентност и проверљивост, јер сви учесници могу независно верификовати историју трансакција. Први блокчејн систем, *Bitcoin* [2], уведен је 2009. године као одговор на потребу за децентрализованом дигиталном валутом, док је *Ethereum* проширио концепт увођењем паметних уговора, отварајући пут ка развоју комплексних децентрализованих апликација.

2.4. Алгоритми консензуса

Да би блокчејн мрежа функционисала без централног ауторитета, неопходно је да сви чворови постигну сагласност о валидности нових блокова. Овај процес обезбеђују консензусни алгоритми, међу којима су најпознатији *Proof of Work* [3] (*PoW*), *Proof of Stake* (*PoS*) [4] и њихове варијанте. *PoW* захтева решавање сложених криптографских задатака, чиме се гарантује сигурност уз високу потрошњу енергије, док *PoS* заснива избор валидатора на уложеним токенима, што смањује трошкове и повећава ефикасност. Поред ових, постоје и алгоритми попут *Practical Byzantine Fault Tolerance* [5], који се користе у приватним мрежама ради бржег постизања консензуса. Ови механизми чине основу децентрализације, јер спречавају манипулацију и обезбеђују интегритет података чак и у присуству злонамерних учесника.

3. ПАМЕТНИ УГОВОРИ

Паметни уговори представљају једну од најзначајнијих иновација у оквиру блокчејн технологије, јер омогућавају аутоматизовано, транспарентно и непроменљиво извршавање уговорних односа без посредника. Овај термин први је увео Ник Сабо [6]. За разлику од традиционалних уговора, који се ослањају на правне институције, судске механизме и поверење између страна, паметни уговори функционишу као програмски код имплементиран на блокчејну. Тиме се обезбеђује висок ниво сигурности, елиминација људске грешке и смањење трошкова трансакција. Њихова логика се извршава детерминистички, једном када су услови дефинисани и уговор постављен на мрежу, извршење је загарантовано без могућности произвољног мењања правила. Ова својства чине паметне уговоре погодним за окружења са ограниченим поверењем, јер се верификација заснива на криптографским механизмима и консензусним алгоритмима, а не на трећим странама.

Примена паметних уговора обухвата широк спектар области: од финансијских трансакција и управљања дигиталним идентитетима, преко аутоматизованих система плаћања и осигурања, до сложених пословних процеса у децентрализованим апликацијама. У ДеФи екосистему, паметни уговори омогућавају креирање протокола за позајмице, размену токена, стакинг и управљање ликвидношћу. Такође, паметни уговори у другим доменима подржавају токене засноване на стандардима (ЕРЦ-20, ЕРЦ-721), управљање власништвом над дигиталном имовином, па чак и имплементацију ДАО структура за колективно доношење одлука. Њихова непроменљивост и јавна проверљивост доприносе транспарентности, али истовремено намећу изазове у погледу флексибилности и скалабилности, јер свака грешка у коду може имати озбиљне последице. Управо због тога, развој паметних уговора захтева ригорозно тестирање, формалну верификацију и примену сигурносних образаца како би се обезбедила поузданост у реалним условима.

3.1. Писање паметних уговора

Писање паметних уговора подразумева дефинисање уговорних правила у облику програмског кода који се извршава на дистрибуираној блокчејн мрежи. За разлику од класичних апликација, код мора бити детерминистички, транспарентан и отпоран на манипулације, јер се извршава на великом броју независних чворова. Сваки чвор верификује резултат трансакције, а само идентични исходи бивају уписани у ланац блокова, чиме се обезбеђује интегритет и непоречивост извршења. Транспарентност се постиже јавном доступношћу изворног кода и историје трансакција, док се сигурност обезбеђује криптографским механизмима и консензусним алгоритмима. Због ових захтева, развој паметних уговора захтева пажљив дизајн, тестирање и примену безбедносних образаца, јер грешке могу имати директне финансијске последице. Правилно написан уговор представља основу поузданих и сигурних дигиталних трансакција у децентрализованом окружењу.

3.2. *Ethereum Virtual Machine EVM*

EVM [7] функционише као дистрибуирани глобални рачунар, где сваки чвор верификује и извршава код уговора, обезбеђујући сигурност и транспарентност. Паметни уговори се најчешће пишу у језику *Solidity*, а њихов код се извршава у изолованом виртуелном окружењу, чиме се спречава утицај на друге процесе. Писање директно у *EVM* бајткоду је непрактично, па се користе језици вишег нивоа. Поред *Solidity*-ја, користе се још и језици *Vyper* и *Yul*. *Ethereum* уводи концепт „гаса“ – свака операција има цену, што спречава злоупотребу ресурса и подстиче оптимизован код. Ови механизми чине *EVM* основом за поуздано и скалабилно извршавање паметних уговора.

4. *REACT*

React [8] је једна од најпопуларнијих *JavaScript* библиотека за развој модерних корисничких интерфејса, заснована на компонентном приступу и виртуелном ДОМ-у, што омогућава модуларност,

високе перформансе и једноставно одржавање кода. Његова декларативна природа и подршка за *JSX* синтаксу олакшавају развој интерактивних апликација, док *hook*-ови (попут *useState* и *useEffect*) поједностављују управљање стањима и асинхроним операцијама. Ове карактеристике чине *React* погодним за комплексне апликације, укључујући децентрализоване *Web3* системе.

4.1. Помоћне библиотеке

У контексту развоја децентрализованих апликација, *React* се често комбинује са библиотекама које проширују његову функционалност. *Ethers.js* омогућава директну интеракцију са *Ethereum* мрежом, управљање новчаницима, слање трансакција и позивање функција паметних уговора. *Wagmi*, заснован на *React*-у, додаје апстракције за повезивање крипто-новчаника као на пример *MetaMask*, управљање сесијама и праћење статуса трансакција, уз интеграцију са *React Query* библиотеком за кеширање и синхронизацију података. За рад са формама користи се *React Hook Form* библиотека, који обезбеђује ефикасну валидацију и минимално поновно исцртавање форме, што је кључно за перформансе. *SweetAlert2* библиотека доприноси побољшању корисничког искуства кроз приказ интерактивних обавештења и дијалога, посебно у критичним тачкама као што су потврде трансакција или обавештења о грешкама.

5. *SOLIDITY*

Solidity [9] је статички типизиран, објектно-оријентисан језик развијен за креирање паметних уговора на *Ethereum* мрежи. Синтакса је инспирисана *JavaScript*-ом, Ц++-ом и *Python*-ом, што олакшава учење и омогућава модуларност кроз наслеђивање, модификаторе и енкапсулацију. Паметни уговор се дефинише као скуп стања и функција, уз подршку за догађаје, грешке, структуре и енумерације. Сваки уговор почиње директивом *pragma* и кључном речи *contract*, а може да садржи променљиве стања, функције и контролне механизме. *Solidity* обезбеђује детерминистичко извршавање на *EVM*-у, при чему је правилно управљање меморијским контекстима (*storage, memory, calldata*) кључно за оптимизацију трошкова гаса и сигурност уговора. Захваљујући овим карактеристикама, *Solidity* је доминантан језик за развој децентрализованих апликација.

5.1. *OpenZeppelin* библиотека

OpenZeppelin [10] је стандардна библиотека отвореног кода која пружа аудитоване компоненте за развој сигурних паметних уговора u *Solidity*-ју. Садржи имплементације ЕРЦ стандарда, контролу приступа кроз *Ownable* и *AccessControl*, као и заштиту од напада попут *reentrancy*-ја помоћу *ReentrancyGuard*. Њена употреба значајно смањује ризик од грешака и убрзава развој ослањајући се на најбоље праксе индустрије.

6. ИМПЛЕМЕНТАЦИЈА *RESET* ПЛАТФОРМЕ

RESET платформа је пројектована као потпуно децентрализовано решење које елиминише потребу за централизованим серверима и базама података. Архитектура платформе обухвата три кључне компоненте: паметне уговоре који чувају пословну логику и податке, *The Graph* протокол за индексирање и претрагу информација са блокчејна, и клијентску апликацију која омогућава интеракцију корисника са системом. Овакав приступ обезбеђује сигурност, транспарентност и отпорност на манипулацију.

6.1. Паметни уговори *RESET* платформе

Језгро система чини скуп модуларних паметних уговора који управљају инцидентима, разменом порука, обрачуном накнада и емитовањем догађаја. Сваки уговор имплементира јасно дефинисане интерфејсе, што омогућава флексибилност и једноставну надоградњу без утицаја на друге компоненте. Као репрезентативан пример, *Incident.sol* паметни уговор користи се за: креирање нових понуда, њихово прихватање/одбијање, завршетак инцидента и емитовање пратећих догађаја, уз контролу приступа и заштиту од reentrancy напада.

6.2. *The Graph* и клијентска апликација

The Graph протокол омогућава ефикасно индексирање догађаја и приступ подацима путем *GraphQL* упита, чиме се елиминише потреба за централизованим серверским слојем. Клијентска апликација, развијена у *React*-у, интегрише *Ethers.js* и *Wagmi* библиотеке за комуникацију са блокчејном, док *React Query* и *SweetAlert2* библиотеке обезбеђују респонзивност и транспарентност интеракција. Ова комбинација омогућава директну, сигурну и децентрализовану комуникацију између корисника и паметних уговора.

7. ПРАКТИЧНА ДЕМОНСТРАЦИЈА

RESET платформа пружа једноставан и безбедан начин за решавање сајбер инцидената на блокчејну. Интеракција са платформом почиње идентификацијом улоге (протокол или нападач), након које корисник може да пријави инцидент или да започиње преговоре кроз креирање, прихватање или одбијање понуда. Све ове трансакције транспарентно су забележене на блокчејну. Вођење преговора се одвија путем енкриптованог канала унутар платформе, чиме се обезбеђује приватност и верификабилност процеса. Статус сваке акције прати интерактивна нотификација са директним линком ка *Etherscan*-у, што корисницима даје потпуну контролу и увид у ток преговора. Овакав приступ спаја децентрализацију, сигурност и интуитивно корисничко искуство.

8. ЗАКЉУЧАК

RESET платформа представља децентрализовано *Web3* решење за сигурну и проверљиву комуникацију између компромитованих протокола и нападача. Систем се ослања na *Ethereum* паметне уговоре писане у *Solidity*-ју, уз подршку *OpenZeppelin* библиотеке

чиме се обезбеђује безбедност. Архитектура укључује паметне уговоре, интеграцију са *The Grap*h протоколом за индексирање и *React* клијентску апликацију, омогућавајући транспарентне преговоре и енкриптовану размену порука. Демонстрација показује да *RESET* интегрише савремене *Web3* технологије у јединствено решење које смањује ризик и повећава поверење у ДеФи екосистему. Будући развој обухвата подршку за више токена, аутентификацију без поверења и оптимизацију индексирања, чиме се платформа припрема за скалабилну продукциону употребу.

9. ЛИТЕРАТУРА

[1] Chainalysis team, „Crypto Hacks Analisys.“ [Online] Доступно на: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/ (приступљено у новембру 2025.)

[2] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“, [Online] Доступно на: https://nakamotoinstitute.org/library/bitcoin/ (приступљено у новембру 2025.)

[3] Wikipedia, „Proof of Work”, [Online] Доступно на: https://en.wikipedia.org/wiki/Proof_of_work (приступљено у новембру 2025.)

[4] Wikipedia, „Proof of Stake”, [Online] Доступно на: https://en.wikipedia.org/wiki/Proof_of_stake (приступљено у новембру 2025.)

[5] GeeksForGeeks, „Practical Byzantine Fault Tolerance”, [Online] Доступно на: https://www.geeksforgeeks.org/computer-networks/practical-byzantine-fault-tolerancepbft/ (приступљено у новембру 2025.)

[6] Nick Szabo, „Smart Contracts: Building Blocks for Digital Markets“ [Online] Доступно на: https://nakamotoinstitute.org/library/smart-contracts-building-blocks-for-digital-markets/ (приступљено у новембру 2025.)

[7] Ethereum.org, „Ethereum Virtual Machine (EVM)“, [Online] Доступно на: https://ethereum.org/developers/docs/evm/ (приступљено у новембру 2025.)

Кратка биографија:

Алекса Чоловић рођен је 25.03.2000. у Новом Саду, где је стекао своје основно и средње образовање. Основне академске студије завршава 2023. године одбраном дипломског рада на тему „Систем за подршку здравог живота“ на Факултету техничких наука. Након чега наставља своје школовање на истом факултету, а мастер рад одбранио је 2025. године.

Контакт: colovic.aleksa11@gmail.com

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.75
DOI: https://doi.org/10.24867/34BE24Skiljevic

PRIMENA PAMETNIH UGOVORA I NEZAMENLJIVIH TOKENA U VEB APLIKACIJAMA ZASNOVANIM NA BLOKČEJN TEHNOLOGIJAMA

APPLICATION OF SMART CONTRACTS AND NON-FUNGIBLE TOKENS IN WEB APPLICATIONS BASED ON BLOCKCHAIN TECHNOLOGIES

Milivoje Škiljević, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu biće prikazana primena pametnih ugovora i NFT tehnologija u okviru veb aplikacija. Poseban akcenat stavljen je na implementaciju nagradnog sistema zasnovanog na blokčejn tehnologijama.*

Ključne reči: *Distribuirani sistemi, blokčejn, pametni ugovori*

Abstract – *This paper will present the application of smart contracts and non-fungible tokens technologies within web applications. Special emphasis will be placed on the implementation of a reward system based on blockchain technologies.*

Keywords: *Distributed systems, blockchain, smart contracts*

1. UVOD

Veb aplikacije zasnovane na blockchain tehnologijama predstavljaju značajan deo modernih informacionih sistema, omogućavajući decentralizovane i transparentne načine upravljanja podacima i interakcijama među korisnicima. Posebno interesantne su implementacije pametnih ugovora, koji omogućavaju automatsko izvršavanje definisanih pravila bez posrednika, kao i tehnologija nezamenjivih tokena (engl. non-fungible tokens - NFTs), koja se koristi za upravljanje digitalnim sredstvima unutar veb platformi.

Iako blockchain tehnologije pružaju mnoge prednosti, njihova implementacija u okviru veb aplikacija nosi tehničke izazove. Posebno je važno pravilno dizajnirati i implementirati pametne ugovore i NFT mehanizme tako da sistem bude funkcionalan, siguran i skalabilan. Ovo uključuje povezivanje frontend i backend delova aplikacije sa blockchain mrežom, upravljanje transakcijama i nagradnim sistemima, kao i testiranje i evaluaciju funkcionalnosti.

Cilj ovog rada je prikaz praktične implementacije veb platforme sa integracijom pametnih ugovora, NFT nagrada i kripto plaćanja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, vanr. prof.

2. POJAM BLOKČEJNA

Da bi se u potpunosti shvatila uloga specijalizovanih programskih jezika za blockchain, prvo je potrebno jasno definisati pojam samog blokčejna. Blokčejn je distribuirana struktura podataka koja se koristi kao jedan od načina za implementaciju logičkog koncepta glavne knjige (engl. ledger) - kao takav je fundamentalan, a konkretne blokčejn tehnologije su onda smo različite implementacije ovakve strukture podataka.

2.1. Osnovni koncepti distribuiranih sistema

Distribuirani sistemi predstavljaju osnovu blockchain tehnologije i obuhvataju skup međusobno povezanih računara (čvorova) koji zajednički rade na postizanju određenih ciljeva, bez centralnog autoriteta [1]. Svaki čvor u sistemu ima svoj deo informacija i sposobnost da učestvuje u obradi i verifikaciji podataka [2].

Razumevanje ovih osnovnih principa ključno je za dalje proučavanje blockchain tehnologija, jer blockchain može biti posmatran kao specijalizovana primena distribuiranog sistema sa dodatnim zahtevima za sigurnost, nepromenljivost i transparentnost [4][5].

2.2. Distribuirana glavna knjiga (DLT)

Distribuirana glavna knjiga (engl. distributed ledger technology - DLT), predstavlja osnovni princip na kojem se zasnivaju blockchain sistemi [3].

Nepromenljivost podataka je jedna od ključnih osobina DLT-a. Jednom kada se zapis unese u distribuiranu glavnu knjigu, njegova izmena ili brisanje postaje gotovo nemoguće bez saglasnosti svih ili većine čvorova u mreži, što obezbeđuje visok nivo integriteta podataka [4].

Konsenzus je ključni mehanizam koji omogućava svim učesnicima distribuirane mreže da se slože oko trenutnog stanja glavne knjige.

2.3. Blockchain arhitektura i struktura blokova

Blockchain se može posmatrati kao specijalizovana forma distribuirane glavne knjige, sa jasno definisanom strukturom podataka i pravilima koja omogućavaju nepromenljivost i sigurnost transakcija. Struktura bloka tipično uključuje nekoliko komponenti: zaglavlje bloka, koje sadrži hash prethodnog bloka, hash trenutnog bloka, vremensku oznaku i informacije o konsenzusu, i telo

bloka, koje obuhvata sve transakcije uključene u taj blok. Osim strukture blokova, važan deo arhitekture blockchaina su mehanizmi konsenzusa. Proof-of-Work (PoW) i Proof-of-Stake (PoS) su dva najčešće korišćena algoritma, koji omogućavaju čvorovima mreže da se slože oko stanja lanca i da validiraju nove transakcije.

2.4 Primene i izazovi blockchain tehnologije

Blockchain tehnologija se u poslednjoj deceniji proširila izvan okvira kriptovaluta i finansijskog sektora, postajući osnova za raznovrsne aplikacije u različitim industrijama [6][9]. Njena sposobnost da obezbedi transparentnost, nepromenljivost i decentralizovanu verifikaciju čini je pogodnom za sisteme gde je poverenje među učesnicima ključno. Jedna od najpoznatijih primena su finansijske transakcije, uključujući Bitcoin, Ethereum i druge kriptovalute, gde blockchain omogućava sigurno slanje i primanje sredstava bez posrednika. U logistici i lancu snabdevanja, blockchain omogućava praćenje proizvoda od proizvođača do krajnjeg korisnika, čime se povećava transparentnost i smanjuje mogućnost falsifikovanja proizvoda. Jedan od posebno aktuelnih domena primene blockchaina su veb platforme sa integracijom NFT tehnologije i kripto plaćanja.

3. PAMETNI UGOVORI

Pametni ugovori predstavljaju jedan od najvažnijih koncepata savremenih blockchain sistema, jer značajno proširuju mogućnosti njihove primene. Oni omogućavaju da se pravila i dogovori između učesnika mreže definišu i izvršavaju automatski, bez potrebe za posrednicima. U ovom poglavlju biće detaljnije objašnjena suština pametnih ugovora, načini njihovog kreiranja, kao i oblasti u kojima se koriste.

3.1. Pojam pametnih ugovora

Pametni ugovori se mogu posmatrati kao programski kod koji se izvršava unutar blockchain mreže i koji omogućava da se unapred definisana pravila i uslovi realizuju automatski, bez posredovanja trećih strana [7][8]. Ideju pametnih ugovora prvi je uveo Nick Szabo još devedesetih godina prošlog veka, kada ih je opisao kao digitalne protokole za prenos informacija i vrednosti, čije izvršavanje ne zavisi od poverenja među učesnicima, već od samog koda i mreže na kojoj se nalaze. Osnovna prednost pametnih ugovora je eliminacija potrebe za centralnim autoritetom. Svaki učesnik mreže može da proveri sadržaj ugovora, dok njegovo izvršavanje zavisi isključivo od ispunjenja uslova navedenih u kodu. Sve operacije vezane za ugovor se beleže u blockchainu, što omogućava potpunu sledljivost i nepromenljivost izvršenih radnji. Pametni ugovori se danas koriste u različitim domenima.

3.2 Specijalizovani jezici za pisanje pametnih ugovora

Kako bi pametni ugovori mogli da funkcionišu u praksi, bilo je neophodno razviti specijalizovane jezike i okruženja za njihovo kreiranje i izvršavanje [9]. Ovi jezici se razlikuju od klasičnih programskih jezika jer su prilagođeni ograničenjima blockchain mreža – kod mora biti deterministički, bez mogućnosti proizvoljnih ulaza i nedeterminisanih rezultata, jer bi to ugrozilo konzistentnost sistema.

3.2.1. Bitcoin Script

Kada se govori o istoriji pametnih ugovora, polazna tačka je Bitcoin mreža i njen jednostavan, ali značajan jezik – Bitcoin Script. Ovaj jezik uveden je 2009. godine zajedno sa Bitcoin protokolom, a njegovu suštinsku svrhu čini definisanje pravila prema kojima se određena sredstva mogu trošiti. Bitcoin Script je baziran na steku, što znači da radi po principu dodavanja i uklanjanja podataka sa steka (stack data structure). Jedna od njegovih važnijih upotreba su tzv. multisignature transakcije (multisig), gde je potrebno više od jednog potpisa da bi transakcija bila validna. Dizajn Bitcoin Script-a je namerno nekompletan u poređenju sa univerzalnim programskim jezicima. Iako je ograničen u poređenju sa savremenim jezicima, Bitcoin Script je istorijski značajan jer je pokazao da blockchain može biti više od obične knjige transakcija.

3.2.2. Ethereum Virtual Machine Code

Pojava Ethereuma 2015. godine označila je prekretnicu u razvoju blockchain tehnologije i pametnih ugovora [9].

Ethereum Virtual Machine se može posmatrati kao globalni, distribuirani računar u kojem svaki čvor mreže poseduje i izvršava istu instancu virtuelne mašine. Programi koji se izvršavaju unutar EVM-a jesu pametni ugovori, a oni se na kraju kompajliraju u specijalizovani bajtkod koji EVM razume. Za razliku od Bitcoin Script-a, EVM je Turing-kompletan, što znači da u teoriji može izvršavati bilo koji program koji bi mogao biti izvršen na univerzalnom računaru. Jedna od specifičnih karakteristika EVM-a jeste upotreba gasa. U tehničkom smislu, EVM funkcioniše kao sandbox okruženje. Tokom godina, EVM je postao svojevrsni standard u blockchain svetu.

3.2.3. Solidity i savremeni jezici za pametne ugovore

Kako je Ethereum mreža postajala sve popularnija, pojavila se potreba za programskim jezikom koji će omogućiti pisanje složenijih pametnih ugovora na način koji je razumljiv i pristupačan većem broju programera. Tako je nastao Solidity, visokonivou jezik razvijen specijalno za Ethereum, sa sintaksom inspirisanom JavaScriptom, Python-om i C++-om [9][10][11]. Za razliku od Bitcoin Script-a, koji je ograničen i nudi samo osnovne funkcionalnosti, Solidity pruža bogat skup programerskih konstrukcija.

Pametni ugovori napisani u Solidity-ju se kompajliraju u EVM bajtkod, koji zatim izvršava Ethereum Virtual Machine. Pored Solidity-ja, razvijeni su i drugi jezici koji nude alternativni pristup pisanju pametnih ugovora. Savremeni jezici za pametne ugovore reflektuju evoluciju blockchain tehnologije. Važno je napomenuti i da razvoj jezika za pametne ugovore ide u pravcu unapređenja sigurnosti i formalne verifikacije.

3.3. Prednosti i ograničenja pametnih ugovora

Pametni ugovori predstavljaju jedan od najznačajnijih doprinosa blockchain tehnologije, jer omogućavaju da se unapred definisana pravila automatski izvršavaju bez posrednika. Njihova osnovna prednost leži u automatizaciji procesa. Druga važna prednost je transparentnost. Kod pametnog ugovora je javan i dostupan svim učesnicima mreže, što znači da svako može da proveri pravila i uslove pre nego što odluči da stupi u interakciju. Pametni ugovori takođe nude sigurnost i nepromenljivost.

Najznačajniji problem je nepromenljivost koda – ukoliko se greška potkrade u implementaciji, ona postaje trajni deo sistema. Drugi problem predstavlja cena izvršavanja.

Sve ove prednosti i ograničenja pokazuju da pametni ugovori nisu univerzalno rešenje, ali predstavljaju ogroman korak napred u automatizaciji i digitalizaciji procesa

4. PROGRAMSKI JEZIK SOLIDITY

Solidity je programski jezik čiji razvoj je inicijalno predložio Gavin Wood, a danas predstavlja najrasprostranjeniji jezik visokog nivoa za implementaciju pametnih ugovora. Kod napisan u Solidity-ju se kompajlira u Ethereum Virtual Machine bajtkod, čime postaje izvršiv na svim čvorovima Ethereum mreže i na drugim EVM-kompatibilnim blockchainovima [10][12].

5. NFT TEHNOLOGIJA I NJENA PRIMENA

NFT tehnologija u poslednjih nekoliko godina postala je jedno od najzapaženijih rešenja u okviru blockchain ekosistema. Ona omogućava digitalnu reprezentaciju jedinstvenih dobara i resursa, čime se otvaraju potpuno nove mogućnosti za upravljanje vlasništvom i vrednošću u digitalnom prostoru [10][13].

5.1. Promena imena promenljivih

NFT predstavlja specijalnu vrstu kripto tokena koja omogućava digitalnu reprezentaciju jedinstvenih dobara i resursa [10]. Za razliku od kriptovaluta poput Bitcoina ili Ethera, koje su fungibilne, NFT tokeni su jedinstveni i ne mogu se jednostavno razmenjivati po principu jedan za jedan. Svaki NFT sadrži metapodatke koji ga razlikuju od drugih, što omogućava da se poveže sa određenim digitalnim ili fizičkim dobrom. Osnovna karakteristika NFT-ova je njihova nedeljivost. NFT obezbeđuje dokaz o vlasništvu i poreklu, jer je istorija tokena zapisana u blockchainu i može se lako verifikovati [14].

NFT-ovi se obično implementiraju kroz pametne ugovore, najčešće koristeći ERC-721 standard na Ethereum mreži. Njihova popularnost naglo je porasla tokom 2020. i 2021. godine, kada su postali sinonim za digitalnu umetnost i kolekcionarske predmete.

5.2. Standardi za implementaciju NFT tokena

NFT tehnologija u najvećoj meri funkcioniše kroz standarde koji definišu pravila ponašanja tokena na blockchain mreži. Standardi obezbeđuju da različite aplikacije, novčanici i platforme mogu na dosledan način komunicirati sa tokenima, čime se postiže interoperabilnost i pouzdanost u radu [13]. Najpoznatiji i najrasprostranjeniji standardi za NFT-ove razvijeni su u okviru Ethereum ekosistema.

ERC-721 je prvi i najpoznatiji standard koji definiše nezamenljive tokene. Svaki ERC-721 token ima jedinstveni identifikator (tokenID), koji ga razlikuje od ostalih u kolekciji [10]. Sa rastom NFT tržišta pojavila se potreba za efikasnijim rukovanjem većim brojem tokena, pa je razvijen ERC-1155. ERC-1155 je posebno popularan u gaming industriji, gde igre zahtevaju istovremeno postojanje jedinstvenih predmeta i standardnih tokena [14]. Standardizacija NFT tokena omogućava kompatibilnost među različitim aplikacijama i servisima.

5.3. Prednosti i ograničenja NFT tehnologije

NFT tehnologija je u kratkom vremenskom periodu postala globalno prepoznatljiv koncept, ali kao i svaka inovacija, ima svoje prednosti i ograničenja. Jedna od najvećih prednosti NFT-ova jeste dokaz vlasništva. NFT-ovi pružaju transparentnost i sledljivost, jer se sve transakcije javno beleže u blockchainu. Druga prednost je monetizacija digitalnih dobara – umetnici i kreatori mogu direktno prodavati svoj rad bez posrednika.

NFT-ovi imaju važnu ulogu u gaming industriji, gde korisnici zaista poseduju svoje predmete i mogu njima slobodno trgovati. Jedan od najvećih problema NFT tehnologije jesu visoki troškovi transakcija na Ethereum mreži. NFT-ovi su izloženi i pravnoj nesigurnosti, jer ne postoji univerzalni pravni okvir koji bi jasno odredio njihov status.

5.4. Primena NFT-ova u različitim domenima

NFT tehnologija je pronašla široku primenu u različitim industrijama, jer pruža mogućnost verifikacije autentičnosti, praćenja vlasništva i monetizacije digitalnih dobara [13]. Najpoznatija upotreba NFT-ova odnosi se na digitalnu umetnost i kolekcionarske predmete [10]. Umetnici mogu tokenizovati svoja dela i prodavati ih kao NFT-ove, pri čemu blockchain garantuje autentičnost i vlasništvo.

Posebno je značajna mogućnost da autori kroz pametne ugovore dobijaju procenat od svake naredne prodaje. Gaming industrija predstavlja jedno od najdinamičnijih područja primene NFT tehnologije. Virtuelni predmeti mogu biti predstavljeni NFT-ovima, čime korisnici stiču pravo stvarnog vlasništva nad njima [13]. NFT-ovi se sve češće koriste i u veb platformama koje implementiraju nagradne sisteme.

5.5. NFT i pametni ugovori – blockchain aplikacije

NFT tehnologija svoju punu vrednost pokazuje tek kada se poveže sa pametnim ugovorima. Pametni ugovori predstavljaju osnovni mehanizam kojim se NFT kreira, upravlja i prenosi sa jednog korisnika na drugog. U najčešćem slučaju, NFT-ovi se implementiraju kroz ERC-721 ili ERC-1155 pametne ugovore [13]. Integracija NFT-ova sa pametnim ugovorima otvara mogućnost dodavanja dodatne logike. Pametni ugovor može automatski dodeliti NFT korisnicima koji ispune određene

kriterijume. Za veb aplikacije koje kombinuju kripto plaćanja i nagradne sisteme, veza između NFT-ova i pametnih ugovora predstavlja osnovu celog poslovnog modela [9].

6. REŠENJE

Ovaj rad demonstrira kako se klasična veb arhitektura može spojiti sa blockchain slojem u jednu funkcionalnu i sigurnu platformu. Cilj implementacije bio je da korisnik kroz poznat UI radi stvari kao što su pretplata, formiranje timova i preuzimanje NFT nagrada, dok logika poverenja živi na lancu. Frontend je razvijen u Next.js/React okruženju, sa Chakra UI za dosledan dizajn i react-icons za vizuelne nagoveštaje. Validacija i rad sa formama rešeni su preko react-hook-form kako bi unos bio brz i pouzdan. Backend koristi Next.js API rute kao tanki servisni sloj koji orkestrira pozive ka bazi i blockchainu. Baza podataka je modelovana kroz Prisma ORM i čuva korisnike, timove, pretplate, transakcije i evidenciju nagrada. Ovakav model omogućava da se stanje sezone i integritet pravila uvek mogu rekonstruisati iz podataka. Autentifikacija je izvedena preko next-auth, uz čuvanje sesija i uloga kroz @next-auth/prisma-adapter. Identitet za kripto operacije zasniva se na MetaMask novčaniku, a aplikacija nikada ne rukuje privatnim ključevima. Komunikacija sa lancem realizovana je bibliotekom ethers.js koja potpisuje i šalje transakcije i čita stanje ugovora. Pametni ugovori su implementirani na osnovu OpenZeppelin ERC-721 šablona kako bi NFT nagrade bile bezbedne i standardne. Ganache je korišćen za lokalno testiranje scenarija plaćanja, mintovanja i kontrole pristupa bez troškova gasa. Tok pretplate ide kroz MetaMask dijalog, nakon čega se hash, iznos i vreme uplate perzistiraju u bazi radi revizije. Po uspešnoj uplati sistem ažurira status pretplate i otključava premium funkcije u aplikaciji. Na kraju sezone administrator pokreće mintovanje, pri čemu svaki NFT dobija jedinstveni tokenID i metapodatke o osvojenoj nagradi. Dodela nagrada je automatizovana, transparentna i proverljiva jer je zapisana na blockchainu i u internim evidencijama. Administratorski panel objedinjuje otvaranje i zatvaranje sezona, validaciju timova, unos rezultata i iniciranje distribucije NFT-ova. Budžetska i pravila bodovanja se primenjuju i na nivou podataka, čime se smanjuju nedoslednosti između UI-a i domenskih ograničenja. Korisnički interfejs je projektovan da nedvosmisleno vodi kroz plaćanje, status transakcije i pregled osvojenih NFT-ova. Rešenje je skalabilno po slojevima: UI se kešira i renderuje efikasno, API rute su stateless, a blockchain rad je izolovan kroz jasne servise. Sigurnosni aspekti pokriveni su kontrolom uloga, OpenZeppelin bibliotekom, on-chain proverljivošću i audit-trail zapisima u bazi. Glavne operativne rizike čine varijabilne cene gasa i moguća neupućenost korisnika, što se adresira jasnim porukama stanja i lokalnim testiranjem. Ukupno posmatrano, implementacija pokazuje da se moderni veb okvir, standardni tokeni i pažljivo vođena domen logika mogu spojiti u održiv ekosistem pretplata i NFT nagrada koji je pouzdan, audibilan i prijatan za korišćenje.

7. ZAKLJUČAK

Rad je pokazao kako se savremene veb tehnologije mogu uspešno kombinovati sa blockchain okruženjem kako bi se izgradio sistem koji prevazilazi okvire klasičnih aplikacija. U teorijskom delu rada obrađeni su koncepti blockchain tehnologije, pametnih ugovora i jezika Solidity, dok je posebna pažnja posvećena NFT-ovima i njihovoj ulozi u savremenim aplikacijama. Praktični deo rada pokazao je da je moguće razviti platformu koja obezbeđuje više nivoa korisničkog iskustva – od jednostavnog pregleda i registracije za goste, preko premium pretplata koje se potvrđuju kripto transakcijama, pa do nagradnog sistema koji koristi NFT tehnologiju. Važno je naglasiti da implementacija ovakvih sistema donosi i brojne izazove – od tehničkih pitanja poput optimizacije troškova gasa i bezbednosti pametnih ugovora, do šireg društvenog i pravnog konteksta koji tek treba da definiše mesto NFT-ova i kriptovaluta. U celini, ovaj master rad je demonstrirao kako kombinacija veb aplikacija i blockchain tehnologije otvara put ka budućim rešenjima gde korisnici ne učestvuju samo pasivno, već aktivno poseduju i kontrolišu deo sistema kroz digitalna sredstva koja su istovremeno transparentna, sigurna i trajna.

LITERATURA

[1] Maarten van Steen and Andrew S. Tanenbaum (2016). A brief introduction to distributed systems. Computing, 98(10), 967–1009.
[2] Apache Hadoop (2012). HDFS Design. [Online]. https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html [pristupljeno oktobra 2025.]
[3] Leslie Lamport, Robert Shostak, and Marshall Pease (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401 (July 1982).
[4] Stuart Haber and W. Scott Stornetta (1991). How to Time-Stamp a Digital Document. Journal of Cryptology, 3(2), 99–111.
[5] Dave Bayer, Stuart Haber, and W. Scott Stornetta (1993). Improving the Efficiency and Reliability of Digital Time-Stamping. In Sequences II: Methods in Communication, Security, and Computer Science, pp. 329–334. New York, NY: Springer-Verlag.
[6] Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://developer.bitcoin.org/reference/rpc/index.html [pristupljeno oktobra 2025.]
[7] Nick Szabo (1994). Smart Contracts. [Online]. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [pristupljeno oktobra 2025.]
[8] Nick Szabo (1996). Smart Contracts: Building Blocks for Digital Markets. [Online]. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [pristupljeno oktobra 2025.
[9] Vitalik Buterin (2013). Ethereum Whitepaper. [Online]. https://ethereum.org/en/whitepaper [pristupljeno

oktobra 2025.]
[10] Docs.Soliditylang. Solidity Documentation (v0.8.17). [Online]. https://docs.soliditylang.org/en/v0.8.17/ [pristupljeno: oktobra 2025.]
[11] Docs.Soliditylang – Language Influences. Languages that Influenced Solidity. [Online]. https://docs.soliditylang.org/en/v0.8.17/language-influences.html [pristupljeno: oktobra 2025.]
[12] Docs.Soliditylang – Structure. Structure of a Contract in Solidity. [Online]. https://docs.soliditylang.org/en/v0.8.17/structure-of-a-contract.html [pristupljeno: oktobra 2025.]
[13] Docs.Soliditylang – Contracts. Contracts in Solidity. [Online]. https://docs.soliditylang.org/en/v0.8.17/contracts.html [pristupljeno: oktobra 2025.]
[14] Docs.Soliditylang – Units and Globals. Solidity: Units and Global Variables. [Online]. https://docs.soliditylang.org/en/v0.8.17/units-and-global-variables.html [pristupljeno: oktobra 2025.]

Kratka biografija:

Milivoje Škiljević rođen je u Trebinju 1995. god. Diplomski rad na Fakultetu tehničkih nauka u Novom Sadu, iz oblasti Elektrotehnike i računarstva – Računarstvo i informatika odbranio je 2017. god.

kontakt:
milivojeskiljevic7@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

УДК: 4.5
ДОИ: https://doi.org/10.24867/34BE25Pesic

КОМПАРАТИВНА АНАЛИЗА ИНКЛУЗИВНОГ ДИЗАЈНА КОМУНИКАЦИОНИХ ПЛАТФОРМИ: МАЈКРОСОФТ ТИМС, ДИСКОРД И СЛЕК КРОЗ ДЕСКТОП, ВЕБ И МОБИЛНА ОКРУЖЕЊА

COMPARATIVE ANALYSIS OF INCLUSIVE DESIGN OF COMMUNICATION PLATFORMS: MICROSOFT TEAMS, DISCORD AND SLACK ACROSS DESKTOP, WEB AND MOBILE ENVIRONMENTS

Ања Пешић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду дата је анализа и поређење комуникационих платформи Мајкрософт Тимс, Слек и Дискорд кроз различита окружења – десктоп, веб и мобилно. На основу детаљне анализе њихових функционалности, приступачности и могућности прилагођавања, изведени су закључци о томе у којој мери свака од платформи испуњава принципе инклузивног дизајна. Сврха анализе је да се утврди на који начин комуникационе платформе могу допринети дигиталној једнакости и равноправном приступу информацијама, као и да се укаже на области које захтевају даља побољшања како би биле потпуно приступачне свим корисницима.*

Кључне речи (три до пет): *инклузивни дизајн, приступачност, комуникационе платформе.*

Abstract – *This paper presents an analysis and comparison of communication platforms Microsoft Teams, Slack, and Discord across different environments – desktop, web, and mobile. Based on a detailed examination of their functionalities, accessibility features, and customization options, conclusions were drawn regarding the extent to which each platform meets the principles of inclusive design. The purpose of the analysis is to determine how communication platforms can contribute to digital equality and equitable access to information, as well as to highlight areas that require further improvement in order to become fully accessible to all users.*

Keywords: (three to five): *inclusive design, accessibility, communication platforms.*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дину Драган, ванр. проф.

1. УВОД

Дигитална комуникација представља основу савременог пословног, образовног и друштвеног живота, јер омогућава повезивање и сарадњу на даљину [1]. Развој и широка примена платформи као што су Мајкрософт Тимс (енгл. Microsoft Teams), Слек (енгл. Slack) и Дискорд (енгл. Discord) довели су до значајне трансформације начина рада и учења, посебно у условима хибридних и онлајн модела [2, 3, 4, 5].

Инклузивни дизајн има централну улогу у равноправном приступу дигиталним технологијама. За разлику од приступачности (енгл. *accessibility*), која се односи на техничку могућност коришћења одређеног садржаја, инклузивни дизајн настоји да укључи што шири спектар корисника већ у процесу развоја производа, водећи рачуна о различитим потребама и контекстима коришћења [1]. Циљ таквог приступа је стварање дигиталног окружења које једнако добро функционише за све кориснике, укључујући особе са инвалидитетом, старије и кориснике са нижим нивоом дигиталних вештина [3]. Овај рад има за циљ компаративну анализу инклузивног дизајна комуникационих платформи Мајкрософт Тимс, Слек и Дискорд кроз десктоп, веб и мобилно окружење. Истраживање се заснива на анализи званичне документације, практичном тестирању и прегледу релевантне литературе, како би се утврдило у којој мери наведене платформе примењују принципе инклузивног дизајна и где постоје могућности за унапређење. Резултати имају за циљ да допринесу разумевању значаја инклузивног дизајна у дигиталној комуникацији и подстицању дигиталне једнакости у савременом друштву.

2. ТЕОРИЈСКИ ОКВИР

У савременом друштву дигитална комуникација представља основу рада, образовања и друштвене интеракције, што указује на потребу примене инклузивног дизајна у развоју платформи које користи велики број људи. Инклузивни дизајн подразумева осмишљавање дигиталних производа који узимају у обзир разноликост корисника од самог почетка, док приступачност обухвата техничке мере које омогућавају особама са инвалидитетом да користе дигиталне алате, попут читача екрана, титлова или навигације путем тастатуре. Тако инклузивни дизајн доприноси једнакости и бољем корисничком искуству за све, укључујући и оне са привременим ограничењима као што су слаба конекција или неповољни услови осветљења [6]. Најзначајнији оквир

за оцену приступачности дигиталних производа су смернице за приступачност веб садржаја ВЦАГ (енгл. *Web Content Accessibility Guidelines*) које дефинишу критеријуме успешности у четири основна принципа: перцептибилност, операбилност, разумљивост и робусност [7]. Концепт универзалног дизајна додатно шири овај оквир јер промовише креирање решења која користе свима, а не само особама са инвалидитетом, као што су титлови или прилагодљиви режими контраста [9]. Инклузивни дизајн посебно је важан за групе као што су особе са оштећењем вида, слуха, моторичким или когнитивним потешкоћама, као и старије особе, али његове предности користе свим корисницима, на пример кроз гласовне команде или различите визуелне режиме [10, 11]. С обзиром да комуникационе платформе представљају централне алате у савременом дигиталном окружењу, њихова инклузивност има друштвени значај јер омогућава равноправно учешће у раду, образовању и комуникацији, чиме се смањује дигитални јаз [1, 11].

3. ПРЕГЛЕД КОМУНИКАЦИОНИХ ПЛАТФОРМИ

У овом поглављу представљене су три комуникационе платформе које су предмет анализе: Мајкрософт Тимс, Слек и Дискорд. Свака од ових платформи развијена је у различитом контексту и за различите циљне групе корисника, али су све постале веома популарни алати за размену информација [2,3,4].

3.1.Мајкрософт Тимс

Мајкрософт Тимс развијен је 2017. године и намењен је пословним и образовним институцијама. Омогућава чет, видео и аудио састанке, дељење докумената и интеграцију са осталим Мајкрософт сервисима. Захваљујући великој бази корисника и наглашеном фокусу на приступачност (титлови, транскрипти, контраст, читачи екрана), Тимс је постао једна од најинклузивнијих платформи за сарадњу [2, 12].

3.1. Слек

Слек је настао 2013. године као алат за интерну комуникацију и брзо се развио у једну од најпопуларнијих пословних платформи. Његова снага лежи у једноставном интерфејсу, организацији комуникације кроз канале, као и богатом екосистему интеграција са више хиљада других апликација.
Слек је нарочито популаран међу технолошким компанијама, стартапима (младим, иновативним компанијама у развоју) и тимовима који користе агилне методе рада. Једна од његових карактеристика је могућност прилагођавања помоћу ботова и АПИ-ја (енгл. *Application Programming Interface*), што омогућава корисницима да обликују платформу према сопственим потребама [4, 14].

3.2. Дискорд

Дискорд је лансиран 2015. године као бесплатна платформа намењена првенствено гејмерима, како би им омогућила гласовну и текстуалну комуникацију током играња игара. Захваљујући својој једноставности, стабилности и бесплатним функцијама, Дискорд је веома брзо стекао огромну базу корисника. Временом је употреба платформе превазишла гејминг заједницу – данас се користи у едукативне сврхе, пословне сарадње, као и за организацију разних заједница и интересних група.
Дискорд комбинује текстуални чет, гласовне и видео канале, могућност креирања сервера и подканала, као и напредне опције за модерацију и интеграцију са другим алатима. Посебно је популаран код млађе популације, јер нуди флексибилан и бесплатан простор за заједничку комуникацију [3, 13].

3.3. Компаративни значај

Иако су све три платформе комуникациони алати, њихова полазна тачка и циљно тржиште значајно се разликују. Мајкрософт Тимс развијен је као пословни и образовни алат, Слек као флексибилна пословна платформа за тимове, а Дискорд као заједнички простор за гејминг заједнице. Ове разлике у контексту развоја одражавају се и на њихову имплементацију инклузивних функција. Зато њихово поређење може пружити значајне увиде у то како различите филозофије развоја и циљна тржишта утичу на ниво и квалитет инклузивног дизајна [2, 3, 4].

4. МЕТОДОЛОГИЈА

Методолошки оквир овог рада заснован је на систематском приступу анализи комуникационих платформи кроз призму инклузивног дизајна. Циљ овог поглавља је да представи кораке који су спроведени током истраживања, као и начине прикупљања, обраде и интерпретације података. Подаци коришћени у анализи прикупљени су из више различитих извора како би се обезбедила поузданост и свеобухватност: директно тестирање платформи од стране аутора рада, званична документација и смернице, стандарди и литература и секундарна литература (стручни чланци и анализе искустава корисника). Анализа је спроведена према пет критеријума: приступачност интерфејса, подршка помоћним функцијама, мултимодалне функције, флексибилност и прилагођавање, и конзистентност кроз окружења. Поређење је извршено унутар сваке платформе и међу њима, како би се идентификовале кључне разлике и заједничке карактеристике. Истраживање је ограничено на јавно доступне верзије апликација у тренутку анализе, као и на чињеницу да није укључивало директно тестирање са корисницима са инвалидитетом, што се препоручује за будућа истраживања.

5. АНАЛИЗА ПО ПЛАТФОРМАМА И ОКРУЖЕЊИМА

5.1. Мајкрософт Тимс

Мајкрософт Тимс показује највиши степен инклузивности у сва три окружења. На десктопу омогућава подешавање величине фонта, теме и контраста, као и потпуну подршку читачима екрана и тастатурној навигацији. Током састанака доступни су

титлови уживо, транскрипти и текст у реалном времену што значајно олакшава комуникацију особама са оштећењем слуха. Имерсив Ридер (енгл. *Immersive Reader*) омогућава читање текста наглас и прилагођавање приказа за особе са дислексијом. Веб верзија задржава већину ових функција, али су неке опције ограничене прегледачем. Мобилна апликација интегрисана је са системским функцијама приступачности (Војсовер – енгл. *VoiceOver*, Токбек – енгл. *TalkBack*) и задржава титлове уживо, али са мање могућности прилагођавања.

5.2. Слек

Слек је дизајниран као пословни комуникациони алат са нагласком на једноставност и прегледност. Интерфејс у десктоп верзији подржава повећање текста, избор теме и навигацију преко тастатуре, али је подршка читачима екрана ограничена у појединим менијима. Недостају напредне функције као што су титлови и транскрипти, што умањује приступачност током видео позива. Веб верзија задржава добру употребљивост и јасан дизајн, док је мобилна апликација оптимизована за брзу комуникацију, али без додатних могућности персонализације. Иако једноставан и интуитиван, Слек не достиже ниво функционалне инклузивности као Тимс.

5.3. Дискорд

Дискорд нуди основни ниво приступачности, али без дубље интеграције инклузивних функција. Десктоп верзија има чист интерфејс и подршку за промену теме и величине текста, али без титлова, транскрипата или напредне контроле контраста. Подршка читачима екрана и навигација преко тастатуре постоји, али је делимична јер пречице не покривају све функције и елементе интерфејса. Веб верзија задржава сличне могућности, док је мобилна једноставна и стабилна, али ограничена на основну комуникацију преко гласа и текста. Иако једноставан за употребу и погодан за млађе кориснике, Дискорд показује најмањи степен инклузивног дизајна у поређењу са осталим платформама.

6. ДИСКУСИЈА

Компаративна анализа Тимса, Слека и Дискорда показала је да свака платформа има различит степен зрелости у области инклузивног дизајна и различите приоритете у развоју. Тимс се издваја по најпотпунијем скупу уграђених функција за приступачност (аутоматски титлови, транскрипти, Имерсив Ридер), што је посебно значајно за кориснике са оштећењем слуха и вида, али и за све остале који раде у неповољним условима. Ипак, Тимс има и најсложенији интерфејс са великим бројем панела, дугмади и менија, што за кориснике са нижим дигиталним компетенцијама може представљати озбиљну баријеру. Ово указује на дилему између богатства функција и једноставности корисничког искуства.

Слек се показао као платформа са веома интуитивним интерфејсом, снажном персонализацијом (теме, главни мени, контрола нотификација) и богатим екосистемом интеграција. Опција нити и сакривања целих секција смањују когнитивни напор јер омогућавају корисницима да сами структурирају садржај. Међутим, недостатак уграђених аутоматских титлова или транскрипта за позиве и даље оставља мултимодални део платформе мање инклузивним, посебно за особе са оштећењем слуха. Ово показује да Слек у текстуалном сегменту достиже високе стандарде, али да гласовне и видео функције заостају по питању инклузивности.

Дикорд нуди највећу флексибилност у комуникационим каналима, управљању серверима, подешавањима нотификација, али нема кључне уграђене функције приступачности као што су аутоматски титлови, доследна подршка за читаче екрана и текстуални описи свих иконица. Сложеност интерфејса са великом количином садржаја, бројним серверима и иконама без текстуалног објашњења може бити изазовна за нове кориснике и оне са когнитивним или визуелним потешкоћама. Ипак, могућност додавања сервиса, управљања улогама, филтрирања и скривања канала омогућава висок ниво прилагођавања – што је значајна карактеристика инклузивног дизајна јер корисници могу креирати окружење које им највише одговара.

Уочена је и јасна разлика између окружења: десктоп апликације имају најпотпуније функције и бољу подршку за помоћне функције, али су сложеније; веб верзије нуде скоро идентично искуство, али зависе од прегледача и интернет конекције, па неке функције могу бити ограничене; мобилне апликације пружају основни скуп функција, али су често боље оптимизоване за системске опције приступачности као што су Војсовер, Токбек, динамичко куцање и текст високог контраста. Овај образац указује да корисници који зависе од читача екрана или напредних опција често добијају најбоље искуство на десктопу, док мобилне верзије, иако једноставније, немају све функције и мање су погодне за сложене радне токове.

Ради прегледнијег приказа резултата, у табели 1 су обједињено приказани резултати евалуације по сваком критеријуму. За сваку платформу и окружење утврђено је у којој мери је критеријум испуњен, при чему је коришћен систем оцењивања заснован на степену подршке и квалитету имплементације функција. Симбол „+“ означава делимичну подршку, „++“ добру али непотпуну реализацију, док „+++“ означава да је функционалност у потпуности развијена и усклађена са принципима инклузивног дизајна. На основу добијених резултата, могуће је сагледати предности и ограничења сваке платформе, као и утврдити у којим аспектима постоји простор за унапређење.

Табела 1 - Резултати евалуације по сваком критеријуму за сваку платформу

Критеријум/ Платформа	Окружење	Мајкрософт Тимс	Слек	Дискорд
Приступачност интерфејса	десктоп	+++	++	+
	веб	++	++	+
	мобилно	++	++	+
Подршка помоћним функцијама	десктоп	+++	++	+
	веб	++	++	+
	мобилно	+++	++	+

Мултимодалне функције	десктоп	+++	++	++
	веб	++	++	++
	мобилно	++	+	++
Флексибилност и прилагођавање	десктоп	+++	++	+
	веб	++	++	+
	мобилно	++	++	+
Конзистентност кроз окружења	сва окружења	+++	++	+

7. ЗАКЉУЧАК

Ово истраживање показало је да Тимс, Слек и Дискорд имају различите приступе инклузивном дизајну, али ниједна платформа није потпуно инклузивна у свим окружењима. Тимс предњачи у функцијама приступачности као што су титлови, транскрипти и Имерсив Ридер, Слек у једноставности и персонализацији текстуалне комуникације, док Дискорд нуди највећу флексибилност у организацији заједница. На основу анализе могу се предложити унапређења попут боље подршке за читаче екрана и тастатурну навигацију, увођења титлова и транскрипата у видео каналима, као и развоја универзалне контролне табле приступачности ради једноставнијег подешавања. Резултати рада указују да је инклузивни дизајн више од техничких стандарда — он представља стратегију за стварање праведнијег и приступачнијег дигиталног окружења за све кориснике.

8. ЛИТЕРАТУРА

[1] R. M. Gilbert, „Inclusive Design for a Digital World “ (2019)
[2] „Microsoft Teams, Wikipedia”
https://en.wikipedia.org/wiki/Microsoft_Teams
[3] „Discord, Wikipedia”
https://en.wikipedia.org/wiki/Discord
[4] „Slack, Wikipedia”
https://en.wikipedia.org/wiki/Slack_(software)
[5] „About Discord”
https://discord.com/company
[6] „Introduction to Web Accessibility”
https://www.w3.org/WAI/fundamentals/accessibility-intro/
[7] „Web Content Accessibility Guidelines”
https://en.wikipedia.org/wiki/Web_Content_Accessibility_Guidelines
[8] „W3C Accessibility Standards Overview”
https://www.w3.org/WAI/standards-guidelines/
[9] „Universal design”
https://en.wikipedia.org/wiki/Universal_design
[10] „Diverse Abilities and Barriers”
https://www.w3.org/WAI/people-use-web/abilities-barriers/
[11] „Microsoft Inclusive Design”
https://inclusive.microsoft.design/
[12] „Microsoft Accesibility Portal”
https://www.microsoft.com/en-us/accessibility
[13] „Slack Accessibility Guide”
https://slack.com/intl/en-gb/accessibility
[14] „Discord Accessibility”
https://discord.com/accessibility

Кратка биографија:

Ања Пешић рођена је у Новом Саду 1999. год. Основне академске студије завршила је 2022. године на Факултету техничких наука. Исте године уписује мастер академске студије на студијском програму Рачунарство и аутоматика.
Контакт: anjapesic0@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.85
ДОИ: https://doi.org/10.24867/Vasilic

Примена кубернетеса и машинског учења у развоју система за временску прогнозу

Application of Kubernetes and Machine Learning in the Development of a Weather Forecasting System

Марко Василић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Овај рад представља развој система за предвиђање температуре у реалном времену који комбинује технологије Кубернетеса, Докера и Long Short-Term Memory (ЛСТМ) неуронских мрежа. Архитектура система заснована је на микросервисима који обухватају сервис за предвиђање, сервис за управљање подацима, графички интерфејс и сервис за заказивање задатака. Систем је имплементиран и тестиран у Minikube Кубернетес кластеру, користећи PostgreSQL базу података за чување података и Streamlit библиотеку за визуелизацију резултата. LSTM модел је обучен на реалним метеоролошким подацима и омогућава прогнозу температуре за наредних 24 сата и 7 дана. Резултати показују да интеграција Кубернетеса и машинског учења омогућава ефикасну оркестрацију и скалабилност при дизајнирању система. Рад представља основу за даљи развој у правцу примене у клауд окружењима и интеграције са системима за аутоматско прикупљање и обраду података.*

Кључне ријечи: *Кубернетес, ЛСТМ, временска прогноза, машинско учење, Докер, Minikube, микросервисна архитектура.*

Abstract – *This paper presents the development of a scalable and automated system for real-time temperature prediction that integrates Kubernetes, Docker, and LSTM neural networks. The system architecture is based on a microservices model, including services for prediction, data management, visualization, and task scheduling. The implementation was carried out using Minikube Kubernetes clusters, with a PostgreSQL database for data storage and the Streamlit library for results visualitzation. The LSTM model was trained on meteorological data, enabling temperature forecasts for the next 24 hours and 7 days. The results demonstrate that the combination of Kubernetes and machine learning provides efficient orchestration and scalability in system design. This work establishes a foundation for further development toward cloud-based deployment and integration with automated data collection and processing systems.*

Keywords: *Kubernetes, LSTM, weather forecasting, machine learning, Docker, Minikube, microservices architecture.*

НАПОМЕНА:Овај рад проистекао је из мастер рада чији је ментор била др Татјана Лончар-Турукало, ред. професор.

1. УВОД

Савремени технолошки развој донио је значајне иновације у начину на који се приступа обради великих количина података и изградњи скалабилних система. Једна од кључних области у том контексту је оркестрација контејнера, која омогућава ефикасно управљање комплексним апликацијама, те примјена машинског учења, које омогућава анализу и предвиђање појава заснованих на подацима.

Комбинација ових технологија представља основу за развој интелигентних и аутоматизованих система. У овом раду описан је процес изградње система за временску прогнозу који користи LSTM (енгл. *Long Short-Term Memory*) неуронске мреже за предвиђање температуре и Кубернетес као платформу за оркестрацију микросервисне архитектуре.

Главни циљ рада је да се прикаже на који начин Кубернетес омогућава лако управљање, скалирање и одржавање апликација заснованих на машинском учењу. У систему је примјењен Minikube кластер, који омогућава локално тестирање инфраструктуре, а модели су обучени на метеоролошким подацима. Развој оваквих система омогућава лакшу интеграцију аналитичких модела у продукциона окружења, што представља значајан корак ка примјени машинског учења у реалним системима.

У раду је описана коришћена методологија докер, и кубернетес платформе као и ЛСТМ мреже, након чега је описана имплементација система.

2. МЕТОДОЛОГИЈА

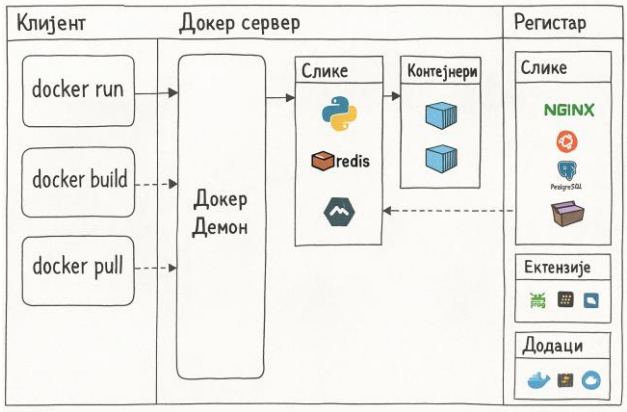
2.1. Докер

Докер је отворена платформа за развој, испоруку и извршавање апликација у контејнерима[1]. Он омогућава изолацију апликација од инфраструктуре, чиме се значајно убрзава развој и тестирање софтвера.

Докер користи архитектуру клијент–сервер, при чему Докер клијент комуницира са Докер демоном који управља контејнерима, сликама и мрежама преко REST API-ја.
Основни елементи Докера су:

- докер слике – шаблони из којих се покрећу контејнери;
- докер контејнери – извршне јединице које садрже апликацију и њене зависности;
- докер демон – сервис који извршава команде и управља контејнерима;
- докер регистар – складиште за слике, јавно или приватно.

Докер контејнери дијеле оперативни систем домаћина, што их чини лакшим и ефикаснијим у поређењу са виртуелним машинама. Захваљујући томе, апликације се могу лако преносити између различитих окружења – од локалне машине до клауда. Приказ Докер архитектуре дат на слици 1.



Слика 1. Илустрација Докер архитектуре

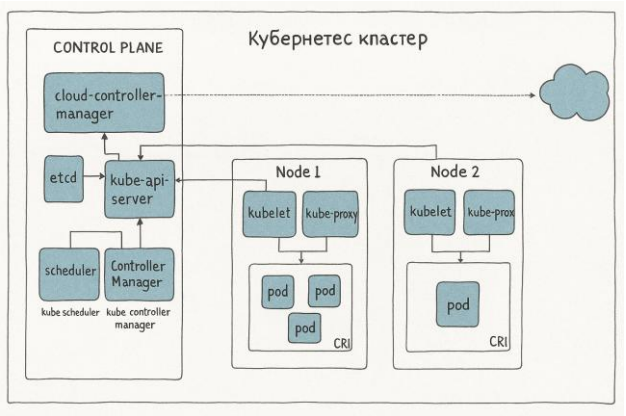
Употребом Докера постиже се: (1) портабилност - исти контејнер ради на свакој платформи; (2) изолација - свака апликација ради у свом окружењу, без конфликта са другим; (3) ефикасност ресурса - дели оперативни систем домаћина, па троши мање меморије и процесорског времена; (4) брза имплементација и скалирање: лако се креирају нови контејнери и систем се може проширити без застоја у раду.
Ове особине чине Докер кључном технологијом у савременим клауд архитектурама, као и у системима који користе Кубернетес за оркестрацију.

2.2. Кубернетес

Кубернетес је отворена платформа за оркестрацију контејнера, која омогућава аутоматизовано распоређивање, управљање и скалирање апликација [2]. Развијен од стране *Google*-а, данас представља индустријски стандард за управљање микросервисним системима у продукцији.
Главна идеја Кубернетеса је да се апликације покрећу у више независних контејнера који се групишу у *Pod*-ове, а затим управљају централизовано у кластеру. Сваки кластер се састоји од контролне равни (која доноси одлуке и радних чворова који извршавају апликације.
Кубернетес обезбјеђује: аутоматско скалирање апликација према оптерећењу, самоопоравак (рестарт падајућих контејнера), распоређивање без застоја (енгл. *rolling updates*), балансирање оптерећења и безбједно управљање конфигурацијама и тајнама.
Захваљујући овим особинама, Кубернетес омогућава да се системи машинског учења као што је овај лако одржавају, проширују и интегришу са другим сервисима.
Архитектура Кубернетеса састоји се од неколико главних компоненти:

- *kube-apiserver* – прима и обрађује све захтјеве у кластеру;
- *etcd* – база података која чува стање кластера (key-value база);
- *kube-scheduler* – одређује расподјелу покретања *Pod*-ова по чворовима;
- *kube-controller-manager* – управља радом система и одржава га у жељеном стању;
- *kubelet* – агент који прати стање контејнера на сваком чвору.

Оваква архитектура омогућава декларативно управљање системом, гдје се у YAML конфигурационим фајловима описује жељено стање, а Кубернетес аутоматски обезбјеђује да систем то стање задржи. Архитектура приказана на Слици 2.
Примјена Кубернетеса у овом систему омогућава: лако распоређивање више микросервиса, аутоматско заказивање задатака, перзистентно чување података, једноставну интеграцију са PostgreSQL базом и визуелизацијом резултата.
Ове карактеристике чине Кубернетес идеалним окружењем за хостовање интелигентних система који комбинују машинско учење и обраду података у реалном времену.



Слика 2. Архитектура Кубернетес кластер-а

2.3. LSTM (*Long Short-Term Memory*)

Рекурентне неуронске мреже (РНН) [6], представљају врсту дубоких неуронских мрежа које су посебно

погодне за анализу секвенцијалних података, као што су временске серије, текст или звук. Кључна карактеристика РНН-а је повратна веза – излаз следећег или неког будућег слоја је улаз у неки ранији слој, на основу чега мрежа може „памтити“ информације из прошлости и користити их за будуће прогнозе.

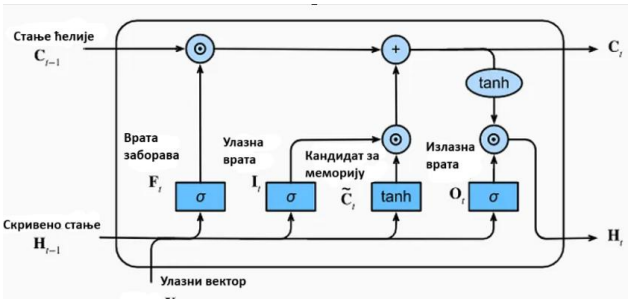
Ипак, класичне РНН мреже имају ограничења у раду са дугим секвенцама, јер током учења долази до појаве великог смањења или повећања градијената што утиче на поступак обуке и перформансе при дугорочном предвиђању градијената, што смањује њихову тачност при дугорочном предвиђању [3].

ЛСТМ (енгл. *Long Short-Term Memory*) [7] је специјализована варијанта RNN-а која уводи механизам меморијских ћелија и врата за контролу протока информација. Свака LSTM јединица садржи: врата заборава – где се одлучује које старе информације ће бити обрисане; улазна врата – где се одређује које нове информације ће бити додате; излазна врата – која контролишу шта ће бити прослијеђено као излаз мреже.

Овом структуром ЛСТМ омогућава моделу да истовремено чува и краткорочне и дугорочне обрасце у подацима, што га чини изузетно погодним за временску прогнозу, гдје су историјски подаци релевантни за предвиђање будућих вредности. Приказ ЛСТМ архитеткуре на слици 3.

За развој система коришћени су метеоролошки подаци за град Јена (Немачка) за 2024. годину, преузети са јавне базе података [4]. Након филтрирања, задржана су следећа обележја: температура (T), притисак (p), релативна влажност (rh), брзина вјетра (wv), густина ваздуха (ρ) и Vpact. Коришћено је 26207 записа (узорака) из базе. Модел је обучаван на нормализованим подацима. За оптимизацију је примјењен Adam оптимизатор, а функција губитка је средњеквадратна грешка (енгл. *Mean Squared Error*, MSE), која представља стандардну метрику за процјену перформанси регресионих модела.

Систем је имплементиран као микросервис у програмском језику Python, уз коришћење PyTorch библиотеке за развој и обуку LSTM неуронске мреже. Микросервис је упакован у Докер контејнер, а оркестрација је реализована помоћу Миникубе алата. За припрему и обраду података коришћене су *pandas* и *numpy* библиотеке.



Слика 3. ЛСТМ архитектура

3. ИМПЛЕМЕНТАЦИЈА СИСТЕМА

3.1. Архитектура решења

Циљ имплементације је развој система за временску прогнозу заснованог на микросервисној архитектури и покренутог у Кубернетес Minikube кластеру. Систем је подијељен у четири независна микросервиса који међусобно комуницирају путем REST API-ја:

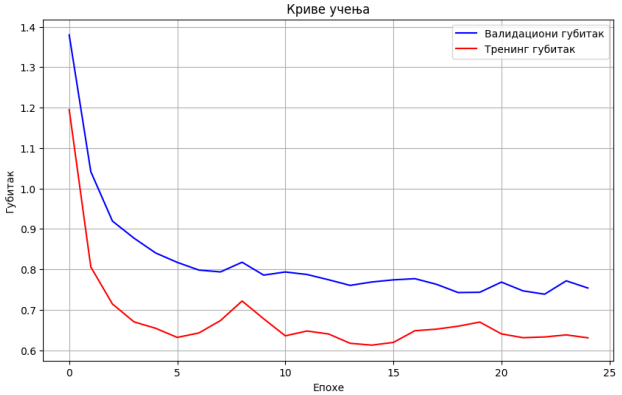
1. Сервис за предикцију – користи обучени ЛСТМ модел за предвиђање температуре;
2. Сервис за повезивање – управља базом података, учитава CSV фајлове и иницира обуку модела;
3. Сервис за графички интерфејс – визуализује резултате предвиђања преко *Streamlit* библиотеке;
4. Сервис за заказивање задатака – аутоматски покреће процес тренинга модела сваки сат времена путем *CronJob* механизма у Кубернетесу.

Сви сервиси су запаковани у Докер контејнере, дефинисани помоћу *YAML* конфигурационих фајлова, и распоређени унутар *Minikube* кластера. Комуникација између њих реализована је преко унутрашњих сервисних ресурса у Кубернетесу.

3.3. ЛСТМ модел и предвиђање

Улазни подаци су нормализовани и структурирани у секвенце од по три дана, што омогућава ЛСТМ моделу да „учи“ временске обрасце и предвиђа температуру за наредни период. ЛСТМ модел се састоји од два слоја (64 и 32 јединице), при чему је у сврху регуларизације коришћен *dropout* (стопа постављена на 30%). Модел је обучаван уз Адам оптимизатор са брзином учења од 0.001. Модел врши двије врсте предвиђања: краткорочно – за наредних 24 сата (сатни интервал), дугорочно – за наредних 7 дана (дневни просјек).

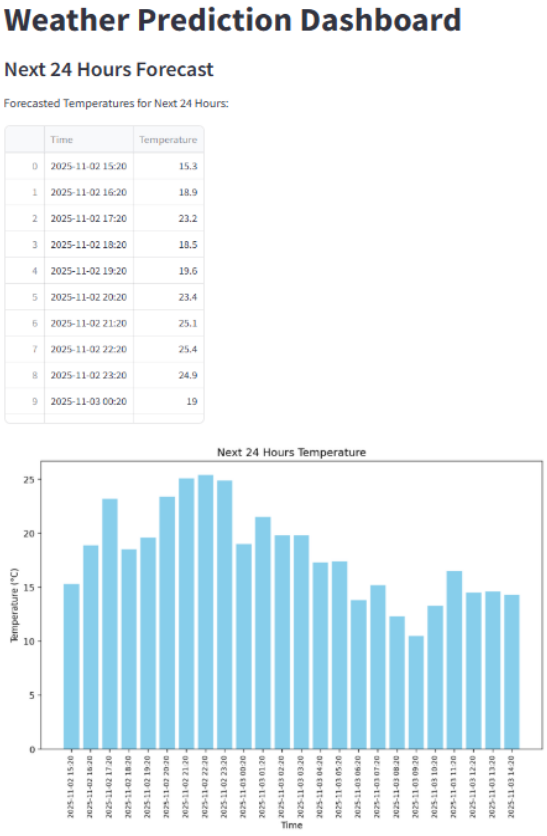
Резултати тренинга показују конвергенцију грешке током 25 епоха, што указује на добру генерализацију модела. Коначни модел постиже средњу апсолутну грешку (MAE) од 0.971 на тест скупу, што представља задовољавајућу тачност предвиђања температуре. Критеријум заустављања био је фиксиран број епоха (25), без примјене раног заустављања на основу валидационе грешке. Приказ криве учења дат је на слици 4.



Слика 4. Криве учења модела за предикцију температуре.

3.4. Визуализација и интерфејс

Кориснички интерфејс (UI) је развијен у *Streamlit*-у и омогућава приказ тренутне прогнозе у виду табеле и графикона. Подаци се аутоматски освјежавају при сваком позиву сервиса, што омогућава реално-временски преглед предвиђених температура (приказ на Слици 5).



Слика 5. Приказ графичког интерфејса

3.5. Интеграција и Кубернетес конфигурација

За сваки микросервис дефинисан је посебан Deployment и Service YAML фајл. PostgreSQL база је имплементирана као *StatefulSet*, за трајно складиштење података.

Сервис *scheduler* користи CronJob ресурс који сваких сат времена покреће процес поновне обуке модела, осигуравајући да предвиђања увијек користе најновије податке. Овај приступ обезбјеђује аутоматизацију, скалабилност и отпорност на грешке, што представља суштинску предност употребе Кубернетеса у оваквим системима.

4. ЗАКЉУЧАК

У овом раду приказан је развој система за временску прогнозу заснованог на ЛСТМ моделу и Кубернетес оркестрацији. Комбинацијом Докера, Кубернетеса и машинског учења постигнута је аутоматизација, скалабилност и поузданост система.

Систем је лако проширив и погодан за даљи развој у клауд окружењима, што представља основу за будуће интеграције интелигентних апликација у реалним сценаријима.

5. ЛИТЕРАТУРА

[1] Docker (n.d.). Docker Documentation. Преузето 27.10.2025. са: https://docs.docker.com/get-started/

[2] Kubernetes (n.d.). Kubernetes Documentation. Преузето 27.10.2025. са: https://kubernetes.io/docs/home

[3] Ralf C. Staudemeyer, Eric Rothstein Morris (2019). Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks. Преузето 27.10.2025. са: https://arxiv.org/abs/1909.09586

[4] Max Planck Institute for Biogeochemistry (n.d.). Weather dataset. Преузето 27.10.2025. са: https://www.bgc-jena.mpg.de/wetter/

[5] Github репозиторијум, са кодом. Преузето 27.10.2025. са: https://github.com/MarkoVasilic/WeatherForecastingMinikube

[6] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. Nature, 323(6088), 533-536. Преузето 27.10.2025. са https://www.nature.com/articles/323533a0

[7] Ralf C. Staudemeyer, Eric Rothstein Morris (2019). Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks. Преузето 27.10.2025.

Кратка биографија:

Марко Василић рођен је 15. септембра 1998. године у Бањој Луци. Мастер рад на Факултету техничких наука у Новом Саду из области Електротехнике и рачунарства одбранио је 2025. године

Зборник радова Факултета техничких наука, НовиСад

УДК: 621.38
ДОИ: https://doi.org/10.24867/34BE27Radivojevic

Анализа рендгенских снимака плућа применом дубоких конволуционих и трансформер модела

Analysis of Chest X-ray Images Using Deep Convolutional and Transformer Models

Катарина Радивојевић, *Факултет техничких наука, Нови Сад*

Студијски програм – ЕНЕРГЕТИКА, ЕЛЕКТРОНИКА И ТЕЛЕКОМУНИКАЦИЈЕ

Кратак садржај – *Овај рад представља примену дубоких конволуционих и трансформер модела за аутоматску класификацију рендгенских снимака грудног коша ради откривања рака плућа. Предложен је каскадни систем који у првом кораку раздваја здраве од патолошких снимака, а у другом врши даљу поделу патолошких случајева на онколошке и неонколошке. Модели су фино подешени на скупу од 20000 снимака различитог порекла, уз примену техника аугментације и уравнотежења класа. Резултати показују високу осетљивост у препознавању болесних случајева и поуздано разликовање онколошких промена, што указује на могућност примене система као помоћног алата у радиолошкој дијагностици.*

Кључне речи: *: рендгенски снимци, дубоко учење, конволуционе неуронске мреже, трансформери, класификација*

Abstract – *This paper presents the application of deep convolutional and transformer models for automated classification of chest X-ray images aimed at lung cancer detection. A cascaded system is proposed, where the first stage separates healthy from pathological images, and the second stage further divides pathological cases into oncological and non-oncological. The models were fine-tuned on a dataset of 20,000 images of various origins, using augmentation and class balancing techniques. The results show high sensitivity in detecting diseased cases and reliable differentiation of oncological changes, indicating the potential of the system as an assistive tool in radiological diagnostics.*

Keywords: *chest X-ray, deep learning, convolutional neural networks, transformers, classification*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Владимир Петровић, ред. проф.

1. УВОД

Рак плућа представља један од најчешћих и најсмртоноснијих облика малигнитета у свету. Иако рано откривање значајно повећава шансе за успешно лечење, велики број случајева се и даље дијагностикује у узнапредовалој фази болести. Рендгенски снимак грудног коша остаје најдоступнији и најчешће коришћени дијагностички алат, али његова интерпретација у великој мери зависи од искуства радиолога и често је ограничена сличностима између различитих патологија.

Развој дубоких неуронских мрежа омогућио је примену аутоматизованих метода у анализи радиолошких снимака. Конволуционе мреже су се показале изузетно ефикасним у препознавању локалних структура, док трансформер модели, засновани на механизму пажње, омогућавају глобалније разумевање слике.

Циљ овог рада је развој и евалуација каскадног система дубоког учења који прво издваја потенцијално патолошке снимке, а затим врши детаљнију класификацију на онколошке и неонколошке. Оваквим приступом смањује се број пропуштених позитивних случајева и обезбеђује већа поузданост система у реалним клиничким условима.

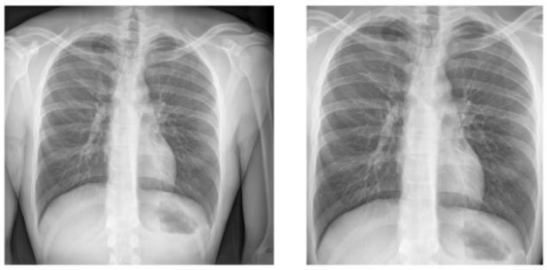
2. ОПИС СКУПА ПОДАТАКА

За потребе овог истраживања формиран је обједињен скуп података који садржи 20000 рендгенских снимака грудног коша, прикупљених из јавних извора (NIH ChestX-ray14, CheXpert, VinBigData) и приватног скупа компаније Visaris. Снимци су одабрани насумичним избором из сва четири скупа, при чему је примењен критеријум повећане осетљивости на присуство онколошких промена, како би модел био обучен на већем броју клинички релевантних случајева.

Скуп је прилагођен потребама каскадног класификатора, те су снимци разврстани у три категорије: здраве, болесне неонколошке и болесне онколошке. Пре обраде извршена је анонимизација и филтрација нечитљивих снимака, као и конверзија из DICOM у PNG формат ради лакше употребе и компатибилности са библиотекама за дубоко учење.

Да би се модел усмерио искључиво на релевантне делове слике, примењен је сопствени алгоритам за издвајање региона плућног поља, заснован на

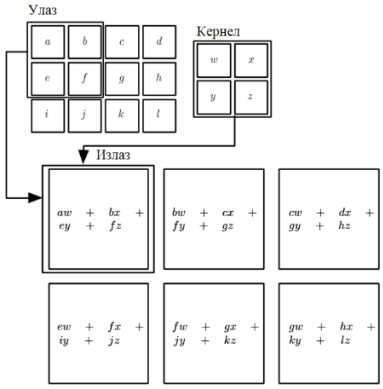
сегментацији. На слици 1 приказан је пример рендгенског снимка пре и после примене овог алгоритма, где се види да се након издвајања задржавају само региони од дијагностичког значаја, док се елиминишу делови позадине и анатомије изван плућног поља.



Слика 1. Слика пре (лево) и слика након (десно) примене алгоритма за издвајање региона плућног поља

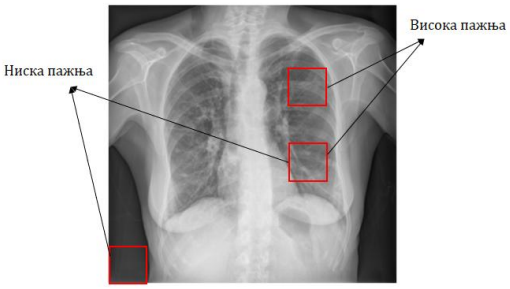
3. ТЕОРИЈСКЕ ОСНОВЕ МОДЕЛА

Конволуционе неуронске мреже (CNN) представљају основу већине савремених модела за анализу медицинских снимака. Њихова кључна предност лежи у способности да препознају локалне карактеристике на сликама као што су ивице, сенке и текстуре. Применом конволуционих филтера који пролазе кроз улазну слику. Сваки филтер (језгро) учи да издвоји специфичан образац, док се у дубљим слојевима граде све апстрактније репрезентације, што омогућава моделу да разликује нормалне и патолошке регионе. На слици 2 приказан је принцип рада конволуционог слоја, где се језгро (кернел) креће преко улазне слике и формира излазну мапу карактеристика (*feature map*) на основу прорачуна пондерисаних вредности пиксела [1].



Слика 2. Принцип рада конволуционог слоја [1]

Супротно томе, трансформерске архитектуре (Vision Transformers – ViT) користе механизам „самопажње“ (*self-attention*), који моделу омогућава да истовремено анализира целу слику и одреди које области су најрелевантније за доношење одлуке. Пажња се рачуна између мањих делова слике тј. печева (*patches*), који представљају сегменте слике трансформисане у векторе високих димензија [2]. Скларним производом тих вектора модел придаје већи значај кључним регионима унутар плућа, као што је илустровано на слици 3, док мање релевантне области добијају мању тежину.



Слика 3. Визуелизација механизма пажње у трансформерској архитектури

4. МЕТОДОЛОШКИ ПРИСТУП

Сви експерименти спроведени су у Google Colab окружењу, уз приступ графичким процесорима (GPU) преко CUDA архитектуре. Истраживање је реализовано у програмском језику Python 3, уз примену библиотеке PyTorch за дефинисање, обуку и евалуацију неуронских мрежа и трансформер модела.

4.1. Избор модела дубоког учења

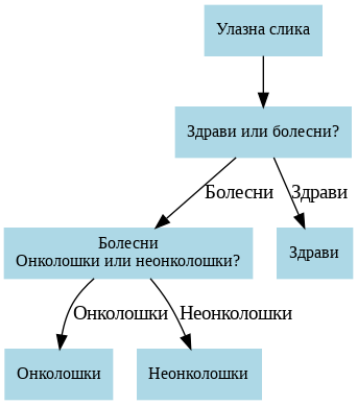
У овом истраживању су од CNN модела испробани ResNet-50 и DenseNet-121, који су се раније показали као изузетно ефикасни у анализи медицинских снимака. ResNet (Residual Network) користи резидуалне везе које омогућавају стабилнији процес обуке и избегавање деградације перформанси код дубљих мрежа. DenseNet (Densely Connected Network) уводи густе повезаности између слојева, што подстиче реупотребу карактеристика и побољшава пропагацију градијената [3].

Од трансформерских модела испитани су DeiT *(*Data-efficient Image Transformer) и Swin Transformer. DeiT је модел развијен од стране компаније Meta (Facebook AI) који представља варијанту ViT-а оптимизовану за обуку на мањим скуповима података, што га чини погодним за ово истраживање. Swin Transformer (Shifted Window Transformer) дели слику на мање, преклапајуће „прозоре“ (*windows*), унутар којих се пажња рачуна локално. Положај прозора се затим помера (*shifted windows*), чиме се омогућава размена информација између суседних региона и постепено гради хијерархијска репрезентација слике [4]. Та особина омогућава прецизније препознавање дисперзних патолошких промена које често карактеришу рак плућа.

4.2. Каскадни приступ класификацији

Да би се повећала осетљивост система и смањио број лажно негативних резултата, примењен је каскадни приступ класификацији, чији се дијаграм може видети на слици 4. Систем се састоји из два модела. Модел А прво класификује рендгенске снимке на здраве и болесне, након чега модел Б анализира само снимке означене као болесне и врши додатну поделу на онколошке и неонколошке. Оваква организација

омогућава постепено сужење анализе и бољу специјализацију сваког модела за свој ниво задатка.



Слика 4. Дијаграм каскадног система класификације

4.3. Припрема података

Формирани скуп од 20000 рендгенских снимака грудног коша подељен је на тренинг (80%), валидациони (10%) и тест (10%) подскуп, уз стратификовану поделу ради очувања односа класа. Пре учитавања у модел, све слике су скалиране на резолуцију 384×384 пиксела, која је одабрана као оптимална за истовремено тестирање конволуционих и трансформерских архитектура. Приликом креирања DataLoader-а примењене су технике аугментације као што су хоризонтално пресликавање, благо прилагођавање контраста и осветљености и додавање Гаусовог шума, док је за патолошке снимке, приликом обуке модела Б, примењена и афина трансформација са смицањем (*shear*).

За уравнотежење класа током обуке коришћен је WeightedRandomSampler, који обезбеђује равномерну заступљеност примера у сваком *batch*-у. Примери снимака пре и након примене ових трансформација приказани су на слици 5, где се може уочити ефекат повећања разноврсности података.

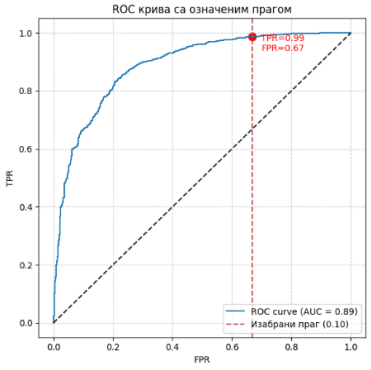
Слика 5. Примери рендгенских снимака пре (горе) и након (доле) трансформације и аугментације

4.4. Подешавање параметара и процес обуке

Сви модели су били претходно тренирани на ImageNet скупу, а затим фино подешени (*fine-tuned*) на скупу од описаном у претходном одељку. При томе је излазни класификациони слој сваког модела замењен новим бинарним слојем, док су претходни слојеви служили као екстрактори карактеристика, што је омогућило бржу конвергенцију и бољу генерализацију на медицинске слике. За обуку је коришћен AdamW оптимизатор са *weight decay* регуларизацијом и величином *batch*-а 32. Стопа учења је прилагођавана појединачно за сваку архитектуру, а примењен је и *scheduler* који је постепено умањивао њену вредност ради стабилније конвергенције. Функција губитка дефинисана је као *weighted cross-entropy*, са већом тежином за класу „болесни“ у моделу А, односно „онколошки“ у моделу Б, како би се повећала осетљивост на позитивне случајеве. За спречавање пренавикавања примењене су технике *dropout*, *weight decay* и рано заустављање (*early stopping*). Најбољи модели су изабрани према највишој вредности AUC показатеља на валидационом скупу.

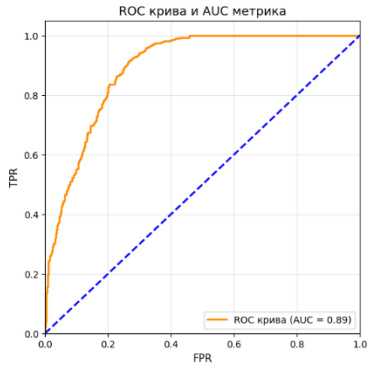
5. РЕЗУЛТАТИ И АНАЛИЗА

Након спроведених експеримената, најбоље резултате у првом кораку (модел А) постигао је DenseNet-121, док је у другом кораку (модел Б) најуспешнији био Swin Transformer. Перформансе су оцењене на тест скупу помоћу стандардних метрика: тачност (*accuracy*), прецизност (*precision*), осетљивост (*recall*), F1-скор и AUC. Код модела А посебан акценат стављен је на избор прага класификације ради повећања осетљивости према класи „болесни“. На слици 6 приказана је ROC крива модела А са изабраним прагом класификације (0.1), којим је постигнут компромис између високе осетљивости и прихватљиве прецизности, док је на слици 7 приказана матрица конфузије за модел А. За модел Б, аналогни резултати дати су на сликама 8 и 9, где је уочљиво боље одвајање класа.



Слика 6. ROC крива и AUC вредност за модел А са одабраним прагом

Слика 7. Матрица конфузије за модел А (DenseNet-121)



Слика 8. ROC крива и AUC вредност за модел Б

Слика 9. Матрица конфузије за модел Б (Swin Transformer)

Резултати приказани у Табелама 1 и 2 показују перформансе оба модела редом. Модел А је након примене прага постигао укупну тачност од 0.77, уз изразито високу осетљивост за класу „болесни“ (0.99). То указује да модел успешно препознаје готово све патолошке снимке, што је кључно за овај корак. Иако је осетљивост за класу „здрави“ нижа (0.33), овај компромис је оправдан у медицинској дијагностици где је приоритет минимизација лажно негативнох случајева. Поред тога, модел је остварио и AUC вредност од 0.89, што потврђује стабилну дискриминативну моћ између класа.

Модел Б је остварио је укупну тачност од 0.82, са уравнотеженим F1 резултатима (0.82 и 0.81). Висока осетљивост за онколошке случајеве (0.93) указује на способност модела да поуздано открије малигне промене, док је за неонколошке снимке постигнута већа прецизност (0.92), што потврђује добру дискриминацију између типова патолошких промена. И код овог модела, постигнута AUC вредност од 0.89 додатно потврђује његову поузданост и стабилност током класификације.

У целини, комбинација ова два модела показује висок потенцијал за примену у каскадним системима, где се у првом кораку обезбеђује максимална осетљивост, а у другом прецизна класификација онколошких случајева.

Табела 1. Мере успешности модела А

	Болесни	Здрави
Прецизност	0.74	0.93
Осетљивост	0.99	0.33
F1 – мера	0.85	0.49
Тачност	0.77	
AUC	0.89	

Табела 2. Мере успешности модела Б

	Онколошки	Неонколошки
Прецизност	0.74	0.92
Осетљивост	0.93	0.72
F1 – мера	0.82	0.81
Тачност	0.82	
AUC	0.89	

6. ЗАКЉУЧАК

У раду је представљен двостепени модел за класификацију, који комбинује предности конволуционих и трансформер архитектура. DenseNet-121 је постигао високу осетљивост у детекцији снимака болесних пацијената, док је Swin Transformer показао већу прецизност у разликовању онколошких и неонколошких случајева. Даља унапређења могла би се остварити проширењем скупа података и применом напреднијих техника предобраде и аугментације, чиме би се побољшала робусност и генерализација модела. Применом оваквих модела могуће је значајно унапредити процес скрининга и раног откривања онколошких промена у плућима, што представља важан корак ка примени вештачке интелигенције у клиничкој пракси.

7. ЛИТЕРАТУРА

[1] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[2] A. Dosovitskiy et al., “An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale,” ICLR, 2021.

[3] G. Huang, Z. Liu, L. van der Maaten, and K. Q. Weinberger, “Densely Connected Convolutional Networks,” *CVPR*, 2017.

[4] Z. Liu et al., “Swin Transformer: Hierarchical Vision Transformer using Shifted Windows,” ICCV, 2021.

Кратка биографија:

Катарина Радивојевић рођена је у Шапцу 2000. год. Мастер рад на Факултету техничких наука у Новом Саду, из области Енергетика, електроника и телекомуникације – смер обрада сигнала, одбранила је 2025.год.

Контакт: kradivojevic1907@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

UDK: 4.75
ДОИ: https://doi.org/10.24867/34BE29Jovic

ОСОБИНЕ БРОКЕРА ПОРУКА И ЊИХОВА ПРИМЕНА У ДИСТРИБУИРАНИМ СИСТЕМИМА

CHARACTERISTICS OF MESSAGE BROKERS AND THEIR APPLICATION IN DISTRIBUTED SYSTEMS

Драгана Јовић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Рад истражује и анализира изабране брокере порука, са фокусом на њихове кључне карактеристике као што су постојаност и очување редоследа порука. У раду се разматра како се ове особине примењују и имплементирају у дистрибуираним системима. Такође, рад се бави евалуацијом перформанси брокера порука.*

Кључне речи: *Брокер порука, Перформансе, Кашњење, Пропусност, Постојаност, Редослед порука, Евалуација*

Abstract – *The paper explores and analyzes selected message brokers, focusing on their key features such as durability and message ordering. The paper examines how these characteristics are applied and implemented in distributed systems. Additionally, the paper evaluates the performance of the message brokers.*

Keywords: *Message broker, Performance, Latency, Throughput, Durability, Messaging order, Evaluation*

1. УВОД

Савремене софтверске апликације често зависе од удаљених услуга и података, што чини интеграцију кључном у дистрибуираним архитектурама. Асинхрона комуникација, реализована путем брокера порука, омогућава да задаци који захтевају више времена буду обрађени у позадини без блокирања захтева. Овакав приступ помаже у решавању изазова дистрибуираних система као што су непоуздане мреже и чврста повезаност [1]. У последње време, нови брокери порука фокусирају се на ниско кашњење и високе перформансе, што значајно утиче на ефикасност и поузданост система.

2. ОПИС РЕШАВАНОГ ПРОБЛЕМА

Рад решава проблем избора адекватног брокера порука за дистрибуирани финансијски систем, у коме су постојаност порука, очување редоследа и перформансе од суштинске важности. У ери када дистрибуирани системи играју кључну улогу у обради података у реалном времену, избор одговарајућег брокера порука постаје критичан фактор који утиче на укупне перформансе, скалабилност и поузданост система.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био проф. др Александар Ердељан

Брокери порука представљају кључни комуникациони слој у дистрибуираним системима, омогућавајући безбедан пренос, постојаност података и отпорност на грешке. У системима са великим количинама података и критичним апликацијама, избор брокера директно утиче на ефикасност и способност система да одговори на различита оптерећења. У зависности од потреба, неки брокери су бољи за високу пропусност, док су други погоднији за обраду у реалном времену, где је кашњење кључно. Кашњење је посебно важно за апликације које захтевају брзу реакцију, попут финансијских или *SCADA* система.

Постојаност порука обезбеђује поуздано чување података и при кваровима, што је критично за системе где је губитак података неприхватљив. Редослед обраде је такође важан када је потребано очувати интегритет података.

Циљ рада је анализа постојаности и очувања редоследа порука код различитих брокера, како би се утврдило који најбоље одговара захтевима дистрибуираног финансијског система. Истраживање обухвата ***Apache ActiveMQ***, ***Artemis*** и ***Kafka***-у, кроз анализу њихових карактеристика, перформанси под оптерећењем и понашања у реалним сценаријима.

Студија случаја заснована је на *AdInsure* систему, који представља платформу за животна и неживотна осигурања, развијеном у *C#* и *.NET 8*. Постојећа инфраструктура за размену порука омогућава лаку интеграцију са брокерима и поуздано тестирање. На основу резултата, рад предлаже брокер који најбоље испуњава критеријуме поузданости, постојаности и перформанси у систему са високим захтевима за скалабилност и ефикасност.

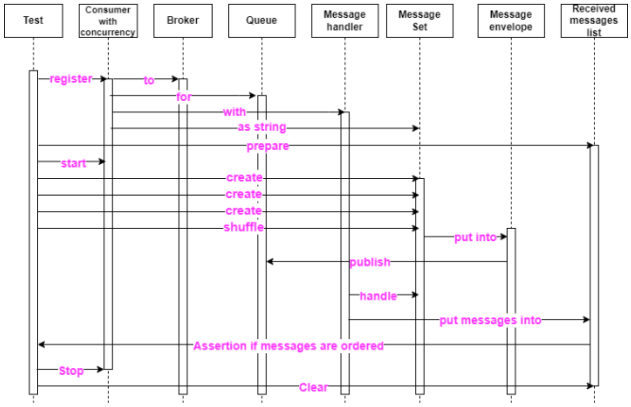
3. ЕВАЛУАТОР БРОКЕРА ПОРУКА

MessageBrokerEvaluator је *.NET 8* конзолна апликација за тестирање постојаности и редоследа порука код различитих брокера. Користи инфраструктуру за размену порука *AdInsure* платформе и конфигурацију из *messagingSettings.json* датотеке, која дефинише магистралу, канале, редове и теме. Циљ је утврдити који брокер најбоље одговара потребама финансијских система попут *AdInsure*-а.

Тестирање се спроводи кроз интеграцијске тестове написане у *C#*-у и *NUnit*-у. Прослеђивање порука од произвођача до потрошача није посебно приказано, јер је то већ обезбеђено самим брокером.

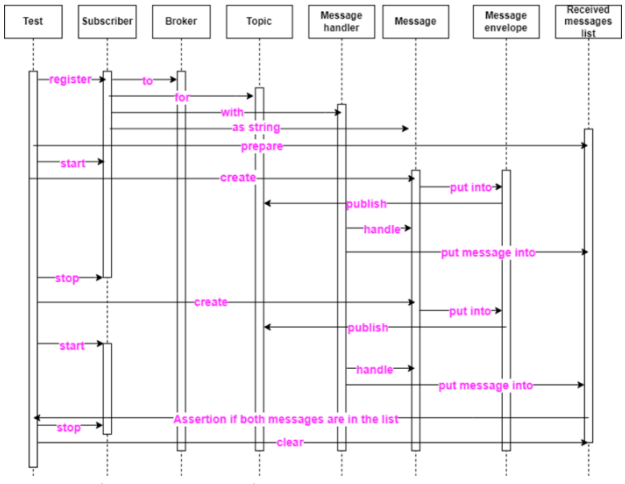
Тестови редоследа порука: Ови тестови проверавају да ли брокер може гарантовати очување редоследа

порука које се шаљу у ред или тему. Више порука се шаље у кратким временским интервалима, а тест осигурава да се поруке конзумирају редоследом којим су послате. Посебно је важно да се провери да ли је *FIFO* (енгл. *First-In-First-Out)* редослед очуван чак и у случају конкуренције међу конзументима. На слици 3.2 је приказан ток тестирања очувања редоследа порука у реду у облику секвенцијалног дијаграма.



Слика 3.2. *Провера очувања редоследа порука у реду*

Тестови постојаности: Ови тестови су осмишљени да провере да ли брокер подржава постојаност претплатника. Тестови симулирају сценарије где претплатник на тему губи везу или је привремено недоступан, па се након неког времена поново повезује. Проверава се да ли претплатник прима поруке које су послате док је био недоступан, што је кључно за финансијске системе где ниједна порука не сме бити изгубљена. На слици 1 је приказан ток тестирања постојаности претплатника на теми у облику секвенцијалног дијаграма.



Слика 1. *Провера издржљивости претплатника на теми*

3.1 Резултати евалуације *ActiveMQ* брокера

У евалуацији *ActiveMQ* брокера, инстанца је покренута као Докер контејнер коришћењем званичне слике *rmohr/activemq* са *Docker Hub*-а. За транспортни протокол коришћена је библиотека *Apache.NMS.ActiveMQ*.

ActiveMQ подржава очување редоследа порука, посебно у сценарију са *једним конзументом по реду*, као и кроз *групе порука*, где се очувава редослед унутар сваке групе путем идентификатора.

Што се тиче постојаности претплатника, у случају постојаних тема сваком претплатнику се чува његова копија поруке. То се постиже конфигурисањем *clientID* и имена претплатника у *JMS* конекцији, што омогућава да претплатник добије све поруке након поновног повезивања [2].

3.2. Резултати евалуације *Artemis* брокера

При евалуацији *Artemis* брокера, инстанца је покренута као Докер контејнер користећи званичну слику *apache/activemq-artemis*. Због подршке за *OpenWire* протокол, коришћена је иста библиотека *Apache.NMS.ActiveMQ,* без потребе за додатним изменама у коду.

За разлику од *ActiveMQ*, *Artemis* користи ***Fully Qualified Queue Name (FQQN)*** за управљање трајним претплатама и виртуелним темама. Уместо класичних назива, користи се структура као што је *VirtualTopic.{Тема}::Consumer.{Претплатник}.Virtual Topic.{Тема}*, што омогућава директан приступ редовима претплатника. Ово понашање се конфигурише параметром ***virtualTopicConsumerWildcards*** [2].

3.3 Резултати евалуације *Kafka* брокера

Kafka брокер је покренут као Докер контејнер користећи званичну *apache/kafka* слику, а за транспорт је коришћена библиотека *Confluent.Kafka*.

Редослед порука је загарантован само унутар једне партиције, што ограничава паралелизам. Ради очувања редоследа на вишем нивоу користе се приступи као што су **алгоритам агрегатора и сортирања**, **коришћење јединственог потрошача унутар групе**, и **примена протокола групног потврђивања и емитовања**. [3].

Постојаност потрошача у *Kafka*-и се остварује кроз **чување и комитовање позиције**, као и коришћењем **потрошачких група**. У *AdInsure* систему, потрошачи деле исти *group ID*, а поставка *AutoOffsetReset = Latest* омогућава наставак читања од последње обрађене поруке. Ручно комитовање позиције након обраде повећава поузданост у односу на аутоматско.

Резултати евалуације показују да сви брокери подржавају концепте очувања редоследа порука и постојаност претплатника. *Artemis* се истиче као једноставна замена за *ActiveMQ*, са идентичним протоколима и библиотекама, осим код виртуелних дестинација које захтевају мање измене конфигурације. У поређењу са *Kafka*-ом, *Artemis* и *ActiveMQ* нуде једноставније очување редоследа, док је у *Kafka*-и редослед ограничен на ниво партиција, што ограничава паралелизам. У финансијском дистрибуираном систему, где су редослед, постојаност и перформансе кључни, ови аспекти су важни за избор брокера. Не постоји универзални избор – прави избор зависи од специфичних приоритета система и захтева пословања.

4. ПЕРФОРМАНСЕ БРОКЕРА

Метрике перформанси играју важну улогу у откривању ефикасности и поузданости брокера порука, пружајући драгоцен увид у њихово оперативно понашање и потенцијал за скалабилност. **Пропусност** и **кашњење** су две основне метрике перформанси за брокере порука [4].

Пропусност указује на ефикасност система у обради порука, одражавајући његову способност да ефикасно управља великим количинама података. С друге стране, кашњење се односи на кашњење које једна порука доживљава док пролази кроз систем, наглашавајући брзину и одзив у испоруци порука.

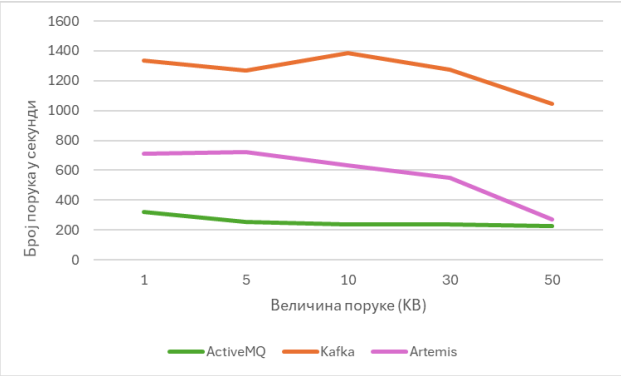
За тестирање перформанси брокера порука *ActiveMQ*, *Artemis* и *Kafka* коришћено је локално окружење, које омогућава потпуну контролу над хардверским ресурсима и елиминисање мрежних варијација. Спецификација хардвера на којем су тестиране перформансе су: *Intel i7* процесор, *32 GB RAM*, *500 GB SSD*.

4.1 Пропусност

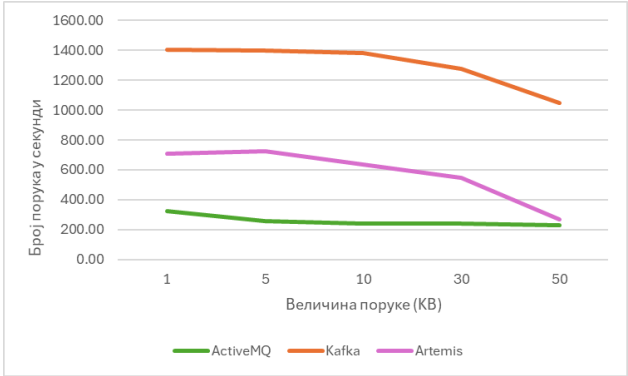
Пропусност порука означава број порука које се могу обрадити у просеку по секунди за N број порука. Овај показатељ мери колико порука може бити обрађено у одређеном временском оквиру. Израчунава се као:

$$\text{пропусност} = \frac{\text{укупан број обрађених порука}}{\text{унупно време потребно за обраду порука}}$$

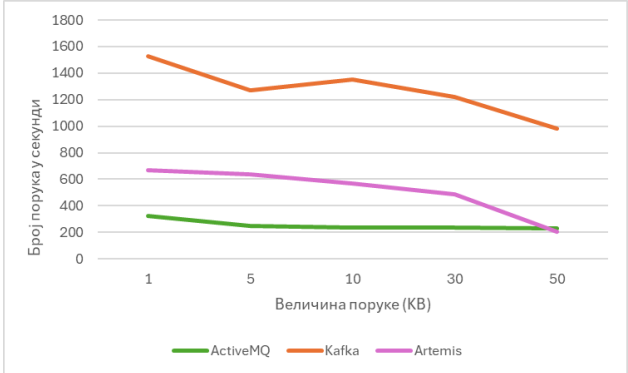
Програм за мерење пропусности развијен је у *C#* као конзолна апликација и симулира паралелно слање порука преко више произвођача. Тестирају се различити сценарији са бројем произвођача (16, 24, 32) и величином порука (1–50 KB), у трајању од 60 секунди. Бележе се укупан број послатих порука и пропусност (поруке/секунди). Апликација користи *AdInsure* инфраструктуру и транспортне протоколе у складу са тестираним брокером. Резултати су приказани на сликама 2, 3 и 4.



Слика 2. Резултати пропусности брокера за 16 паралелних произвођача у зависности од величине порука (од 1 до 50), где је величине порука представљена у килобајтима (kB)



Слика 3. Резултати пропусности брокера за 24 паралелна произвођача у зависности од величине порука (од 1 до 50), где је величине порука представљена у килобајтима (kB)



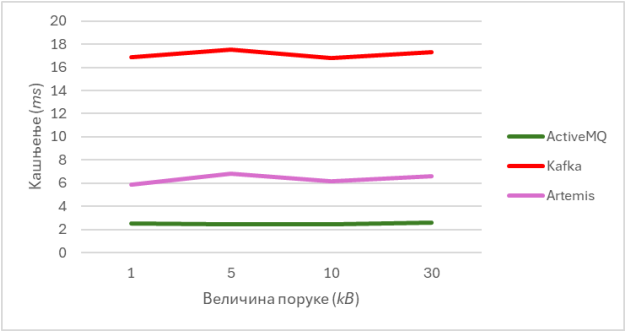
Слика 4. Резултати пропусности брокера за 32 паралелна произвођача у зависности од величине порука (од 1 до 50), где је величине порука представљена у килобајтима (kB)

4.2. Кашњење

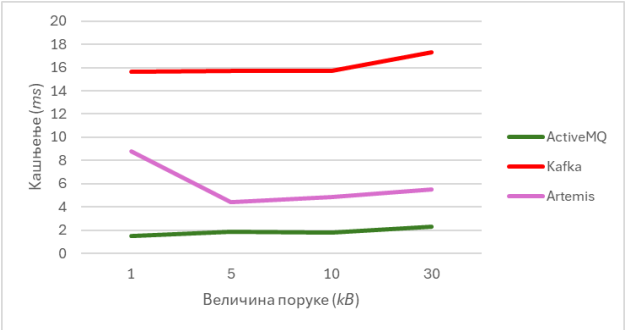
Просечно кашњење представља просечно време кашњења за све поруке у скупу од N порука. Израчунава се као:

$$\text{просечно кашњење} = \frac{1}{N}\sum_{n=1}^{N} \text{кашњење}(n)$$

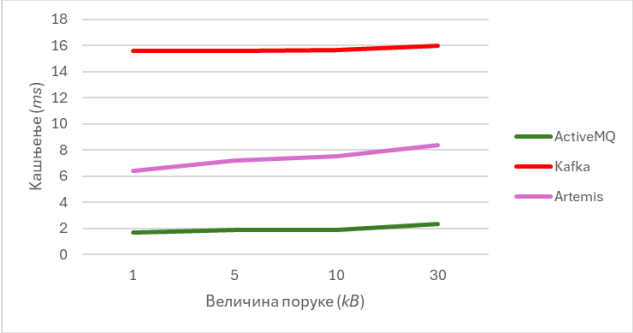
Кашњење се мери у склопу програма развијеног у *C#* конзолној апликацији. Тестирање кашњења подразумева следеће кораке: регистрација потрошача на канал за пријем порука који бележи време пријема, слање порука од стране произвођача, који за сваку поруку бележи време слања и израчунавање разлике између времена слања и пријема порука. На крају, програм израчунава просечно кашњење свих порука и приказује резултате. Тестирање је спроведено за *ActiveMQ*, *Artemis* и *Kafka* брокере, сви са инстанцама на Докеру. Резултати су дати у наставку, на сликама 5, 6, и 7 и графички илуструју кашњење у зависности од броја послатих порука.



Слика 5. Резултати кашњења брокера у милисекундама (ms) за 1000 послатих порука у зависности од величине порука (1-30) у килобајтима (kB)



Слика 6. Резултати кашњења брокера у милисекундама (ms) за 10000 послатих порука у зависности од величине порука (1-30) у килобајтима (kB)



Слика 7. Резултати кашњења брокера у милисекундама (ms) за 50000 послатих порука у зависности од величине порука (1-30) у килобајтима (kB)

На основу спроведених тестова перформанси, утврђено је да сваки од анализираних брокера – *ActiveMQ*, *Artemis* и *Kafka* – има своје специфичне предности и мане у зависности од сценарија употребе. *ActiveMQ* се истиче најнижим кашњењем, што га чини погодним за апликације које захтевају брзу обраду порука, али његова пропусност опада при повећању оптерећења. *Artemis* нуди баланс између пропусности и кашњења, што га чини добрим избором за системе који захтевају компромис између брзине испоруке и обима порука. С друге стране, *Kafka* доминира у пропусности, нарочито у сценаријима са великим бројем произвођача, али уз жртвовање кашњења, што је чини идеалном за обраду великих количина података где брзина испоруке није критична.

5. ЗАКЉУЧАК

Обезбеђивање постојаности и редоследа у дистрибуираном финансијском систему могуће је код свих разматраних брокера порука, али са различитим нивоима сложености и перформанси. *ActiveMQ* је најбољи избор за системе са ниским кашњењем и умереним оптерећењем, док *Artemis* пружа добар компромис између пропусности и кашњења. Оба брокера омогућавају релативно једноставну имплементацију очувања редоследа порука као и постојаности брокера. *Kafka*, иако најпогоднији за високу пропусност и скалабилност, захтева сложенију имплементацију за очување редоследа и постојаности и има веће кашњење. Избор брокера зависи од специфичних захтева апликације, укључујући критичне факторе као што су кашњење, пропусност и обим обраде података.

6. ЛИТЕРАТУРА

[1] Magnoni L: “Modern messaging for distributed sytems”, J. Phys.: Conf. Ser. 608 012038, 2015

[2] *ActiveMQ*, https://activemq.apache.org/ - датум последњег приступа новембар 2024. године

[3] Shashank Kumar, Aryan Jadon, Sachin Sharma: *“Global Message Ordering using Distributed Kafka Clusters”,* 2023 15th International Conference on Innovations in Information Technology (IIT), 2023

[4] John, Vineet, and Xia Liu. "A survey of distributed message broker queues." *arXiv preprint arXiv:1704.00411* (2017).

Кратка биографија:

Драгана Јовић рођена је у Новом Саду 1991. год. Основну школу „Петар Кочић“ завршила је у Темерину 2006. године. Гимназију „Светозар Милетић“ у Новом Саду завршила је 2010. године. Основне академске студије на Факултету техничких наука у Новом Саду, одсек Електротехника и рачунарство, смер Рачунарство и аутоматика, усмерење Примењене рачунарске науке и информатика, завршила је 2014. године. Мастер академске студије на Факултету техничких наука у Новом Саду, студијски програм Електроенергетски софтверски инжењеринг, уписала је 2014. године.

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/34BE30Jovin

KOROZ - *eBPF BAZIRANI OSVEŽIVAČ DNS CACHE-a*

KOROZ - eBPF BASED DNS CACHE REFRESHER

Vladimir Jovin, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Ovaj rad istražuje upotrebu eBPF tehnologije za optimizaciju DNS saobraćaja. Implementacijom sistema baziranog na eBPF-u, XDP-u i Rust programskom jeziku, predstavljena je efikasna inspekcija i manipulacija mrežnim paketima u realnom vremenu. Prikazani su teorijski osnovi, opisane ključne komponente rešenja, rezultati i predloženi pravci daljeg razvoja, uključujući integraciju heuristika i veštačke inteligencije za optimizaciju DNS keš mehanizma.*

Ključne reči: *dns, ebpf, rust, ddi*

Abstract – *This paper explores the use of eBPF technology for DNS traffic optimization. By implementing a system based on eBPF, XDP, and the Rust programming language, real-time inspection and manipulation of network packets is demonstrated. Theoretical foundations are presented, key solution components are described, results are evaluated, and future development directions are proposed, including the integration of heuristics and artificial intelligence for DNS cache optimization.*

Keywords: *dns, ebpf, rust, ddi*

1. UVOD

U radu je predstavljena primena eBPF (Extended Berkeley Packet Filter) tehnologije za unapređenje performansi i sigurnosti DNS (Domain Name System) sistema. Korišćenjem XDP (Express Data Path) mehanizma i Aya razvojonog okvira u Rust-u, omogućena je brza i sigurna obrada DNS upita na nivou jezgra operativnog sistema.

Rad daje pregled teorijskih osnova, motivaciju za izbor tehnologija i opisuje mane tradicionalnih DNS rešenja. Cilj je detaljno prikazati implementaciju, analizu rezultata i smernice za dalji razvoj u oblasti optimizacije mrežnih protokola.

Korišćenjem XDP mehanizma, omogućava se efikasna inspekcija i obrada mrežnog saobraćaja pre nego što stigne do mrežnog interfejsa. Ova metoda ne samo da dozvoljava manipulaciju DNS upita i odgovora, već i omogućava dodatne mogućnosti za analizu i filtriranje saobraćaja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Veljko Petrović, docent

DNS serveri se suočavaju sa problemima u pogledu performansi i sigurnosti, što može dovesti do usporavanja mrežnih aplikacija i servisa. Korišćenje eBPF tehnologije omogućava implementaciju rešenja za optimizaciju DNS saobraćaja, uključujući inteligentno keširanje, prediktivno učitavanje i analizu obrazaca korišćenja u realnom vremenu.

Tehnologije za obradu mrežnog saobraćaja su ključne za unapređenje performansi i sigurnosti mrežnih sistema. Jedna od najznačajnijih inovacija u ovoj oblasti je eBPF (Extended Berkeley Packet Filter), tehnologija koja omogućava izvršavanje korisničkog koda unutar jezgra operativnog sistema, pružajući mogućnost za inspekciju i manipulaciju mrežnim paketima.

Rad je organizovan u pet ključnih poglavlja: uvod koji definiše problematiku DNS optimizacije, teorijski okvir koji temeljno obrazlaže DNS i eBPF koncepte, detaljna implementacija sistema "Koroz" sa tehničkim aspektima XDP obrade, evaluacija performansi sa konkretnim metrikama, te zaključak sa smernicama za dalja istraživanja.

2. DNS

DNS je sistem koji omogućava prevod ljudski čitljivih naziva domena u IP adrese, čime se olakšava pristup resursima na internetu [1; 2]. Sistem je razvijen u ranim 1980-im godinama kao odgovor na rastući broj računara povezanih na internet [3]. Pre DNS-a, korišćen je centralizovani *hosts.dat* fajl koji je sadržavao informacije o svim računarima na mreži, što je postalo neodrživo sa rastom interneta.

DNS je prvi put definisan u RFC 1034 [1] i RFC 1035 [2], objavljenim u novembru 1987. godine. Ovi dokumenti su postavili temelje za hijerarhijsku strukturu DNS-a i osnovne funkcionalnosti koje se koriste i danas. DNS funkcioniše na osnovu hijerarhijske strukture koja se sastoji od root servera na vrhu, TLD (Top-Level Domain) servera, i autoritativnih servera za specifične domene.

DNS obezbeđuje nekoliko ključnih funkcionalnosti: prevođenje imena u IP adrese, distribuciju podataka kroz decentralizovanu strukturu, keširanje odgovora za poboljšanje performansi, i podršku za različite tipove zapisa koji omogućavaju kompleksne mrežne konfiguracije.

3. eBPF

eBPF predstavlja tehnologiju koja je evoluirala iz originalnog BPF protokola razvijenog u ranim 1990-im godinama [4]. Dok je originalni BPF omogućio filtriranje mrežnih paketa, eBPF je proširio ove mogućnosti daleko van mrežnog konteksta, omogućavajući izvršavanje sigurnog koda u različitim delovima jezgra operativnog sistema.

Arhitektura eBPF-a se sastoji od nekoliko ključnih komponenti. eBPF programi se pišu u specijalizovanom jeziku sličnom C-u i kompajliraju se u eBPF bajt kod. Ovi programi prolaze kroz rigorozan proces verifikacije koji osigurava da ne mogu dovesti do nevalidnih stanja ili neovlašćenog pristupa memoriji [5]. Verifikator analizira sve moguće putanje izvršavanja i garantuje da program neće pristupiti nedozvoljenim memorijskim lokacijama.

3.1. Povezanost između DNS-a i eBPF-a

Kombinacija DNS-a i eBPF-a daje mogućnosti za optimizaciju mreža. Korišćenjem eBPF-a, moguće je implementirati efikasne mehanizme za inspekciju DNS upita i odgovora u realnom vremenu, bez značajnog uticaja na performanse sistema. Ova tehnologija omogućava analizu DNS saobraćaja, identifikaciju obrazaca korišćenja, i implementaciju inteligentnih strategija keširanja.

eBPF programi mogu prikupljati detaljne statistike o DNS saobraćaju, uključujući informacije o najčešće traženim domenima, latencijama upita, i obrascima pristupa. Ovi podaci mogu biti korišćeni za optimizaciju DNS servera i implementaciju prediktivnog keširanja koji može poboljšati performanse mrežnih aplikacija.

Važno je napomenuti da je ovaj pristup potpuno agnostičan prema konkretnoj DNS implementaciji, što znači da može raditi sa različitim DNS serverima kao što su BIND, Unbound, ili PowerDNS, bez potrebe za modifikacijama postojećih sistema.

4. MOTIVACIJA I TEHNOLOGIJE

Razvoj mrežnih aplikacija zahteva optimizaciju performansi i sigurnosti. U velikim mrežama, opterećenje DNS servisa prati organske obrasce pri čemu su TTL vrednosti uglavnom tipične za različite tipove zapisa. Analiza krive opterećenja DNS servera pokazuje da se određeni upiti ponavljaju u kratkim vremenskim intervalima, često pre nego što isteknu njihovi TTL-ovi.

Ova observacija otkriva priliku za optimizaciju. Umesto da se čeka da TTL istekne prirodno, sistem može proaktivno da osveži zapise koji se često koriste, pre nego što isteknu. Ovaj pristup može drastično smanjiti latenciju za krajnje korisnike i poboljšati ukupne performanse sistema.

eBPF tehnologija pruža mehanizam za implementaciju ovakve optimizacije jer omogućava posmatranje DNS saobraćaja bez uticaja na postojeće sisteme, kao i donošenje odluka o tome koji zapisi treba da se osveže u realnom vremenu.

4.1. Aya radni okvir

Za razliku od tradicionalnih pristupa koji se oslanjaju na libbpf ili bcc, Aya je izgrađena od nule isključivo u Rust-u, koristeći samo libc biblioteku kao zavisnost za sistemske pozive [6].

Jedan od benefita Aya razvojnog okvira je korišćenje musl libc umesto GNU libc (glibc). GNU C Library je podrazumevana standardna biblioteka na većini Linux distribucija i poznata je po svojoj bogatoj funkcionalnosti i širokoj kompatibilnosti. Međutim, zbog svoje kompleksnosti, glibc zahteva dinamičko linkovanje što može stvoriti probleme sa kompatibilnošću između različitih verzija sistema. Dodatno, musl je implementacija standardne C biblioteke zasnovana na API-ju sistemskih poziva Linuxa, uključujući interfejse definisane u osnovnom jezičkom standardu, kao i široko prihvaćenim proširenjima, koja omogućava potpuno statičko linkovanje.

Aya takođe pruža podršku za BPF Type Format (BTF) što omogućava da eBPF programi kompajlirani za jednu verziju kernela rade na različitim verzijama kernela bez potrebe za rekompajliranjem. Ova funkcionalnost je kritična za distribuciju eBPF aplikacija u heterogenim okruženjima.

4.2. XDP

XDP (eXpress Data Path) je izabran kao primarna tehnologija za obradu paketa zbog svojih prednosti u odnosu na alternative kao što su TC (Traffic Control) i tradicionalno procesiranje kroz SKB (Socket Buffer) strukturu.

XDP omogućava izvršavanje eBPF programa na najranijem nivou mrežnog steka, direktno na nivou mrežnog interfejsa. Ovo omogućava inspekciju i obradu paketa pre nego što stignu do bilo kog dela mrežnog steka operativnog sistema, što rezultuje niskim latencijama i visokim performansama.

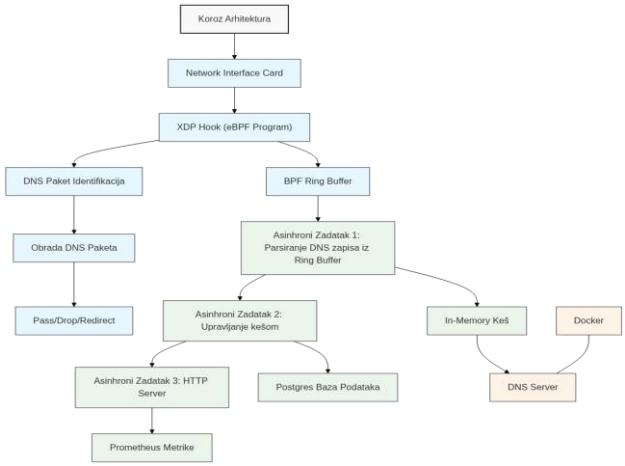
U poređenju sa TC (Traffic Control), koji omogućava upravljanje mrežnim saobraćajem na višem nivou u mrežnom steku, XDP pruža direktan pristup paketima bez potrebe za alokacijom SKB struktura. Ovo uklanja kompleksnost koja je povezana sa procesiranjem paketa.

SKB (Socket Buffer) je struktura podataka koja se koristi za skladištenje informacija o mrežnim paketima unutar jezgra. Iako je SKB veoma fleksibilan i podržava kompleksne operacije, njegova upotreba uvodi kompleksnost u obliku alokacije memorije i kopiranja podataka. XDP, s druge strane, radi direktno sa paketima u njihovoj originalnoj memorijskoj lokaciji, što uklanja potrebu za dodatnim kopiranjem podataka.

5. IMPLEMENTACIJA

Implementacija se sastoji od dve glavne komponente koje rade u koordinaciji: eBPF program koji se izvršava u jezgru operativnog sistema na XDP sklopci, i korisnički program koji upravlja prikupljenim podacima i implementira logiku za optimizaciju DNS keša (Slika 1).

eBPF program je odgovoran za inspekciju DNS saobraćaja koji prolazi kroz specifikovani mrežni interfejs. Program identifikuje DNS pakete analizirajući Ethernet i IP zaglavlja, a zatim UDP zaglavlje kako bi potvrdio da se radi o DNS saobraćaju (port 53). Kada se identifikuje relevantni paket, program ekstraktuje potrebne informacije i šalje ih u korisnički prostor putem BPF prstenastog bufera.



Slika 1: *Arhitektura sistema*

Korisnički program implementira složeniju logiku sistema kroz četiri glavna asinhrona zadatka.

Prvi zadatak kontinuirano čita podatke iz BPF prstenastog bufera, parsira DNS odgovore i prosleđuje ih za dalju obradu.

Drugi zadatak skladišti DNS odgovore u memorijski keš implementiran kao binarni hip, kao i u perzistentnu PostgreSQL bazu podataka za dugoročno čuvanje i analizu.

Treći zadatak implementira analizu DNS zapisa na osnovu njihovih TTL vrednosti i donošenje odluka o tome koji zapisi treba da se prethodno osveže. Ovaj zadatak periodično prolazi kroz keš, identifikuje zapise koji se približavaju isteku, i pokreće proces invalidacije i repopulacije kroz eksterni DNS resolver.

Četvrti zadatak implementira HTTP server koji omogućava pristup metrikama sistema za potrebe monitoringa (Prometheus), kao i REST API za pristup trenutnom stanju keša i statistikama.

5.1. BPF prstenasti bufer kao mehanizam komunikacije

BPF prstenasti bufer je izabran kao primarni mehanizam za komunikaciju između eBPF programa i korisničkog prostora zbog svojih značajnih prednosti u odnosu na alternative kao što je BPF *perf buffer* [7]. Prstenasti bufer predstavlja višestruki proizvođač, jednostruki potrošač (*MPSC*) red koji može bezbedno da se deli između više CPU-ova istovremeno.

U poređenju sa perf buferom, BPF prstenasti bufer nudi nekoliko ključnih prednosti. Prvo, efikasnije korišćenje memorije jer koristi jedan zajednički bafer umesto više bafera po CPU-u. Drugo, garantovane su bolje garancije redosleda događaja jer se svi događaji emituju u zajedničkom buferu umesto u *per-CPU* buferima koji se mogu potrošiti različitim brzinama.

Treće, prstenasti bufer podržava "*reserve/submit*" API koji omogućava rezervaciju prostora za podatke unapred, čime se izbegava dodatno kopiranje memorije i omogućava efikasnije korišćenje resursa. Ova funkcionalnost je posebno važna u visoko performantnim scenarijima gde svako kopiranje podataka može imati značajan uticaj na performanse.

5.2. Strategije optimizacije i heuristike

Sistem implementira strategiju za odlučivanje o tome koji DNS zapisi treba da se osveže. Osnovna heuristika se zasniva na analizi TTL vrednosti i obrasce pristupa zapisima. Zapisi koji se često koriste i čiji TTL se približava isteku imaju viši prioritet za osvežavanje.

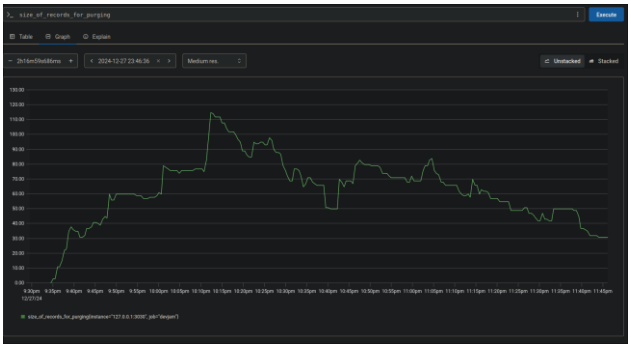
Algoritam koristi binarni hip strukturu podataka za efikasno održavanje zapisa sortiranih po vremenu isteka. Ova struktura omogućava *O(log n)* složenost za dodavanje novih zapisa i *O(1)* složenost za pristup zapisu koji će prvi da istekne. Periodično, zadatak prolazi kroz *heap* i identifikuje zapise koji se nalaze unutar konfigurabilnog vremenskog okvira pre isteka. Za zapise koji se identifikuju za osvežavanje, prvo se poziva proces invalidacije koji uklanja postojeći zapis iz DNS resolver keša. Nakon uspešne invalidacije, pokreće se proces repopulacije koji eksplicitno traži svežu verziju zapisa od autoritativnog servera.

Takođe su implementirane metrike za praćenje efikasnosti optimizacije, uključujući broj uspešnih invalidacija, broj neuspešnih operacija, latencije operacija, i ukupno vreme uštede za krajnje korisnike. Ove metrike omogućavaju kontinuirano podešavanje sistema i identifikaciju mogućnosti za dalje poboljšanje.

6. REZULTATI

Testiranje sistema je sprovedeno u kontrolisanom uobičajenom okruženju upotrebe tokom nekoliko dana kontinuiranog rada. Prometheus metrike pokazuju da sistem uspešno identifikuje i procesira DNS saobraćaj, sa dominantnim učešćem A (IPv4) i AAAA (IPv6) zapisa što je u skladu sa očekivanjima.

Analiza kardinaliteta reda za invalidaciju pokazuje stabilne vrednosti sa maksimumom od 115 zapisa u posmatranom periodu i prosekom značajno ispod tog nivoa (Slika 2).



Slika 2. *Kardinaliet reda zapisa u memoriji*

Metrike o broju invalidiranih i repopuliranih zapisa pokazuju obrasce DNS saobraćaja. Vidljivo je da dominiraju A (IPv4) rekordi, koji su za 2 sata dostigli 14000 akcija. Sistem demonstrira sposobnost da prati varijacije u opterećenju i prilagodi svoje operacije u skladu sa tim (Slika 3).

Slika 3: *Akcije nad zapisima*

Posebno značajna je observacija da implementacija održava nizak nivo neuspešnih operacija, što ukazuje na robusnosti efikasno rukovanje greškama. Ova karakteristika je kritična za produkcijska okruženja.

6.1. Pravci budućeg razvoja

Jedan od pravaca budućeg razvoja je proširenje sistema na korišćenje proizvoljnih heuristika i integracija AI modela. Ideja je da se sistem transformiše u otvorenu platformu koja klijentima omogućava implementaciju proizvoljne logike za optimizaciju putem REST API-ja.

Ovaj pristup bi omogućio kreiranje ekosistema gde različite komponente mogu da dele svoje heuristike i strategije optimizacije, što bi dovelo do poboljšanja efikasnosti DNS sistema. AI modeli bi mogli da analiziraju obrasce u DNS saobraćaju i predvide koji zapisi će verovatno biti potrebni u budućnosti, omogućavajući proaktivnost.

Drugi značajan pravac razvoja je dodatno pomeranje logike iz korisničkog prostora u eBPF program. Kako se eBPF tehnologija dalje razvija i podržava sve kompleksnije operacije, postaje moguće implementirati logiku direktno u jezgru. Ovo bi moglo da poboljša performanse eliminišući potrebu za komunikacijom između jezgra i korisničkog prostora za mnoge operacije.

7. ZAKLJUČAK

Ovaj rad demonstrira primenu eBPF tehnologije za optimizaciju DNS saobraćaja kroz implementaciju koja posmatra DNS upite i odgovore i proaktivno osvežava DNS keš na osnovu uočene potrebe. Kombinacija eBPF-a, XDP-a, Aya razvojnog okvira i Rust programskog jezika pokazala se kao adekvatna platforma za razvoj mrežnih aplikacija.

Predstavljene su praktične primene eBPF tehnologije za DNS optimizaciju, implementacija efikasnog sistema za analizu mrežnog saobraćaja u realnom vremenu, i razvoj arhitekture koja može da se prilagodi različitim okruženjima i zahtevima.

Integracija eBPF-a sa DNS-om omogućava razvoj naprednih rešenja koja poboljšavaju performanse, sigurnost i efikasnost mrežnih usluga. Ova sinergija predstavlja značajan korak napred u optimizaciji mrežnog saobraćaja i unapređenju korisničkog iskustva. Korišćenjem eBPF-a, XDP-a i Rust-a, moguće je implementirati efikasne mehanizme za inspekciju i manipulaciju mrežnim paketima u realnom vremenu. Dalji razvoj može dodatno unaprediti ove elemente i omogućiti još složenije i efikasnije operacije direktno u jezgru operativnog sistema.

8. LITERATURA

[1] RFC 1034 - DOMAIN NAMES - CONCEPTS AND FACILITIES
https://www.rfc-editor.org/rfc/rfc1034
(pristupljeno u decembru 2024.)

[2] RFC 1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
https://www.rfc-editor.org/rfc/rfc1035
(pristupljeno u decembru 2024.)

[3] Hon K 2024 Web, URLs, domains, DNS Technology and security for lawyers and other professionals (Edward Elgar Publishing) pp 317–36

[4] eBPF
https://ebpf.io/what-is-ebpf/
(pristupljeno u decembru 2024.)

[5] eBPF Verifier
https://ebpf.io/what-is-ebpf/#verification
(pristupljeno u decembru 2024.)

[6] Aya framework
https://aya-rs.dev/
(pristupljeno u decembru 2024.)

[7] BPF Ring Buffer
https://docs.kernel.org/bpf/ringbuf.html
(pristupljeno u decembru 2024.)

Kratka biografija:

Vladimir Jovin rođen je u Novom Sadu 1999. godine. Osnovu školu i gimnaziju završio je u Novom Sadu. Diplomski rad na Fakultetu tehničkih nauka u Novom Sadu odbranio je 2022. godine.

kontakt: me@dovla.rs

Зборник радова Факултета техничких наука, НовиСад

УДК: 621.39
ДОИ: https://doi.org/10.24867/34BE31Stanisic

Дизајн протокола за масиван случајан приступ који користе сукцесивно поништавање интерференције

Design of protocols for massive random access which use successive interference cancellation

Теодора Станишић, *Факултет техничких наука, Нови Сад*

Студијски програм – ЕНЕРГЕТИКА, ЕЛЕКТРОНИКА И ТЕЛЕКОМУНИКАЦИЈЕ

Кратак садржај – *У раду су проучене модерне технике приступа мрежи у системима са великим бројем уређаја који на случајан и непредвидив начин приступају мрежи Интернета ствари. Посебан акценат је стављен на алгоритме случајног приступа мрежи базираним на сукцесивном поништавању интерференције, укључујући и њихову теоријску асимптотску анализу и методе за оптимизацију перформанси.*
Кључне речи: *Бежичне комуникације, Интернет ствари, сукцесивно поништавање интерференције, случајан приступ, IRSA*

Abstract – *The paper studies modern network access techniques in systems with a large number of devices that access the Internet of Things network in a random and unpredictable manner. Special emphasis is given to random network access algorithms based on successive interference cancellation, including their theoretical asymptotic analysis and performance optimization methods.*

Keywords: *Wireless Communication, Internet of Things, Successive Interference Cancellation, Random Access, IRSA*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дејан Вукобратовић, ред. проф.

1. УВОД

Са порастом интернета ствари (IoT - Internet of Things) и масивних машинских комуникација (mMTC - massive Machine-Type Communication), број уређаја који има потребу да шаље податке се драстично повећава. Како би сви корисници успешно обавили комуникацију, постоје протоколи за случајан приступ (RA - Random Access) дељеном медијуму. Због тога је потребно да ови протоколи буду ефикасни, да имају велики проток, мало кашњење и малу могућност губитка пакета.

У овом раду су истражени протоколи за случајан приступ који примењују принцип сукцесивног поништавања интерференције (SIC - Successive Interference Cancellation). Овај принцип омогућава разрешавање судара под одређеним условима. Извршена је теоријска анализа, као и симулација ових протокола и упоређене су њихове перформансе.

2. ПРОТОКОЛИ ЗАСНОВАНИ НА SIC ПРИНЦИПУ

Класични протоколи, попут Aloha и Slotted Aloha (SA), посматрају судар као искључиво лошу појаву, односно пакете преношене у слоту где се десила колизија сматрају неповратно изгубљеним. Новије гледиште претпоставља да се пакети из слота у којем је настао судар ипак могу повратити. Идеја је да се реплике које су успешно примљене (нпр. у слотовима без судара) уклоне из слотова који садрже колизију и да се тако открију нови успешно примљени пакети. Овај процес се примењује итеративно, односно сукцесивно [1].

Contention Resolution Diversity Slotted Aloha (CRDSA) је протокол који користи овај принцип. Он подразумева да сваки корисник емитује тачно две копије свог пакета, при чему сваки пакет садржи показивач на слот у којем је послата друга копија. Уколико се детектује слот са само једним пакетом, тај показивач се користи да се уклони интерференција коју друга реплика изазива у другом слоту [2, 3].

Irregular Repetition Slotted Aloha (IRSA) представља уопштење CRDSA протокола. Уместо да шаље тачно две копије, сваки корисник бира случајан број понављања l из неке унапред одређене фиксне расподеле вероватноће. Оптимизација ове расподеле представља кључан проблем у дизајну IRSA протокола. Корисник затим шаље тих l реплика у l различитих, насумично и униформно изабраних слотова унутар фрејма [2].

3. ОСНОВНИ ПРИНЦИПИ SIC ПРОТОКОЛА

3.1. Објашњење система

Посматра се систем где m корисника жели да комуницира са заједничким пријемником (базном станицом). Комуникација се одвија у фрејмовима, где је сваки фрејм састављен од n слотова. Пренос једног пакета одвија се у тачно једном слоту.

Нормализовани понуђени саобраћај (G) представља просечан број преноса пакета по слоту, и дат је као

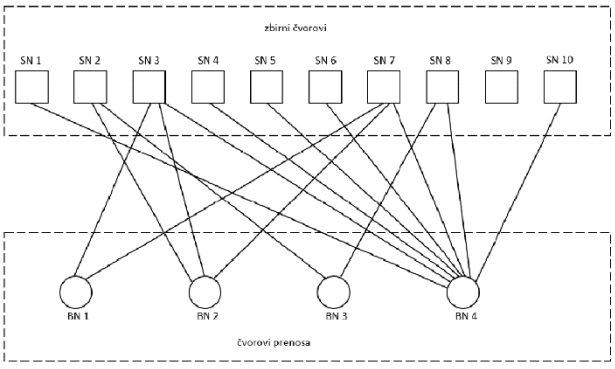
$G = m / n$. Нормализовани проток (T) дефинише се као вероватноћа успешног преноса пакета по слоту [2].
Код класичног Slotted Aloha протокола, проток се може изразити као $T(G) = Ge^{-G}$, што даје максимални проток од $T = 1 / e \approx 0.37$ при $G = 1$ [4].
Протоколи базирани на SIC принципу теже да превазиђу ово ограничење.

3.2. SIC Алгоритам

Сваки пакет који се шаље садржи показиваче на позиције осталих реплика у фрејму које је тај исти корисник послао [1, 2].
Алгоритам за сукцесивно поништавање интерференције се одвија итеративно у два корака. Први корак је декодовање, где пријемник тражи слотове у којима се десио само један пренос пакета (тзв. "singleton" слотови), због чега се поруке из тих слотова успешно декодују. Други корак је поништавање, у којем из сваке успешно декодоване поруке пријемник извлачи показиваче на остале слотове где су реплике те поруке пренете, а затим се допринос (интерференција) тих реплика одузима из одговарајућих слотова.
Ова два корака се понављају. Уклањањем интерференције у другом кораку, неки слотови који су претходно имали колизију (нпр. два пакета) могу постати "singleton" слотови (јер је један од пакета уклоњен), омогућавајући тако даље декодовање у наредној итерацији [2].

4. ГРАФИЧКО ПРЕДСТАВЉАЊЕ И АНАЛОГИЈА

Процес сукцесивног поништавања интерференције се може веома погодно графички представити помоћу бипартитног графа. Овај граф се састоји од: m чворова преноса (BN - Burst Nodes, где сваки представља једног корисника, односно његов пакет) и n збирних чворова (SN - Sum Nodes, где сваки представља један временски слот у фрејму).
Грана повезује i-ти чвор преноса (BN) и j-ти збирни чвор (SN) ако и само ако је корисник i послао реплику свог пакета у слоту j.
Пример бипартитног графа је приказан на Слици 1, где квадрати представљају збирне чворове, а кругови чворове преноса.



Слика 1. Пример бипартитног графа

Ово графичко представљање омогућава успостављање директне везе између процеса SIC и итеративног декодовања заштитних кодова заснованих на ретким графовима, конкретно LDPC (Low-Density Parity-Check) кодова [1].
Процес SIC се може посматрати као итеративни "слојевити" (peeling) декодер. Пронађу се сви збирни чворови (слотови) који имају степен један (тј. садрже само једну реплику). Ти пакети се сматрају успешно декодованим. Одговарајући чворови преноса (корисници) мењају статус у "познат". Уклоне се све гране повезане са тим, сада познатим, чворовима преноса. Ово симулира одузимање њиховог доприноса (интерференције) из других слотова. Након уклањања грана, поново се рачунају степени збирних чворова. Неки други збирни чворови могу постати степена један, па се процес понавља итеративно [1, 2].
Аналогија са LDPC кодовима омогућава употребу техника из теорије кодовања за пројектовање оптималне расподеле вероватноће $\Lambda(x)$ којом корисници бирају свој број понављања, како би се генерисали графови на којима је овај алгоритам успешан са великом вероватноћом [1].

5. АНАЛИЗА АСИМПТОТСКОГ СЛУЧАЈА

Да би се пронашле оптималне расподеле $\Lambda(x)$, користи се анализа асимптотског случаја. Овај случај се дефинише посматрањем система где број корисника m и број слотова n теже бесконачности, али под условом да њихов однос, понуђени саобраћај $G = m / n$, остане константан [5].
Ова претпоставка ($n \to \infty$) омогућава да се граф сматра ретким и без петљи, што значајно поједностављује математичку анализу понашања итеративног декодера. Понашање система се тада може описати техником познатом као "праћење густине" (density evolution).
Уводе се две кључне вероватноће у i-тој итерацији. Са q_i се означава вероватноћа да је грана "непозната", посматрано из перспективе чвора преноса (BN). Вероватноћа p_i означава да је грана "непозната", посматрано из перспективе збирног чвора (SN).
Ове вероватноће се могу изразити рекурзивно једна преко друге, користећи полиномске репрезентације расподела степена грана $\lambda(x)$ и $\rho(x)$. Коначне једначине су дате помоћу (1) и (2)

$$q_i = \lambda(p_{i-1}) \quad (1)$$

$$p_i = 1 - \rho(1 - q_i) \quad (2)$$

Кључни део анализе је што, за разлику од $\lambda(x)$ (који дефинише дизајнер система), $\rho(x)$ (расподела из перспективе слотова) није директно контролисана. Међутим, у асимптотском случају, може се показати да расподела броја пакета у слоту прати Поасонову расподелу. Ово омогућава извођење тачног облика за $\rho(x)$ који зависи само од G и просечне стопе понављања $\Lambda'(1)$ дато у (3):

$$\rho(x) = e^{-G\Lambda'(1)(1-x)} \quad (3)$$

Циљ је пронаћи расподелу $\Lambda(x)$ (а тиме и $\lambda(x)$) која максимизује праг саобраћаја G^*. Ово је максимална вредност G за коју итеративни декодер успешно декодује све пакете (тј. вероватноћа грешке тежи нули). Праг се одређује као максимално G такво да важи $q > \lambda(1 - e^{-G\Lambda'(1)q})$, за свако $q \in (0, 1]$ [2].

6. ОПТИМИЗАЦИЈА РАСПОДЕЛЕ СТЕПЕНА

Анализа асимптотског случаја пружа директан алат за оптимизацију. Циљ је пронаћи оптималну расподелу степена чворова преноса Λ (x) као и максимално могуће оптерећење G (праг G^*) тако да SIC протокол може успешно да декодује све пакете.

Ово се своди на решавање проблема нелинеарне оптимизације. Формално, проблем се дефинише као:

$$\begin{gathered} \max G \\ \text{tako da} \sum \Lambda_l = 1 \\ \Lambda_l \geq 0 \\ \Lambda_1 = 0 \\ q > \lambda\left(1 - \rho\left(1 - q\right)\right), \forall q \in (0, 1] \end{gathered} \tag{4}$$

Прва два ограничења у (4) произилазе из чињенице да расподела Λ (x) мора бити валидна расподела вероватноће. Треће ограничење постоји зато што чворови преноса степена један не доприносе SIC процесу, јер немају друге реплике којима би поништили интерференцију у другим слотовима. Последње ограничење је услов стабилности из асимптотске анализе који гарантује успешно декодовање.

Решавањем овог оптимизационог проблема добијају се оптималне Λ (x) расподеле за различите максималне дозвољене стопе понављања ($l_{\max}$).

Резултати оптимизације су приказани у Табели 1.

Табела 1. Оптималне расподеле и прагови саобраћаја за различите максималне стопе понављања

$l_{\max}$	Оптимална расподела Λ (x)	G^*
4	$0.5144x^2 + 0.4856x^4$	0.868
5	$0.5572x^2 + 0.0582x^3 + 0.3846x^5$	0.897
6	$0.5463x^2 + 0.1682x^3 + 0.2855x^6$	0.915
8	$0.5098x^2 + 0.2698x^3 + 0.2204x^8$	0.941
10	$0.4867x^2 + 0.2706x^3 + 0.0639x^4 + 0.1788x^{10}$	0.953
12	$0.5202x^2 + 0.127x^3 + 0.2094x^4 + 0.1434x^{12}$	0.961
14	$0.5173x^2 + 0.1463x^3 + 0.1199x^4 + 0.0956x^5 + 0.121x^{14}$	0.967
16	$0.5145x^2 + 0.1822x^3 + 0.1983x^5 + 0.1051x^{16}$	0.971

Ова анализа показује да се коришћењем нерегуларних расподела (IRSA) могу постићи значајно виши прагови од регуларних (CRDSA).

На пример, за максималну стопу понављања $l_{\max} = 4$, оптимална IRSA расподела ($\Lambda(x) = 0.5144x^2 + 0.4856x^4$) постиже праг саобраћаја $G^* = 0.868$. Ради поређења, 4-регуларна CRDSA расподела (где сви корисници шаљу тачно 4 реплике) има значајно нижи праг од $G^* = 0.772$. Дакле, асимптотски, IRSA омогућава повећање протока за приближно 12.44% у односу на CRDSA, користећи исти максимални број реплика.

Слично, за $l_{\max} = 5$, оптимизована IRSA расподела ($G^* = 0.897$) постиже повећање протока од скоро 28% у односу на 5-регуларну CRDSA расподелу ($G^* = 0.701$) [2].

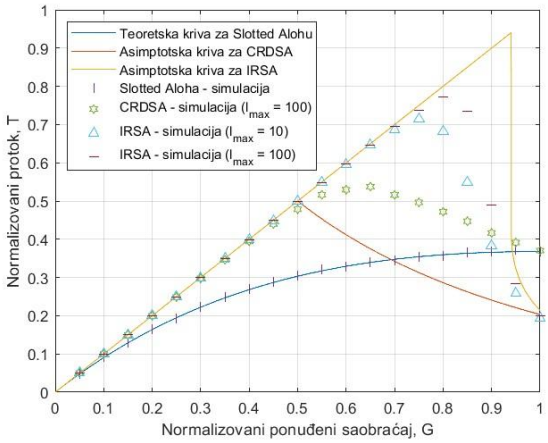
Ови асимптотски резултати служе као основа за дизајн протокола који се затим тестирају у симулацијама са коначном дужином фрејма.

7. АНАЛИЗА РЕЗУЛТАТА СИМУЛАЦИЈА

Да би се потврдиле перформансе у реалнијем окружењу (са коначним бројем слотова), извршене су Монте Карло симулације које се баве искључиво MAC слојем. Посматрана је фиксна величина фрејма од $n = 200$ слотова. За IRSA алгоритам коришћена је оптимална расподела степена из Табеле 1 са максималном стопом понављања 8.

7.1. Поређење протока

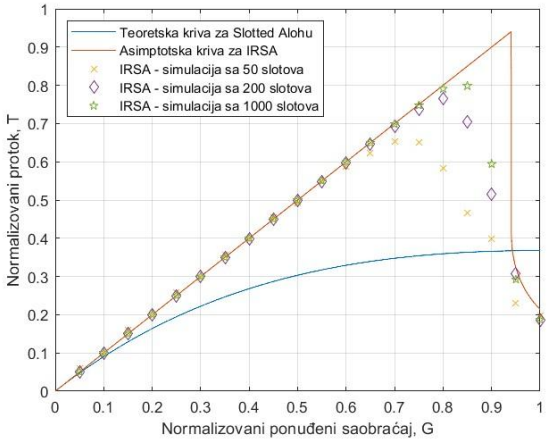
На Слици 2. приказане су криве протока за SA, CRDSA и IRSA, у поређењу са теоријским и асимптотским кривама.



Слика 2. Проток различитих алгоритама

Као што се види, класични Slotted Aloha (SA) протокол има максимални проток од $T \approx 0.37$. CRDSA протокол (са 2 понављања, симулација са $I_{\max}$=100) постиже знатно виши проток, $T \approx 0.55$. Међутим, IRSA протокол са оптималном расподелом и истим бројем итерација постиже проток близу $T \approx 0.78$. Чак и са ограничењем броја итерација на 10 (због мање сложености), IRSA и даље постиже проток већи од 0.7.

На Слици 3. су приказане перформансе IRSA са максималним бројем итерација постављеним на вредност 20 за различите величине фрејмова.



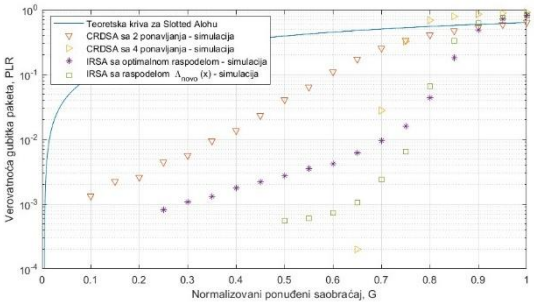
Слика 3. Проток са различитим бројем слотова у фрејму

Повећањем величине фрејма перформансе симулације IRSA се приближавају теоријском асимптотском

прагу, што потврђује исправност модела. На пример, за вредност саобраћаја G = 0.8, фрејм са 50 слотова постиже проток мало мањи од 0.6, фрејм који садржи 200 слотова успева да досегне вредност протока од скоро 0.77, док кад је у питању фрејм од 1000 слотова, проток износи чак приближно 0.8.

7.2. Поређење вероватноће губитка пакета (PLR)

Још битнија метрика за многе IoT апликације је вероватноћа губитка пакета (PLR - Packet Loss Ratio). На Слици 4. упоређене су PLR вредности за SA, CRDSA (са 2 и 4 понављања) и IRSA шеме, за n = 200 слотова и I_{max} = 20.



Слика 4. Вероватноћа губитка пакета различитих алгоритама (n = 200, Imax = 20)

Да би се постигао циљани PLR од 10^{-2}, SA мора да ради при веома ниском саобраћају од $G \approx 0.01$. CRDSA са 2 понављања показује знатно побољшање и може да подржи саобраћај $G \approx 0.35$. IRSA шема са оптималном расподелом постиже исти PLR (10^{-2}) при саобраћају од $G \approx 0.7$, што представља двоструко већу вредност у односу на CRDSA. Ово показује драматично побољшање у ефикасности искоришћења канала.

8. ЗАКЉУЧАК

Примена масивног случајног приступа је изузетно значајна код масивних машинских комуникација и интернета ствари. Кључно је да протоколи који имплементирају ову функцију имају добре перформансе, као што су велики проток и мала вероватноћа губитка пакета.

У овом раду су анализирани протоколи који користе принцип временског сукцесивног поништавања интерференције. Урађена је детаљна теоријска анализа помоћу графичке представе и асимптотске анализе и оптимизације. Затим су извршене и симулације за фрејмове коначне дужине. Показано је да ови протоколи (посебно IRSA са оптимизованом расподелом) постижу значајно боље резултате и много већу ефикасност канала од класичних протокола за случајан приступ као што је Slotted Aloha.

9. ЛИТЕРАТУРА

[1] E. Paolini, C. Stefanovic, G. Liva, and P. Popovski, “Coded random access: applying codes on graphs to design random access protocols,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 144–150, Jun. 2015.

[2] G. Liva, "Graph-based analysis and optimization of contention resolution diversity slotted ALOHA," *IEEE Transactions on Communications*, vol. 59, no. 2, pp. 477–487, Feb. 2010.

[3] E. Casini, R. De Gaudenzi, and O. Del Rio Herrero, "Contention resolution diversity slotted ALOHA (CRDSA): An enhanced random access scheme for satellite access packet networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 4, pp. 1408–1419, Apr. 2007.

[4] N. Abramson, "The throughput of packet broadcasting channels," *IEEE Transactions on Communications*, vol. 25, no. 1, pp. 117–128, Jan. 1977.

[5] D. Jakovetić, D. Bajović, D. Vukobratović, and V. Crnojević, "Cooperative slotted aloha for multi-base station systems," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1443–1456, Apr. 2015.

Кратка биографија:

Теодора Станишић рођена је у Новом Саду 2002. год. Дипломски рад на Факултету техничких наука одбранила је 2024.год. из области Информационо-комуникационе технологије. Од 2025. год. је запослена у звању сарадника у настави, на Катедри за телекомуникације и обраду сигнала, Департман за енергетику, електронику и телекомуникације.
Контакт:
dodastanisic@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.9
ДОИ: https://doi.org/10.24867/34BE32Kacanski

Анализа и имплементација Тендерминт консензус алгоритма и његових варијација

Analysis and Implementation of the Tendermint Consensus Algorithm and Its Variations

Данило Кањански, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *Овај рад се бави анализом и имплементацијом Тендерминт консензус алгоритма и његових варијација, које су настале као његове надоградње. У првом делу рада описане су теоријске основе, механизам постизања консензуса и варијације Тендерминта, док се други део рада односи на његову експерименталну симулацију. Добијени резултати показују да Тендерминт задржава кључне особине чак и у присуству византијских валидатора, чиме се потврђује примењивост у савременим blockchain системима.*

Кључне речи (три до пет): *Тендерминт консензус, Византијска толеранција на грешке, Дистрибуирани системи, Blockchain*

Abstract – *This paper focuses on the analysis and implementation of the Tendermint consensus algorithm and its variations, which have emerged as extensions of it. The first part of the paper describes the theoretical foundations, the mechanism of achieving consensus, and the variations of Tendermint, while the second part is dedicated to its experimental simulation. The obtained results demonstrate that Tendermint preserves its key properties even in the presence of the Byzantine validators, thereby confirming its applicability in modern blockchain systems.*

Keywords: (three to five): *Tendermint consensus, Byzantine fault tolerance, Distributed systems, Blockchain*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дарко Чапко, ред. проф.

1. УВОД

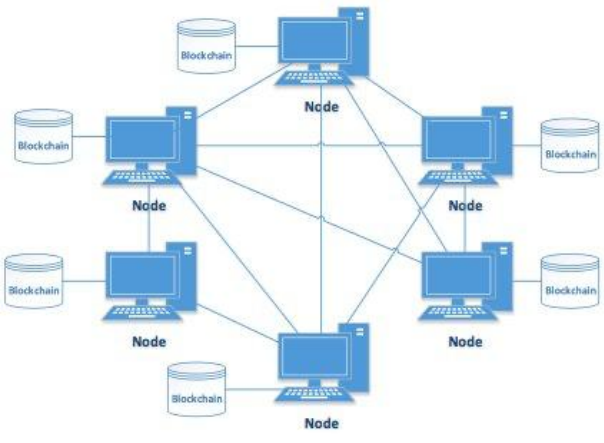
Постизање договора око неке вредности је одувек био један од **главних проблема у дистрибуираним системима**. Развитком технологије и настанком *blockchain* система, овај проблем добија још једну димензију. Сада је број валидатора за неколико реда величина већи, не припадају истом административном домену и прети опасност од злонамерних (византијских). Алгоритми који су се претходно користили, као што су *Paxos* и *Raft*, нису више примењиви због ових нових проблема који доносе *blockchain* системи. Управо из тог разлога су развијени *BFT (Byzantine Fault Tolerant)* алгоритми који омогућавају консензус, чак и када се део валидатора понаша злонамерно [6].

Једно од најпознатијих *BFT* решења је **Тендерминт**, алгоритам који започиње предлогом за додавање блока од стране лидера, и наставља се гласањем кроз даље фазе. За разлику од осталих приступа, Тендерминт омогућава додавање валидних блокова са високом отпорношћу на византијске валидаторе. Његова једноставност и могућност примене у *Proof-of-Stake* системима учинили су га **основом за велики број модерних *blockchain* мрежа** [1].

Осим **анализе** и **имплементације Тендерминт консензус алгоритма**, дат је и **преглед његових варијација**, које су настале ради превазиласка неких од његових недостатака [5,7,8]. Помоћу експерименталне симулације која је имплементирана, могуће је испитивање најважнијих особина Тендерминта и његово тестирање под различитим комбинацијама параметара мреже и валидатора.

2. ТЕНДЕРМИНТ АЛГОРИТАМ

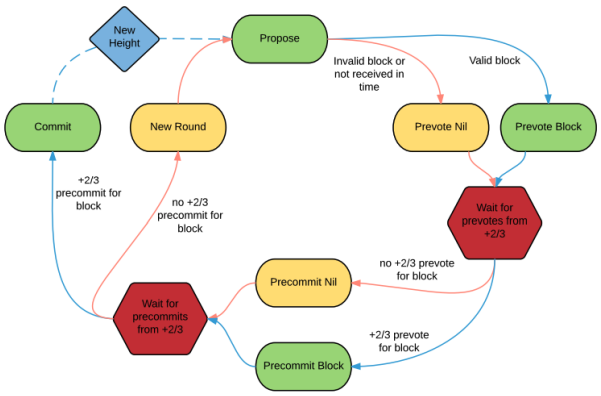
Тендерминт је дизајниран тако да обезбеди **детерминистичку финалност** блока, другим речима једном када је блок прихваћен, он више не може бити опозван [1].



Слика 1. Мрежа валидатора у *blockchain* систему [2]

Структуриран је тако да се на свакој висини, по потреби понавља кроз рунде. У свакој рунди бира се један лидер који предлаже нови блок, док остали валидатори гласају у више фаза како би одредили да ли ће предлог бити прихваћен.
Основне фазе Тендерминта су:

Propose → Prevote → Precommit → Commit → NewHeight



Слика 2. Главне фазе Тендерминт консензуса [4]

У случају да у некој рунди не дође до прихватања блока (на пример због кашњења порука или неактивног лидера), покреће се нова рунда са новим лидером. Оваква структура алгоритма гарантује прогресивност, јер се рунде настављају све док се не постигне консензус.
У фази *Propose*, лидер предлаже нови блок, који садржи скуп трансакција и хеш претходног блока. Током *Prevote* фазе сваки валидатор гласа за предложени блок или за *nil* (уколико га сматра неважећим).
Ако се више од две трећине валидатора сложи око истог блока, систем прелази у наредну фазу *Precommit,* у којој се гласови потврђују и валидатори закључавају на ту вредност.
Када више од две трећине валидатора пошаље *precommit* за исти блок, он се сматра потврђеним (*Commit*) и додаје у *blockchain.*
Да би све ово постигао, Тендерминт користи систем тајмера који спречава да било која од наведених фаза траје неограничено. Уколико време истекне, чворови прелазе у нову рунду, тајмер се експоненцијално увећава, чиме се гарантује прогресивност и финалност у неком тренутку, чак и у делимично синхроним условима.

3. БЕЗБЕДНОСТ и ПРОГРЕСИВНОСТ

Најважнија карактеристика Тендерминта јесте његова гаранција **безбедности** (*safety*) и **прогресивности** (*liveness*) [1]. Безбедност значи да ниједна два исправна чвора неће потврдити различите блокове на истој висини, док прогресивност осигурава да ће систем, без обзира на застоје и губитке порука, пре или касније доћи до консензуса.
Механизам који омогућава ове две особине је **закључавање блокова**. Када валидатор током *Precommit* фазе пошаље глас за неки блок, он се онда закључава на исти, и не може да подржи ниједан други на истој висини док не добије потврду да је систем напредовао. На овај начин се спречава појава конфликтних потврда и одржава конзистентност *blockchain*-а.
Детаљније, да би се прогресивност обезбедила, сваки валидатор има локалне промењиве *validRound* и *validValue*, у којима се чува последња рунда и вредност за коју је добијена двотрећинска већина у *Prevote* фази. Лидер ове информације користи у наредним рундама како би предложио блок са којим је задовољна већина валидатора без додатног гласања. Због тога се знатно смањује стагнација, и систем напредује чак и у делимично синхроном окружењу.
Да би се решио случај када нека фаза траје предуго, уводи се **систем тајмера** (*timeoutPropose, timeoutPrevote, timeoutPrecommit*). Време трајања се увећава експоненцијално, тако да и у случају да поруке касне пуно, консензус се постиже по истеку времена стабилизације мреже.
Тендерминт помоћу овакве структуре осигурава да се може донети само једна одлука, и да се процес не може трајно зауставити, а управо тиме истовремено гарантује и безбедност и прогресивност.

4. ВАРИЈАЦИЈЕ И НАДОГРАДЊЕ ТЕНДЕРМИНТА

Развој Тендерминта је подстакао настанак више варијанти и надоградњи које су имале за циљ да побољшају његове различите аспекте. У почетним фазама развоја, **фокус** је био на **формалним доказима исправности** Тендерминта, као што је приказано у раду *Correctness of Tendermint-Core Blockchains* [6], док су каснији радови попут *Lock-free Enhanced Tendermint* [7], *Tenderbake* [5] и *TenderTee* [8] направили **конкретна** и **практична побољшања**.
Ове три варијације у већој или мањој мери модификују Тендерминт, уводећи нове механизме за избор валидатора, убрзавање консензуса и повећање безбедности, тако да ће у наставку бити нешто више речи о њима.

4.1. LOCK-FREE ENHANCED TENDERMINT

Прва модификација, представљена у раду *Fair and Trustworthy: Lock-free Enhanced Tendermint Blockchain Algorithm* [7], се односи на низ побољшања усмерених ка **пропусности** система и **избегавања застоја** у комуникацији.
Најважнија модификација је увођење *lock-free* приступа, чиме се уклања закључавање током фаза гласања. Као што је већ напоменуто, у Тендерминту се валидатори закључавају на вредност блока, док се у овој верзији фазе гласања извршавају паралелно, док се само *Commit* фаза извршава секвенцијално. Овим приступом се смањује време потребно за достизање консензуса, и постиже се линеаризабилност, тј. особина да су резултати добијени конкурентним извршавањем програма идентични као и код секвенцијалног извршавања.
Друга иновација се односи на **динамичко одређивање скупа валидатор**а, али тако да се број валидатора подешава помоћу нивоа поузданости и осетљивости података. У случају да је поверење у мрежи високо

мањи број валидатора је довољан, док се у критичним ситуацијама користи већи скуп валидатора.
Наредно побољшање је **фер избор валидатора** помоћу стохастичког алгоритма *random walk*, којим се смањује вероватноћа пристрасности и повећава униформност добијања награда.
За крај, последња модификација ове варијације је *wait-freedom* механизам. Он након истека дефинисаног времена, све поруке које нису пристигле третира као *nil* гласове. Због тога се консензус увек завршава у коначном времену, чиме се постиже још већи степен прогресивности.

4.2. TENDERBAKE

Наредна варијација је *Tenderbake*, који се не бави само формалном теоријом, већ проналази и своју **примену** и *Tezos blockchain*-у [5].
Он уводи концепт **динамичког поновљеног консензуса** (*Dynamic Repeated Consensus - DRC*), где се састав валидатора може мењати кроз сваку рунду, али не као у претходној верзији кроз подскупове, већ додавањем и уклањањем валидатора, који су купили и продали токен задужен за расподелу гласачке снаге. Како аутори рада наводе основна својства која сваки *DRC* мора задовољити (*Agreement*, *Validity* и Progress) обезбеђују да се све одлуке доносе конзистентно и да *blockchain* расте континуирано.
Друга модификације је увођење *best-effort broadcast*-а, помоћу ког се елиминише потреба за поузданим слањем порука. Овако се толерише губитак порука без утицаја на сигурност система, а истовремено се и мрежно оптерећење значајно смањује.
Трећа иновација је употреба **кворум сертификата** (*Quorum Certificates - QC*) који представљају агрегиране криптографске потписе валидатора. Захваљујући њима, *Tenderbake* постиже консензус у највише $f + 2$ рунде (где је f број византијских валидатора), што је велико побољшање у односу на Тендерминт где је таква гаранција била могућа тек у случају када се прођу сви валидатори.
Захваљујући овим изменама, *Tenderbake* доноси брже и ефикасније доношење одлука у делимично синхроном окружењу и као што је већ наведено успешно је интегрисан у *Tezos blockchain*, што потврђује његову примену у пракси.

4.3. TENDERTEE

Последња обрађена варијација јесте *TenderTee*, и усмерена је ка **повећању безбедности** и **отпорности** на византијске валидаторе [8]. За разлику од претходних приступа који су имали друге предмете оптимизације, *TenderTee* **помера границу толеранције** на византијске валидаторе са $f < \frac{n}{3}$ на $f < \frac{n}{2}$, што представља значајан корак у детерминистичким *PBFT* протоколима.
Ово је постигнуто увођењем **хардверске компоненте** *Attested Append-Only Memory (A2M)*, која гарантује да ће свака порука бити јединствено забележена и непромењива. Такође изразито битна ствар је то што *A2M* гарантује да валидатор не може послати две различите поруке у истој рунди, чиме се елиминише најгора верзија византијског понашања *equivocation*.
Сем тога, свака порука садржи и **дигиталан потпис**, који је заснован на систему јавних кључева, што омогућава да се сваки корак консензуса криптографски провери. На овај начин уз помоћ *A2M* се ствара **двострука заштита**, комбинацијом хардверског и софтверског слоја.
За крај, *TenderTee* даје и формално дефинисање **поновљеног консензуса**, који осигурава да ће сви исправни валидатори имати идентичан *blockchain* и након произвољно великог броја итерација, за разлику од осталих приступа који су помоћу индукције гарантовали ову особину. На овај начин се обезбеђује детерминистичка финалност и непромењивост одлуке, што је кључно за примену у реалним *blockchain* системима.

4.4. ЗАКЉУЧАК

Приказане варијације показују **континуирану еволуцију Тендерминта**, бавећи се унапређивањем његових различитих карактеристика. *Lock-free Enhanced Tendermint* [5] повећава ефикасност и флексибилност, *Tenderbake* [7] формализује динамички консензус и смањује број потребних рунди, док *TenderTee* [8] проширује границе безбедности и уводи хардверску заштиту од византијског понашања.
Све три варијације имају исту суштину, а свака уноси додатни степен сигурности, скалабилности или правичности, што чини Тендерминт темељем савремених *PBFT* протокола који се налазе иза модерних *Proof-of-Stake* система.

5. ИМПЛЕМЕНТАЦИЈА

Имплементација је реализована у програмском језику **Go**, због изразите подршке за конкурентно програмирање и једноставног управљања асинхроним догађајима у мрежи. Главни циљ имплементације је био да се изгради симулација која представља експериментално окружење у којем се може испитати понашање Тендерминта у различитим мрежним и византијским условима [1]. Систем је подељен на три нивоа: **консензус језгро**, **мрежни слој** и **конфигурациони интерфејс**.
Консензус језгро симулира све фазе алгоритма (*Propose*, *Prevote*, *Precommit* и *Commit*) и прати кључне промењиве као што су *lockedValue*, *lockedRound*, *validValue* и *ValidRound* које служе да би се обезбедила безбедност и прогресивност консензуса. Лидер се бира насумично, пропорционално гласачкој снази, док се процес гласања одвија кроз рунде са временским ограничењима. Уколико дође до истека времена, помоћу система тајмера, рунда се аутоматски понавља са новим лидером, без чега не би било могуће гарантовати завршетак алгоритма, тј. прогресивност.
Мрежни слој је заснован на *in-memory gossip* протоколу који омогућава симулацију реалних услова у мрежи, укључујући кашњења, губитке порука и насумичне поремећаје (*jitter*). Сваки валидатор спроводи комуникацију преко посебних канала, а поруке бивају потписане и верификоване од стране *Ed25519* алгоритма. Поред стандардних подешавања мрежа подржава моделовање различитих врста византијског понашања као што су ћутање, намерно

гласање за *nil* или слање контрадикторних порука. На овај начин могуће је тестирање свих особина протокола, под свим могућим условима.
На највишем нивоу се налази **конфигурациони слој**, који омогућава покретање једне или више симулација са различитим параметрима. Корисник може дефинисати број валидатора, расподелу гласачке снаге, понашање сваког од њих, топологију мреже, трајање свих кључних промењивих, итд. Резултати се аутоматски чувају у *.csv* форматима и садрже све кључне метрике потребне за даљу анализу.
Додатно, реализовани су различити **тестни сценарији**, чију израду и интеграцију пружа језик *Go*. Окружење је дефинисано тако да испитује кључне особине Тендерминта и његову исправност у различитим условима. Тестови се извршавају без кашњења и насумичних одступања, да би се обезбедило њихово детерминистичко извршавање. У оквиру тестног модула се испитују случајеви као што су постизање консензуса уз присуство византијских валидатора, прекид рада симулације у случају прекорачења прага броја византијских валидатора (преузето из практичних решења) и стабилност у случају ограничене комуникације. Овакав модул за тестирање омогућава брзу проверу исправности протокола и његових особина, као и лако проширење новим тестовима. Захваљујући томе, након сваке веће промене симулатора, може се лако написати нови тестни случај, и на брз и коректан начин проверити исправност Тендерминта са новим проширењима.

6. ЗАКЉУЧАК

Рад је представио **теоријску анализу Тендерминта** [1], **његове варијације** и **практичну имплементацију**, који данас чини основу за велики број *Proof-of-Stake blockchain*-ова. Нагласак овог рада јесте на повезивању теоријских принципа са практичним механизмима примене, како би се истакла практична вредност Тендерминта у реалним условима имплементације децентрализованих мрежа, које захтевају висок ниво поузданости. Кроз приказ основног алгоритма и његових варијација (*Lock-Free Enhanced Tendermint*, *Tenderbake* и *TenderTee* [5, 7, 8]), показано је како се исти концепт развијао од почетног *PBFT* решења, до напредних система који обезбеђују већу ефикасност, флексибилност и отпорност на византијске валидаторе.
Развијена имплементација доказује да је могуће детерминистички и експериментално утврдити понашање Тендерминта у контролисаном окружењу, као и пратити утицај свих подесивих хиперпараметара мреже и валидатора. На основу симулација је потврђено да Тендерминт задржава своје кључне особине, безбедност и прогресивност, чак и у граничним случајевима што се тиче броја византијских валидатора и непропусности мреже.
Симулатор представља **добру основу** за даљу **квантитативну анализу** Тендерминта и **његова проширења**. Проширења која се природно настављају на већ имплементиран алгоритам јесу увођење реалног *ABCI* слоја, динамички избор валидатора и права *P2P* комуникација. Након тога би такође било занимљиво пробати неке од техника које варијације Тендерминта користе.
Овим рад заокружује целу причу око развоја и практичне примене Тендерминт консензус алгоритма, који је један од најзначајнијих ослонаца модерних *PBFT blockchain* система.

7. ЛИТЕРАТУРА

[1] Buchman, Ethan, Jae Kwon, and Zarko Milosevic. "*The latest gossip on BFT consensus.*" arXiv preprint arXiv:1807.04938 (2018).

[2] Koteska, Bojana, Elena Karafiloski, and Anastas Mishev. "*Blockchain implementation quality challenges: a literature*." In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications, vol. 11, p. 2017. 2017.

[3] Bounceur, Ahcène, Ahmed-Sami Berkani, Hamouma Moumen, and Saber Benharzallah. "*The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms.*" IEEE Access (2025).

[4] Lagaillardie, Nicolas, Mohamed Aimen Djari, and Önder Gürcan. "*A computational study on fairness of the tendermint blockchain protocol."* Information 10, no. 12 (2019): 378.

[5] Aştefanoaei, Lăcrămioara, Pierre Chambart, Antonella Del Pozzo, Thibault Rieutord, Sara Tucci, and Eugen Zălinescu. "*Tenderbake--A Solution to Dynamic Repeated Consensus for Blockchains.*" arXiv preprint arXiv:2001.11965 (2020).

[6] Amoussou-Guenou, Yackolley, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni. "*Correctness of tendermint-core blockchains.*" In 22nd International Conference on Principles of Distributed Systems (OPODIS 2018), pp. 16-1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2019.

[7] Assiri, Basem, and Wazir Zada Khan. "*Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm.*" TELKOMNIKA (Telecommunication Computing Electronics and Control) 18, no. 4 (2020): 2224-2234.

[8] Beltrando, Lionel, Maria Potop-Butucaru, and Jose Alfaro. "*TenderTee: Secure Tendermint.*" Cryptology ePrint Archive (2022).

Кратка биографија:

Данило Кањански рођен је у Новом Саду 2001. год. Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства одбранио је 2025. год.
Контакт: kacanski.ra26.2020@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

УДК: 621.38

ДОИ: https://doi.org/10.24867/34BE34Pajic

ТЕРМИЧКИ АСПЕКТИ СТРУЈНЕ ОПТЕРЕТИВОСТИ ЕЛЕКТРОЕНЕРГЕТСКИХ КАБЛОВА

THERMAL ASPECTS OF THE CURRENT-CARRYING CAPACITY OF POWER CABLES

Милош Пајић, *Факултет техничких наука*, Нови Сад

Студијски програм – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду је приказан прорачун термички трајно дозвољене струје електроенергетских каблова. При томе је анализиран утицај различитих фактора на вредност термички трајно дозвољене струје, међу којима су конструкција и начин полагања каблова, температура и термички отпор земљишта у које се каблови полажу, утицај исушивања земљишта и променљивог дијаграма оптерећења. Добијене вредности термички трајно дозвољене струје су упоређене са вредностима које се користе у домаћој електропривреди.*

Кључне речи: *електроенергетски каблови, термички трајно дозвољена струја, температура земљишта, термички отпор земљишта, променљиви дијаграм оптерећења*

Abstract – *This paper presents calculation of the current-carrying capacity of power cables. Also, it is analyzed how different factors affect the current-carrying capacity of power cables, including construction of the cables, soil temperature, soil thermal resistivity, soil drying and the influence of time-varying load. The results of current-carrying capacity obtained in this paper are compared with the values that are used in power utilities in Serbia.*

Keywords: *power cables, current-carrying capacity, soil temperature, soil thermal resistivity, time-varying load*

1. УВОД

Електроенергетски каблови су кључна компонента система за пренос и дистрибуцију електричне енергије, посебно у урбаним индустријским и просторно ограниченим срединама. Један од најважнијих параметара у њиховој експлоатацији је термички трајно дозвољена струја, односно максимална струја коју кабл може дуготрајно да преноси без прегревања.

Називна струја кабла је она трајна струја која при основној (називној) температури околине и основним условима хлађења, загреје кабл до граничне температуре, односно изазове гранично повишење температуре кабла у односу на околину. Струја којом се може оптеретити кабл тако да, у зависности од тренутних услова, загревање кабла буде максимално, односно повишење температуре кабла у односу на околину буде максимално, јесте термички трајно дозвољена струја кабла.

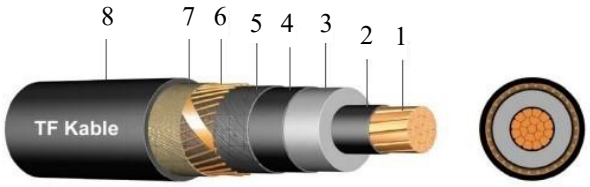
Циљ овог рада је да се, кроз анализу конкретних случајева, прикаже утицај различитих услова на термички дозвољену струју кабла.

НАПОМЕНА:

Овај рад проистекао је из мастер рада чији ментор је био доцент др Невен Ковачки

2. КОНСТРУКЦИЈА ЕЛЕКТРОЕНЕРГЕТСКИХ КАБЛОВА

У овом раду анализира се кабл ознаке XHE 49 1×95/16 mm², 20/35 kV који је приказан на слици 1. XHE 49 је једножилни кабл са бакарним проводником пресека 95 mm² и електричном заштитом пресека 16 mm², која је изведена у виду омота или оплета од бакарних жица и трака. Ознака 49 означава да је електрична заштита постављена око сваке жиле посебно, у виду омота или оплета од металних жица, односно омота од металних трака, као и да кабл поседује заштиту од продора влаге. Напонска ознака 20/35 kV означава да је 20 kV фазни напон, а 35 kV линијски напон између фаза [1].



Слика 1. Конструкција и попречни пресек кабла

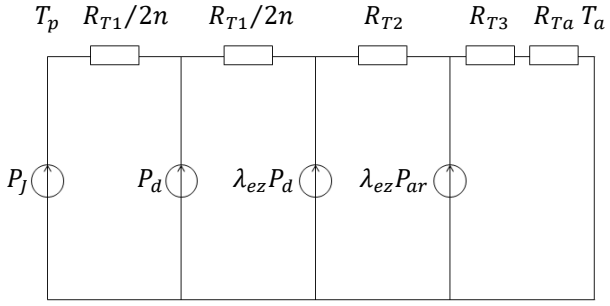
На слици 1 бројевима од 1 до 8 означени су поједини конструктивни елементи кабла [2]:

1) Вишежични проводник израђен од бакра,
2) Екран проводника (слабопроводни слој),
3) Изолација, умрежени полиетилен (XPE),
4) Екран изолације, слабопроводни слој на изолацији. Екрани служе за обликовање електричног поља испуњавањем неравнина између проводника и изолације, односно изолације и електричне заштите
5) Сепаратор, бубрива полуводљива трака. Њихова улога је да спрече продор воде у кабл
6) Електрична заштита – метални екран, бакарне жице и контраспирала од бакарне траке,
7) Сепаратор, бубрива полуводљива трака,

8) Спољашњи плашт од полиетилена (PE).

3. ОСНОВНИ ПРОРАЧУН ТЕРМИЧКИ ТРАЈНО ДОЗВОЉЕНЕ СТРУЈЕ

Прорачун термички трајно дозвољене струје кабла заснива се на еквивалентној шеми на слици 2.



Слика 2. Еквивалентна шема за термички прорачун кабла [3]

У еквивалентној шеми се појављују следеће термичке отпорности:

- Термичка отпорност између проводника и електричне заштите:

$$R_{T1} = \frac{\rho_{tPE}}{2\pi} \cdot \ln\frac{d_i}{d_p} \quad (1)$$

- Термичка отпорност између електричне заштите и кабла:

$$R_{T2} = \frac{\rho_{tPE}}{2\pi} \cdot \ln\frac{d_k}{d_{ez}} \quad (2)$$

- Термичка отпорност омотача механичке заштите:

$$R_{T3} = 0 \quad (3)$$

- Термичка отпорност земље (амбијента):

$$R_{Ta} = R_{Tz} = \frac{\rho_{tz}}{2\pi} \cdot (\ln k + \ln k_a) \quad (4)$$

Геометријски фактори који утичу на термичке отпорности израчунавају се по следећим релацијама:

- Фактор геометрије кабла

$$k = \frac{2h}{d_k} + \sqrt{\left(\frac{2h}{d_k}\right)^2 - 1} \quad (5)$$

- Фактор утицаја суседних каблова

$$k_a = \sqrt{1 + \left(\frac{2h}{a}\right)^2} \quad (6)$$

Температуре потребне за прорачун узимају се као:

- Максимална температура проводника

$$\mathrm{T}_p = \mathrm{T}_{max} = 90^0 C \quad (7)$$

- Температура референтне земље

$$\mathrm{T}_a = \mathrm{T}_0 = 20^0 C \quad (8)$$

Губици у проводнику и електричној заштити дати су изразима:

- Џулови губици

$$P_J = n \cdot R_{90^oC} \cdot I_{max}^2 \quad (9)$$

- Диелектрични губици

$$P_d \approx 0 \quad (10)$$

- Губици у електричној заштити

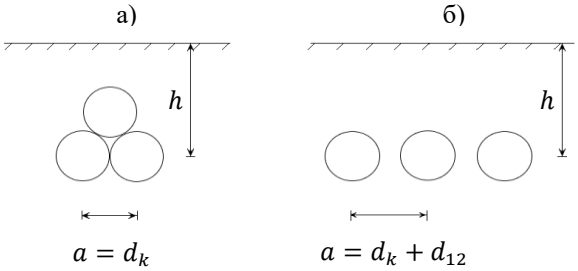
$$P_{ez} = \lambda_{ez} P_J \quad (11)$$

- Губици у механичкој заштити

$$\lambda_{ar} P_J = 0 \quad (12)$$

У наставку су посебно приказани резултати за случајеве када су разматрани једножилни каблови положени у снопу и у равни, како је приказано на слици 3. У горњим релацијама су коришћене следеће вредности [4]:

- ρ_{tPE} – специфична термичка отпорност изолације од умреженог полиетилена $\rho_{tPE} = 3{,}5\ Km/W$,
- ρ_{tz} – специфична термичка отпорност земљишта чија вредност зависи од типа и карактеристика земљишта, неисушено земљиште $\rho_{tz} = 1\,Km/W$, исушено земљиште $\rho_{tiz} = 2{,}5\,Km/W$,
- d_p – пречник проводника,
- d_i – пречник сепаратора преко изолације,
- d_{ez} – пречник електричне заштите,
- d_k – пречник кабла,
- h – дубина полагања кабла,
- a – растојање између оса каблова,
- d_{12} – растојању између суседних каблова када се поставе у равни, $d_{12} = 7\ cm$
- n – број жила проводника,
- R_{90^oC} – електрични отпор проводника при температури од 90°C,
- I_{max} – максимална струја оптерећења кабла,
- λ_{ez} – фактор губитака у електричној заштити, када су три кабла постављена у снопу $\lambda_{ez} = 0{,}0135$, а када постављена у равни $\lambda_{ez} = 0{,}054$



Слика 3. Три једножилна кабла положена у а) снопу; б) равни

3.1. Прорачун за каблове положене у снопу

Уколико се три једножилна кабла полажу у снопу у земљу на дубину 0,7 m применом горе наведених формула добијају се конкретне вредности термичких отпорности:

- $R_{T1} = 0{,}586\,Km/W$
- $R_{T2} = 0{,}092\ Km/W$
- $R_{Tz} = 1{,}8047\,Km/W$

На основу тих вредности, дозвољена струја се рачуна из израза:

$$I_{max} = \sqrt{\frac{T_{max} - T_0}{R_{90^oC} \cdot \left(R_{T1} + R_{T2} + R_{Tz} + \lambda_{ez} \cdot (R_{T2} + R_{Tz})\right)}} \quad (13)$$

Резултат прорачуна:

- $I_{max} = 337\ A$

Према вредностима које се користе у домаћој електропривреди максимално дозвољена трајна струја износи 350 А, што представља одступање од свега 3–4% у односу на прорачунату вредност [5].

3.2. Прорачун за каблове положене у равни

Уколико се три једножилна кабла полажу у равни у земљу на дубину 0,7 m само се вредност термичког отпора земље мења због промене геометрије и она износи:

- $R_{Tz} = 1{,}482\,Km/W$

Рачуном по истој формули добија се:

- $I_{max} = 356{,}23\,A$

У домаћој електропривреди максимално дозвољена трајна струја износи $370\,A$, што такође представља разлику од 3-4%, потврђујући тачност методологије [5]. Каблови у равни, у већем броју случајева, могу се више оптеретити због мањег утицаја загревања међусобно. Ипак, када се каблови полажу у равни, повећава се фактор губитака електричне заштите, што треба узети у обзир.

4. УТИЦАЈ ИСУШИВАЊА ЗЕМЉИШТА

Када је кабл положен у земљу, током експлоатације долази до ослобађања топлоте услед оптерећења. Ова топлота доводи до исушивања околног земљишта, што директно утиче на смањење његове способности одвођења топлоте. Последично, повећава се температура кабла, што захтева смањење струје оптерећења да би температура остала у дозвољеним границама. Због тога је максимално дозвољена струја у исушеном земљишту нижа него у нормалним условима. Термичке отпорности, као и корекциони фактори, рачунају се као у поглављу 3. Отпорност исушеног слоја земљишта добија се следећом релацијом:

$$R_{tiz} = \frac{\rho_{tiz}}{2\pi} \cdot (\ln k + \ln k_a) = \frac{\rho_{tiz}}{\rho_{tz}} \cdot R_{tz} \qquad (14)$$

Пошто важи претпоставка као и у претходном поглављу, да је оптерећење константно, може се узети да је пад температуре у неисушеном слоју земљишта $\triangle\theta_{\mathrm{xz}} = 15^0 C$ [4].

Термички трајно дозвољена струја се рачуна као:

$$I_{max} = \sqrt{\frac{T_{max} - T_0 + \frac{\rho_{tiz} - \rho_{tz}}{\rho_{tz}} \cdot \triangle\theta_{\mathrm{xz}}}{X}} \qquad (15)$$

$$X = R_{90^oC} \cdot \left(R_{T1} + R_{T2} + R_{Tiz} + \lambda_{ez} \cdot (R_{T2} + R_{Tiz})\right)$$

- Фактор геометрије слоја земљишта који се исушује:

$$k_x = \exp\left(\frac{2\pi \cdot \triangle\theta_{xz}}{3 \cdot \rho_{tz} \cdot \mathrm{P}}\right) \qquad (16)$$

Где је:

- Снага губитака у једном каблу $P = R' \cdot \mathrm{I}^2_{\mathrm{max}}$ (17)
- Фиктивна електрична отпорност проводника кабла $R' = R_{90^oC} \cdot (1 + \lambda_{\mathrm{ez}})$ (18)

Након израчунавања струје, проверава се валидност претпоставке о исушености земљишта. Услов који мора бити испуњен је:

$$d_x > 2a \qquad (19)$$

- d_x – пречник исушене зоне земљишта

Уколико је услов испуњен, резултат је валидан и треба уважити утицај исушивања земљишта. У супротном, примењују се вредности прорачуна без утицаја исушености [3].

4.1. Прорачун за каблове положене у снопу

За полагање три кабла у снопу на дубини од h = 0,7 m, термичке отпорности, геометријски параметри и максимално дозвољена струја су (из погл. 3):

- $a = d_k = 40{,}26\ mm$
- $I_{max} = 337\ A$

Прорачунати параметри:

- $R' = 0{,}249 \cdot 10^{-3}\ \Omega/m$
- $P = 28{,}28\ W/m$
- $k_x = 3{,}037$
- $d_x = 0{,}260\ m$

Пошто је услов да долази до исушења, $d_x > 2a$ испуњен, претпоставка о исушивању је валидна. Термичка отпорност исушене земље и максимална дозвољена струја износе:

$$R_{tiz} = 4{,}51175\ Km/W$$
$$I_{max} = 267{,}74\ \mathrm{A}$$

Треба проверити да ли је при овој струји испуњен услов $d_x > 2a$ што у овом случају јесте јер је:

$$d_x = 0{,}497\ m$$

Према вредностима које се користе у домаћој електропривреди максимално дозвољена трајна струја при карактеристици потпуно исушеног земљишта и на референтној температури износи $237{,}65\ A$ [5].

4.2. Прорачун за каблове положене у равни

За полагање три кабла у равни на дубини од h = 0,7 m, термичке отпорности, геометријски параметри и максимално дозвољена струја су (из погл. 3):

- $a = d_k + d_{12} = 110{,}26\ mm$
- $I_{max} = 356{,}23\ A$

Прорачунати параметри:

- $R' = 0{,}259 \cdot 10^{-3}\ \Omega/m$
- $P = 32{,}87\ W/m$
- $k_x = 2{,}6$
- $d_x = 1{,}264\ m$

Пошто је услов да долази до исушења, $d_x > 2a$ испуњен, претпоставка о исушивању је валидна.

Максимална струја којом се кабл може оптеретити уважавајући исушење износи:

$$I_{max} = 286{,}39\ \mathrm{A}$$

Према вредностима које се користе у домаћој електропривреди, максимално дозвољена трајна струја износи $251{,}23\ A$ [5].

Иако су прорачуном добијене нешто више вредности струје у односу на вредности које се уобичајено користе у домаћој електроенергетској пракси, разлика се може приписати различитим моделским претпоставкама. Вредности које се примењују у пракси засноване су на условима потпуно исушеног земљишта са фиксном термичком отпорношћу, док спроведени прорачун узима у обзир постепену промену термичких карактеристика тла у зависности од оптерећења кабла. У домаћим препорукама се при израчунавању дозвољене струје полази од основних вредности које се затим коригују редукционим фактором, како би се уважавао утицај различите термичке отпорности земљишта.

5. УТИЦАЈ ПРОМЕНЉИВОГ ДИЈАГРАМА ОПТЕРЕЋЕЊА

У реалним условима рада електроенергетских каблова, оптерећење није константно већ варира у току дана. Ове варијације зависе од карактеристика потрошачког подручја, доба дана, као и навика

корисника. Као последица променљивог оптерећења, варира и снага губитака, што директно утиче на загревање кабла и околног тла. Код променљивог оптерећења, у земљишту се формира уски слој тла око кабла који „прати“ температурне осцилације услед промена струјног оптерећења. Димензије овог слоја зависе од облика и учестаности дијаграма оптерећења. Унутар овог слоја земљиште се загрева под утицајем максималне снаге губитака, док се остатак земљишта загрева у складу са средњом вредношћу оптерећења. Промена оптерећења у прорачуну се уважава преко фактора оптерећења m, који представља однос између стварног оптерећења кабла и његовог максималног дозвољеног оптерећења током одређеног периода. Вредност фактора m зависи од облика дијаграма оптерећења и времена трајања појединих интервала. На основу њега се коригује израчуната термички дозвољена струја, тако да вредности дозвољене струје при променљивом оптерећењу буду нешто више него код константног оптерећења, јер током дана постоје периоди нижег оптерећења који омогућавају спорије загревање кабла [3].

У табели 1 су приказане прорачунате вредности термички трајно дозвољене струје за константно и променљиво оптерећење. Добијени резултати показују да се у случају променљивог оптерећења кабл може оптеретити већим струјама.

Табела 1. Поређење максимално дозвољене струје

Начин полагања	Константо оптерећење	Променљиво оптерећење
У снопу	337 A	378 A
У равни	356 A	408 A

6. УТИЦАЈ ТЕМПЕРАТУРЕ ЗЕМЉИШТА

Термички дозвољена струја којом се кабл може дугорочно оптеретити зависи од услова околине, пре свега од температуре амбијента и стања земљишта у коме је кабл положен. У досадашњим прорачунима коришћена је референтна температура земље од 20°C, али у реалним условима температура варира у зависности од годишњег доба, што директно утиче на капацитет оптерећења каблова [5].

Табела 2. Поређење максимално дозвољене струје када су каблови у снопу

Температура	Прорачуната вредност	Вредност из праксе
30^0C	312 A	322 A
20^0C	337 A	350 A
5^0C	371 A	385 A

Табела 3. Поређење максимално дозвољене струје када су каблови у равни

Температура	Прорачуната вредност	Вредност из праксе
30^0C	330 A	340 A
20^0C	356 A	370 A
5^0C	393 A	407 A

7. ЗАКЉУЧАК

У овом раду извршена је анализа термички трајно дозвољене струје електроенергетских каблова, са циљем бољег разумевања утицаја различитих фактора на струјно оптерећење и безбедан рад кабловских система. Кроз прорачун и разматрање конструктивних и спољашњих параметара, изведени су закључци који имају директну примену у пројектовању и експлоатацији електроенергетских мрежа. Добијени резултати показују да конструкција каблова, термичке карактеристике земљишта (температура и влажност), као и облик дијаграма оптерећења, представљају кључне факторе у одређивању термички дозвољене струје каблова.

8. ЛИТЕРАТУРА

[1] Конструкција XHE 49 кабла и попречни пресек
https://www.fkz.rs/katalozi/FKZSPDF.pdf
приступљено 14.11.2024.

[2] Електроенергетски каблови
https://www.ucg.ac.me/skladiste/blog_4397/objava_67323/fajlovi/!!Pr%20EEK%202018.pdf
приступљено 10.11.2024.

[3] Драган Тасић, „*Основи електроенергетске кабловске технике*“, Електронски факултет у Нишу, Ниш 2001.

[4] Никола Рајаковић, Драган Тасић, Гојко Савановић „*Дистрибутивне и индустријске мреже*“, Београд 2004

[5] Кончар, „*Каталог Технички прорачуни*“, Електроиндустрија д.д., Загреб 2023

Кратка биографија

Милош Пајић је рођен 1997. године у Лозници. Завршио је средњу „Техничку школу“ у Лозници. Дипломски рад на факултету техничких наука из области електротехнике и рачунарства – Електроенергетски системи одбранио је 2020. godine.
Контакт: milospajic1712@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 4.9
ДОИ: https://doi.org/10.24867/34BE35Djanic

Примена факторизације матрица у системима препорука

Application of Matrix Factorization in Recommender Systems

Леополдина Ђанић, *Факултет техничких наука, Нови Сад*

Студијски програм – РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У овом раду се разматра и изучава примена медода факторизације матрица у системима препорука. Проучавају се различите методе факторизације матрица. Циљ је да се побољшају тачности и персонализација препорука. Проблем који се решава се односи на што прецизније предвиђање оцена које би корисник дао филмовима. Технике коришћене у експерименту су СВД, СВД++ и ТимеСВД++.*

Кључне речи: *системи препорука, факторизација матрица, СВД, СВД++, ТимеСВД++*

Abstract – *This paper examines and explores the application of matrix factorization methods in recommender systems. Various matrix factorization techniques are studied with the goal of improving the accuracy and personalization of recommendations. The main problem addressed is achieving more precise prediction of the ratings that users would assign to movies. The techniques used in the experiment are SVD, SVD++ and TimeSVD++.*

Keywords: *recommendation system, matrix factorization, SVD, SVD++, TimeSVD++*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Драган Иветић, ред. проф.

1. УВОД

Развојем интернета у последњих пар деценија повећала се и количина информација која се налази на интернету. Корисник сам не може да се снађе у овако великом обиму информација и да пронађе оно што га занима. Ова велика појава информација се назива још и преоптерећење информацијама (*енг. Information overload*). Системи препорука уведени су да олакшавају корисницима претрагу чинећи је бржом и омогућавајући корисницима да пронађу што више релевантних података. Најкоришћенији тип система препорука који се користе су системи препорука засновани на сарадњи [1]. Поред предности које су увели системи препорука, јављају се и проблеми у њиховом коришћењу као што су проблем реткоће информација (*енг. Sparsity*) и проблем хладног старта (*енг. Cold start problem*). У циљу решавања ових проблема уведени су системи препорука базирани на моделу а најпопуларнији овакав систем је систем препорука који користи факторизацију матрице. Факторизација матрице је добила знатно на популарности након такмичења које је организовала компанија Нетфликс 2006. године [2]. Циљ овог рада је да се истраже различити модели факторизације матрице и да се испитају њихове предности и мане.

2. ФАКТОРИЗАЦИЈА МАТРИЦЕ

Факторизација матрице је модел латентних фактора [2]. У моделима факторизације матрице је циљ да се и корисницима и филмовима придруже латентни фактори [3]. Латентни фактори се добијају учењем и тренирањем модела и служе да прикажу колико је корисник или филм повезан са појединим фактором. Код филмова латентни фактори могу бити жанрови иако их рачунар и модел неће видети у семантичком смислу као конкретан жанр, повезаће их са корисницима на исправан начин. Факторизација матрица је постала веома доминантна техника у примени у системима препорука [2]. Разлог увођења факторизације матрица је да се реше основни проблеми система препорука као што су реткоћа информација. Реткоћа информација је појава која настаје због недостатака информација о кориснику, корисници не оцењују све филмове које погледају, корисници су одгледали само јако мали део филмова од укупног броја филмова који постоје. То доводи до тога да матрица корисник-филм има веома велики број празних ћелија, што доводи до беспотребног заузећа меморије.

Основна идеја факторизације матрица је да почетну матрицу корисник-филм раздвоји на две нове матрице нижег ранга: корисник-фактор и филм-фактор [4]. У изразу (1) је приказана ова формула при чему је $\hat{A}$ матрица приближна почетној матрици, U^{T} је транспонована матрица корисник-фактор, а V је матрица филм-фактор.

$$\hat{A} \approx U^{T}V \tag{1}$$

Рачунање предвиђене оцене по овом основном моделу би се рачунало као што је приказано у изразу (2), где је u корисник који оцењује, i је филм који се оцењује, $\hat{r}_{ui}$ је предвиђена оцена, p_u је ред из матрице корисник-фактор, док је q_i ред из матрице филм-фактор.

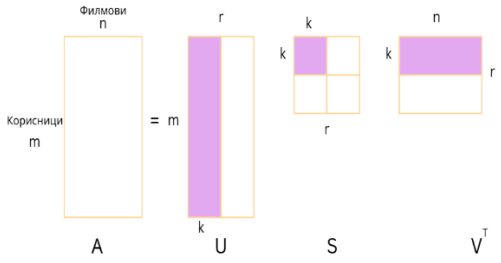
$$\hat{r}_{ui} = p_u q_i \tag{2}$$

2.1. Декомпозиција сингуларне вредности

Декомпозиција сингуларне вредности (*енг. Singular Value Decomposition, скр. СВД*) се први пут појавила као модел 2000. године у системима препоруке [5]. СВД модел, за разлику од основног модела факторизације матрице разлаже почетну матрицу A на 3 матрице: U, S и V. Димензије ових матрица су редом $m \times n$, $m \times r$, $r \times r$, $r \times n$, где су m број корисника, n је број филмова, r је ранг матрице A. У изразу (3) приказана је формула коју користи СВД модел.

$$A = USV^T \tag{3}$$

Циљ СВД модела је да смањи димензионалност почетне матрице и то ради тако што изабере константу k па из израчунате матрице U узме првих k колона, из матрице S узме исечак $k \times k$, а из матрице V узме првих k колона. На слици 1 приказана је ова редукција на нижи ранг.



Слика 1. Пример смањивања ранга [4]

2.2. СВД++

СВД модел није узимао у обзир ништа осим оцена корисника. Такође, СВД модел има ману проблема хладног старта. Овај проблем се јавља приликом регистрације новог корисника на систем. Не постоје подаци о кориснику, он још није оценио ни одгледао ниједан филм, па систем не зна шта би могао да му препоручи. Овај проблем се дешава и када се појави нови филм у систему који нема ниједну оцену. Како би се решио проблем хладног старта настао је нови модел СВД++ [6]. Разлика у односу на основни СВД модел је што СВД++ уводи посматрање корисниковог понашања, односно имплицитне податке о кориснику [7]. Поред имплицитних података СВД++ посматра и предрасуде корисника и предрасуде самог филма.

Предрасуда корисника према неком филму се јавља када корисник зна да ће у филму бити добар глумац или глумац којег воли, ако је филм режирао режисер који је пре тога увек режирао добре филмове. Ови фактори ће утицати на корисникову коначну оцену коју да филму након што га одгледа, а та оцена не мора да буде реална, односно може бити већа или мања у односу на стварну вредност оцене којом би филм требао бити оцењен.

Предрасуда филма показује колико је филм прецењен или потцењен у односу на реалну оцену. У предрасуду филма се убрајају и популарност филма у одређеном временском периоду, као што су новогодишњи филмови популарни у зимском периоду, хорор филмови су популарнији у периоду око празника Ноћи вештица и у том периоду је већа шанса да филм буде оцењен бољим оценама него у било ком другом периоду године.

У изразу (4) приказана је формула коју СВД++ модел користи за рачунање предикције оцене коју би корисник u дао филму i. У формули $\hat{r}_{ui}$ је израчуната предвиђена оцена, μ је укупна просечна оцена свих филмова, b_u је предрасуда корисника u, b_i је предрасуда филма i, q_i је вектор латентних фактора филма i, p_u је вектор латентних фактора корисника u, y_j су имплицитни фактори корисника са филмовима које је одгледао, $N(u)$ је скуп филмова са којима је корисник имао интеракцију (оценио их је, претраживао, одгледао).

$$\hat{r}_{ui} = \mu + b_u + b_i + q_i^T \left(p_u + \frac{1}{\sqrt{|N(u)|}} \sum_{j \in N(u)} y_j\right) \tag{4}$$

2.3. ТимеСВД++

Како би се побољшао СВД++ модел и повећала тачност у предикцијама уведен је и временски фактор чиме је креиран ТимеСВД++ модел који је предложен 2010. године [5]. ТимеСВД++ модел узима у обзир и временски тренутак када је корисник оценио филм. Корисников укус и интересовања могу да се промене током времена, њега могу данас интересовати филмови који припадају жанру акција, а да за пар месеци или година промени интересовање и да га више занимају филмови који припадају жанру комедија. Расположење корисника може утицати на оцену коју ће дати одгледаном филму, већина корисника је обично уморна радним данима и ако погледају филм увече може се десити да га нису доживели исто као што би то био случај да су филм гледали викендом или када су одморни. ТимеСВД++ модел посматра корисниково понашање током читавог времена, а не само у блиској прошлости [3]. Он може уочити патерне корисниковог оцењивања.

Параметар корисниковог предрасуда b_u се мења током времена, јер филм који оцени једном оценом, након неког времена може оценити већом или мањом оценом, што се често дешава јер корисник у једном тренутку крене да упоређује филмове и оцене које је дао филмовима. Корисник може постати строжи у оцењивању током времена.

Параметар предрасуда филма b_i се мења током времена због утицаја популарности самог филма. ТимеСВД++ модел може уочити када је филм мање или више популаран на основу генералних оцена које филмови добијају коришћењем података о оценама и времену када су оцене додељене филму. Популарност новог филма може да порасте нагло, ако се зна да ће познати глумци глумити у филму. Може се десити да након неког времена популарност филма опадне, јер корисници стекну утисак да ли је филм добар или није и после неког времена га оцењују реалнијим оценама.

У изразу (5) приказана је формула коју користи ТимеСВД++ модел да израчуна оцену коју би корисник u дао филму i. Ова формула представља проширење формуле коју користи СВД++ модел, а која је приказана у изразу 4. тиме што је уведено да предрасуд корисника $b_u(t)$ зависи од времена,

предрасуд филма $b_i(t)$ зависи од времена и латентни фактори корисника $p_u(t)$ зависе од времена.

$$\hat{r}_{ui}(t) = \mu + b_u(t) + b_i(t) + q_i^T(p_u(t) + \frac{1}{\sqrt{|N(u)|}}\sum_{j\in N(u)} y_j) \quad (5)$$

3. МЕТРИКЕ ЕВАЛУАЦИЈЕ

За мерење грешке коју су модели направили у експериментима коришћене су средња апсолутна грешка и корен средње квадратне грешке.

3.1. Средња апсолутна грешка

Средња апсолутна грешка је грепка која се рачуна као однос суме апсолутних вредности разлика стварне и израчунате вредности и броја рачунања [9]. У изразу (6) је приказана формула рачунања средње апсолутне грешке, при чему n представља укупан број предвиђених вредности, y_{ti} је стварна оцена, док је y_i предвиђена оцена.

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_{ti} - y_i| \quad (6)$$

3.2. Корен средње квадратне грешке

Корен средње квадратне грешке се рачуна као корен збира квадрата разлике између израчунате предвиђене оцене и стварне оцене, подељене са бројем предвиђених оцена [10]. У изразу (7) је приказана формула рачунања корена средње квадратне грешке означене са *RMSE*, при чему n представља број предвиђених оцена, y_{ti} представља тачну вредност оцене, док y_i представља предвиђену вредност оцене.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_{ti} - y_i)^2} \quad (7)$$

4. ЕКСПЕРИМЕНТИ

За експерименте, њихову имплементацију и евалуацију резултата је коришћен програмски језик *Python.* Скуп података који је коришћен за тренирање различитих модела факторизације је *MovieLens* који је преузет са сајта *Kaggle* [8]. Овај скуп података се састоји од 2 табеле. Прва табела састоји се од 3 колоне, при чему је прва колона идентификатор филма, друга колона је назив филма и трећа колона представља жанрове филма. Друга табела се састоји од 4 колоне, где је прва колона идентификатор корисника, друга колона је идентификатор филма који је корисник оценио, трећа колона је вредност оцене коју је корисник дао филму и четврта колона је временски тренутак када је корисник оценио филм. Прва табела састоји се од преко 62 хиљаде филмова, а друга се састоји од преко 25 милиона података.
Како би се олакшало рачунање и избегли проблеми који настају због непопуњености матрице, подаци су филтрирани тако што су узети само они филмови који имају више од 50 оцена и само они корисници који су оценили више од 20 филмова. Овом филтрацијом добијена је матрица од преко 162 хиљаде корисника и преко 13 хиљада филмова.
Модели који су тренирани су модели описани у претходном поглављу: СВД, СВД++ и ТимеСВД++. Модели су тренирани над узорком података од 10 000 редова из матрице корисник-филм, за тренинг је узето 80% узорка, док је за тестни скуп узет остатак од 20% узорка. Метрике коришћене за евалуацију су средња апсолутна грешка наведена у изразу (6) и корен средње апсолутне грешке наведене у изразу (7).
Резултати су приказани у табели 1 из које се види да највећу грешку даје СВД модел, где је PMCE 2.4552, а MAE 2.1379. Много бољи резултат постигао се коришћењем СВД++ модела чије грешке су PMCE: 0.8805, а MAE: 0.6778. Најбољи резултат и најмању грешку дао је ТимеСВД++ модел који је за нијансу бољи у односу на СВД++ модел, PMCE: 0.8787, MAE: 0.6752.

Табела 1. Поређење резултата грешака различитих модела

Грешка / Модел	СВД	СВД++	ТимеСВД++
PMCE	2.4552	0.8805	0.8787
MAE	2.1379	0.6779	0.6752

5. ЗАКЉУЧАК

Факторизација матрице је увела велико побољшање у системима препоруке. Резултати који су добијени у експерименту су показали да када модел има више информација о корисницима и филмовима може да израчуна тачнију предикцију и тачније одреди који филм би се кориснику више свидео.
Поред података коришћених у експерименту додатни подаци који би могли да се користе су локација где је сниман филм, локација корисника, старосна доб корисника, пол корисника. Све ове податке би систем могао да искористи да направи прецизније предикције.
Због своје велике користи, системи препорука ће постати незаобилазна ставка у свим великим апликацијама, сајтовима и платформама и због тога будућа истраживања треба да се посвете не само побољшању употребе факторизације матрица у системима препоруке, истицању њених предности и умањивању њених мана, већ и проналазак нових техника које ће можда дати боље резултате у системима препорука.

6. ЛИТЕРАТУРА

[1] X. Zhou, J. He, G.Huang, Y. Yhang, “SVD based incremental approacher for recommender systems”, Joiurnal of Computer and System Sciences, Vol. 81, pp. 717-733, June 2015.

[2] R. Bell, C. Volinosky, “Matrix factorization techniques for recommender systems”, Computer, pp. 30-37, August 2009.

[3] Y. Koren, “Collaborative filtering with temporal dynamics”, Proceeding of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 447-456, June 2009.

[4] F. O. Isinkaye, “Matrix Factorization in Recommender Systems: Algorithms, Applications and Peciuliar Challenges”, IETE Journal of research, pp. 6087-6100, November 2021.

[5] R. Mehta, K. Rana, “A Review on Matrix Factorization Techniques in Recommender Systems”, CSCITA, pp. 269-274, April 2017.

[6] M. Jallouli, S. Lajmi, I. Amous, “When contextual information meets recommender systems: extended SVD++ models”, International Journal of Computers and Applications, pp. 349-356, May 2020.

[7] B. Zhang, X. Zhou, J. Li, L. Li, “Recommendation Algorithm Based on Matrix SVD with Exponential Correction”, CIPAE 2020, pp. 71-75, October 2020.

[8]https://www.kaggle.com/datasets/parasharmanas/movie-recommendation-system, (pristupljeno u oktobru 2025.)

[9] S. Jiang, J. Li, W. Zhou, “An Application of SVD++ Method in Collaborative Filtering”, IEEE, pp. 192-197, January 2021.

[10] https://www.datacamp.com/tutorial/rmse, (pristupljeno u oktobru 2025.)

Кратка биографија:

Леополдина Ђанић рођена је у Врбасу 2001. године. Завршила је Електротехничку школу „Михајло Пупин“ у Новом Саду, 2020. године. Факултет техничких наука у Новом Саду је уписала 2020. године. Дипломирала је на Факултету техничких наука на одсеку Рачунарство и аутоматика 2024. године са просечном оценом 9.68. Године 2024. је уписала мастер академске студије на Факултету техничких наука у Новом Саду, студијски програм рачунарство и аутоматика.
Контакт:
leopoldina.djanic01@gmail.com

Зборник радова Факултета техничких наука, НовиСад

УДК: 621.38
ДОИ: https://doi.org/10.24867/34BE36Pavlovic

СИМУЛАЦИЈА И ТЕСТИРАЊЕ РАДА УПРАВЉАЧКЕ ЈЕДИНИЦЕ РЕКЛОЗЕРА У РЕАЛНОМ ВРЕМЕНУ

SIMULATION AND TESTING OF RECLOSER CONTROL UNIT IN REAL-TIME OPERATIONS

Андреа Павловић, Невен Ковачки, *Факултет техничких наука, Нови Сад*

Студијски програм – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Овај рад обрађује симулацију и тестирање рада управљачке јединице реклозера ABB RER615 у симулационом окружењу Typhoon HIL, уз интеграцију са симулатором HIL604 преко уређаја Universal HIL Connect. Примјеном методологије Controller Hardware-in-the-Loop (C-HIL) омогућено је тестирање стварне управљачке јединице без потребе за сложеним лабораторијским условима. Кратки спојеви се симулирају безбједно и поновљиво, што унапређује верификацију заштитних функција. Симулације су обухватиле различите типове кварова и трајања поремећаја, уз анализу реакције прекострујне заштите и логике аутоматског поновног укључења.*

Кључне речи: *управљачка јединица реклозера, кратак спој, заштита, аутоматско поновно укључење, симулација*

Abstract – *This paper deals with the simulation and testing of ABB RER615 recloser control unit within the Typhoon HIL simulation environment, integrated with the HIL604 simulator via the Universal HIL Connect device. By applying the Controller Hardware-in-the-Loop (C-HIL) methodology, real control unit testing is enabled without the need for complex laboratory conditions. Short circuits are simulated safely and repeatably, enhancing the verification of protection functions. The simulations covered various fault types and disturbance durations, with analysis of the overcurrent protection response and automatic reclosing logic.*

Keywords: *recloser control unit, short circuit, protection, automatic reclosing, simulation*

1. УВОД

Савремени електроенергетски системи (ЕЕС) све више се ослањају на дигиталне технологије и интелигентне електронске уређаје ради унапрјеђења поузданости, флексибилности и ефикасности дистрибутивних мрежа (ДМ). У том контексту, реклозери представљају један од најшире коришћених елемената у аутоматизацији ДМ, омогућавајући брзо отклањање поремећаја и смањење времена прекида напајања, јер се након краткотрајног квара самостално поново укључују путем механизма аутоматског поновног укључења АПУ. Поред основне функције прекидања и АПУ, савремени реклозери омогућавају напредну дијагностику, комуникацију и интеграцију са SCADA системима. Њихова примјена значајно доприноси стабилности ДМ и селективности заштите у оквиру ДМ [1].

Традиционалне методе тестирања управљачких функција ових уређаја захтијевају сложене и често ризичне лабораторијске услове. Као одговор на те изазове, све више се примјењује C-HIL методологија, која омогућава директно повезивање стварног управљачког уређаја са симулатором који у реалном времену израчунава електроенергетске услове система. У оквиру овог приступа, Typhoon HIL софтвер се користи за моделовање дистрибутивне мреже, док се симулација извршава на хардверском симулатору реалног времена. Повезивање управљачке јединице са симулатором реализује се преко Universal HIL Connect (UHC) уређаја, који врши конверзију аналогних сигнала у опсегу ±10 V из симулатора реалног времена у одговарајуће аналогне сигнале за физички уређај, чиме се обезбјеђује стабилна и прецизна интеракција између симулираног модела и стварног хардвера.

На тај начин, уређај управља симулираним објектом као да је у стварном окружењу, чиме се омогућава прецизна анализа одзива, верификација алгоритама и безбједно тестирање без потребе за физичким моделима или опасним испитивањима [2].

2. РЕЛЕЈНА ЗАШТИТА У ДИСТРИБУТИВНИМ МРЕЖАМА

Кварови у ЕЕС најчешће настају усљед оштећења изолације, атмосферских пражњења, механичких напрезања или контакта са страним тијелима као што су гране, птице или влага. У средњенапонским мрежама, овакви поремећаји могу довести до кратког споја (КС), прекида у напајању и оштећења опреме. Због тога је неопходна системска заштита која брзо, селективно и поуздано реагује на поремећаје у раду мреже.

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Невен Ковачки, доцент

Та функција се остварује кроз релејну заштиту, на основу које прекидачка опрема изолује оштећени дио система и спрјечава ширење квара. Релејна заштита обухвата различите типове релеја, који се повезују на мјерне трансформаторе и прекидаче, а њен задатак је да надзире електричне величине и пошаље сигнал прекидачу када се прекораче подешене вриједности, на основу кога се прекидач отвара [3].
Са развојем електронских технологија и потребом за већом прецизношћу, брзином и флексибилношћу у реаговању на поремећаје, класични електромеханички релеји постепено су замијењени дигиталним рјешењима. Тако је настао концепт микропроцесорске релејне заштите, који обједињује више функција у једном уређају и омогућава напредну обраду сигнала и комуникацију.

2.1. Микропроцесорска релејна заштита

Микропроцесорски релеји представљају најсавременији облик релејне заштите, који обједињује више функција у једном уређају. Улазни сигнали се дигитално обрађују, пореде са референтним вриједностима, а уређај реагује активирањем прекидача, снимањем догађаја или обавјештавањем оператера. Поред основне заштитне функције, омогућена је и анализа поремећаја, локална и даљинска конфигурација, као и интеграција у надзорне системе.
Ови релеји подржавају самодијагностику, даљински надзор и комуникацију са SCADA системима , уз подршку за стандардне протоколе као што су IEC 61850, Modbus, DNP3 итд. Примјена алгоритама као што су дискретна Фуријеова трансформација и модели у простору стања омогућава прецизну идентификацију кварова. Захваљујући брзини, флексибилности и могућности адаптације, микропроцесорска заштита постаје стандард у модерним ЕЕС [4].

2.2. Прекострујна заштита

Прекострујна заштита је најстарији и најраспрострањенији облик релејне заштите. Њена основна функција је да детектује струју већу од подешене и иницира искључење оштећеног дијела система. Примјењује се на водовима, трансформаторима и другим елементима мреже.
У радијалним мрежама користи се неусмјерена прекострујна заштита, док се у сложенијим топологијама примјењује усмјерена варијанта. Подешавање релеја врши се на основу прорачуна нормалних режима и очекиваних струја КС, уз уважавање захтјева за селективност и брзину реаговања [4].

3. КОНСТРУКЦИЈА И ПРИНЦИП РАДА РЕКЛОЗЕРА

У средњенапонским ДМ, већина кварова је пролазног карактера и траје само неколико секунди. Без реклозера, сваки квар узрокује испад цијелог вода и захтијева теренску интервенцију. Реклозери омогућују АПУ, чиме се пролазни кварови превазилазе без трајног прекида напајања.
Реклозер је прекидач са самосталним управљањем који детектује прекомјерну струју и извршава више циклуса отварања и затварања. У случају трајног квара, уређај прелази у режим закључавања до ручне интервенције. Постављају се дуж извода ради секционисања и селективне заштите, а не користе се на подземним водовима због трајне природе кабловских кварова.
Савремени реклозери имају вакуумски прекидач, управљачки орман, сензоре, комуникационе интерфејсе и заштитне функције. Подржавају даљинско управљање, дијагностику, снимање догађаја и интеграцију у SCADA системе [1, 3].
RER615 је савремени микропроцесорски управљачки уређај намијењен примјени у средњенапонским ДМ, са подршком за заштиту, управљање, аутоматизацију и анализу квалитета електричне енергије. Заснован је на серији Relion 615 и у потпуности подржава IEC 61850 и GOOSE, што омогућује интеграцију у напредне SCADA системе, вишеструко АПУ, рад у радијалним и упетљаним мрежама, као и конфигурацију преко софтверског алата PCM600. Управљање се може врши локално преко HMI панела или даљински, уз подршку за више комуникационих протокола.
Основне функције укључују прекострујну и земљоспојну заштиту, термичку заштиту, провјеру синхронизације и напредну дијагностику. Уређај се испоручује у конфигурацијама A, D и E. У овом раду тестирана је конфигурација D [5]. На слици 1 приказан је изглед предње стране управљачке јединице ABB RER615, са HMI панелом који омогућава локално управљање и надзор параметара током рада.

Слика 1. *Изглед предње стране управљачке јединице реклозера ABB RER615 [5]*

4. СИМУЛАЦИЈА РАДА УПРАВЉАЧКЕ ЈЕДИНИЦЕ РЕКЛОЗЕРА У TYPHOON HIL ОКРУЖЕЊУ

Развој компоненте „RER615 Circuit Breaker and Measurements“ у оквиру Typhoon HIL платформе започет је унутар Schematic Editor-a, гдје је графички моделована структура управљачке јединице реклозера ABB RER615. Компонента је конципирана тако да обухвата трофазни прекидач, трофазне мјерне јединице, дигиталне улазе и излазе, као и логичке блокове који одговарају стварној конфигурацији уређаја. Сви елементи су повезани са сигналима симулатора, а параметри као што су називни напон, струја и логички услови дефинисани су унутар

картица компоненте у којима се подешавају технички параметри управљачке јединице. Ови параметри морају бити усклађени са конфигурацијом уређаја ABB RER615, која се врши преко PCM600 софтвера, како би се обезбиједила тачна симулација и поуздана интеракција са физичким уређајем. Маскирање компоненти у један подсистем омогућило је управљање унутрашњом структуром преко Python функција, уз динамичко прилагођавање изгледа и понашања компоненте. Повезивањем са физичким уређајем преко UHC, обезбиједена је директна интеракција између симулираног модела и стварне управљачке јединице, што је приказано на слици 2. Оваква архитектура омогућава реалистичну симулацију понашања уређаја у различитим оперативним условима, без потребе за физичким моделом мреже.

Слика 2. *Физичка интеграција управљачке јединице у тестно окружење*

5. ТЕСТИРАЊЕ РАДА УПРАВЉАЧКЕ ЈЕДИНИЦЕ РЕКЛОЗЕРА У TYPHOON HIL ОКРУЖЕЊУ

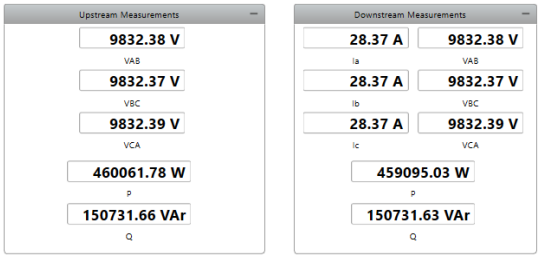
Након развоја компоненте „RER615 Circuit Breaker and Measurements“ унутар Schematic Editor-a, она је интегрисана у симулациони модел дистрибутивне мреже, што је приказано на слици 3. АПУ је конфигурисан унутар управљачке јединице реклозера ABB RER615 преко PCM600 софтвера, при чему је подешен на два циклуса са безнапонским паузама од 3 и 10 секунди.

Мрежни модел представља поједностављену структуру дистрибутивне мреже са линијским напоном 10 kV, трофазном снагом КС 35 MVA и фреквенцијом 50 Hz. Водови су дефинисани са подужном отпорношћу 0,32 Ω/km и реактансом 0,205 Ω/km, при чему су дужине секција:

- од извора мреже до прве сабирнице: 1 km
- иза реклозера: 1,5 km
- до крајњег потрошача: 3 km

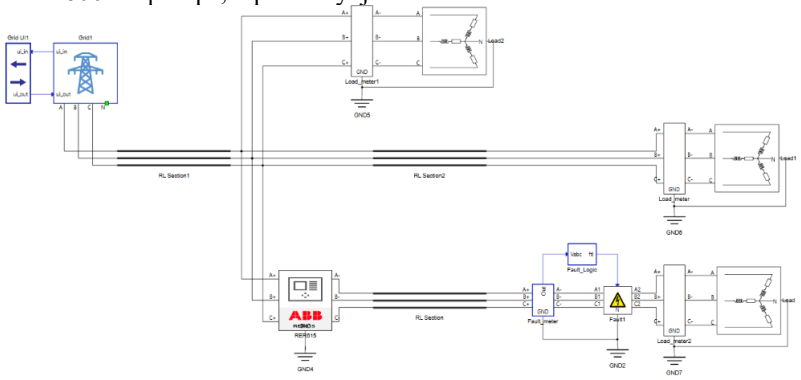
На воду су прикључена три потрошача са снагама од 500 kVA, 300 kVA и 200 kVA, уз факторе снаге од 0,95, 0,97 и 0,98. Између реклозера и потрошача постављена је компонента „Fault“, која омогућава симулацију различитих типова КС и дефинисање њиховог трајања.

Симулација је спроведена у реалном времену, уз надзор преко HIL SCADA панела и HMI екрана управљачке јединице. По учитавању HIL SCADA панела, који омогућава надзор аналогних и дигиталних сигнала, као и интеракцију са управљачком јединицом реклозера ABB RER615 може се приступити подпанелу компоненте „RER615 Circuit Breaker and Measurements“, у којем се налази команда „External Close Command“ (спољна команда за затварање). Активирањем ове команде, управљачка јединица ABB RER615 шаље сигнал прекидачу да затвори контакте, чиме се омогућује напајање потрошача иза реклозера. На слици 4 приказана су мјерења на реклозеру унутар HIL SCADA панела.

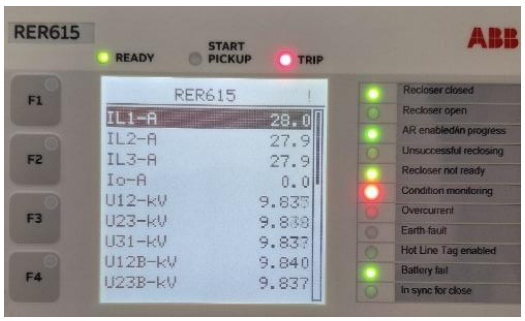


Слика 3. *Приказ мјерења на реклозеру у HIL SCADA панелу*

Подаци о струјама и напонима доступни су и на LCD екрану управљачке јединице, што потврђује синхронизацију између симулатора и физичког уређаја, као што је приказано на слици 5.



Слика 4. *Модел мреже у Schematic Editor-у*



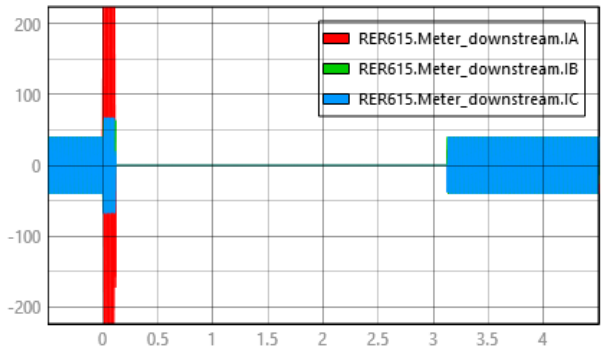
Слика 5. *Приказ мјерења на управљачкој јединици током симулације у реалном времену*

У оквиру прозора „Fault“, у HIL SCADA панелу, могуће је одабрати тип КС и његово трајање, чиме се иницира поремећај у мрежи и активира заштитна логика уређаја.

Иако су у оквиру истраживања тестирани сценарији са три различита трајања поремећаја (1 s, 5 s и трајни) за једнофазне (A–N) и трофазне (A–B–C) кратке спојеве, због ограничења простора у овом раду приказани су само резултати за једнофазан кратак спој са трајањем квара од 1 секунде.

На слици 6 приказан је одзив управљачке јединице реклозера ABB RER615 током једнофазног КС A–N. Квар се јавља у тренутку t=0 s, након чега управљачка јединица преко заштитне функције прекострујне заштите са струјно-независном карактеристиком детектује поремећај и активира заштитну реакцију. Прекидач се отвара 114 ms након појаве квара.

Струје иза реклозера падају на нулу и остају у том стању током безнапонске паузе од 3 секунде. Сигнал квара се гаси након 1 секунде, а прекидач се затвара по истеку безнапонске паузе, чиме се напајање потрошача наставља. Потрошачи испред реклозера остају под напајањем током читавог поремећаја.



Слика 6. *Графички приказ мјерених струја на управљачкој јединици реклозера ABB RER615 током симулације*

Овај резултат потврђује исправност конфигурације функције АПУ и синхронизовану реакцију управљачке јединице у условима симулације у реалном времену. На основу добијених резултата, може се закључити да је уређај ABB RER615 у конфигурацији D способан да поуздано изврши заштитну селекцију и АПУ у складу са дефинисаном логиком.

6. ЗАКЉУЧАК

Циљ овог рада био је да се развије и тестира библиотечка компонента управљачке јединице реклозера ABB RER615 у симулационом окружењу Typhoon HIL, уз интеграцију са симулатором HIL604 у реалном времену. Потврђено је да компонента вјерно реплицира понашање уређаја, а да је комуникација са симулатором стабилна и технички поуздана. Примјеном C-HIL методологије омогућено је безбједно, поновљиво и ефикасно тестирање заштитних функција без потребе за ризичним лабораторијским испитивањима. Овај приступ показао се као изузетно ефикасан за верификацију заштитних алгоритама, анализу реакције уређаја на различите типове кварова, као и процјену селективности и стабилности система у условима прелазних стања. Додатна предност овог приступа огледа се у могућности брзе реконфигурације тест сценарија и проширења модела без потребе за физичким интервенцијама. На тај начин, симулационо окружење постаје флексибилан алат за инжењерску анализу, развој и верификацију интелигентних електронских уређаја у складу са захтјевима савремених EEC.

7. ЛИТЕРАТУРА

[1] J. L. Blackburn, T. J. Domin: *Protective Relaying – Principles and applications*, fourth edition, Taylor & Francis, 2014.

[2] A. Genić, O. Gagarica, „Controller Hardware-In-the-Loop Simulation: Step by step guide“, Encyclopedia of Electrical and Electronic Power Engineering, 2023.

[3] J. Nahman, V. Mijailović: *Razvodna postrojenja*, drugo izdanje, Akademska misao, Beograd, 2015.

[4] D. Bekut: *Relejna zaštita*, Fakultet tehničkih nauka, Univerzitet u Novom Sadu, Novi Sad, 2009.

[5] ABB, „Grid Automation Recloser Protection and Control RER615: Product Guide“ Version 2.0, ABB Group, 2018.

Кратка биографија:

Андреа Павловић рођена је у Фочи 1999. Дипломски рад на Факултету техничких наука из области Електротехнике и рачунарства – Електроенергетски системи одбранила је 2022.год.
Контакт:
pavlovic.andrea@uns.ac.rs

Невен Ковачки рођен је 1987. године у Зрењанину. Дипломирао је на Факултету техничких наука из области Електротехнике и рачунарства – Електроенергетски системи 2010., 2011. и 2018. године.
Контакт:
kovackin@uns.ac.rs

Зборник радова Факултета техничких наука, Нови Сад

УДК: 621.316.925
ДОИ: https://doi.org/10.24867/34BE37Radic

Вјетроелектране у дистрибуираним мрежама и њихова заштитна опрема
Wind power plants in distribution grids and their protection eqipment

Немања Радић, Александар Станисављевић, *Факултет техничких наука, Нови Сад*

Студијски програм – ЕНЕРГЕТИКА, ЕЛЕКТРОНИКА И ТЕЛЕКОМУНИКАЦИЈЕ

Кратак садржај – *У раду је описан рад вјетроелектране и њихове заштитне опреме, а такође је и урађена симулација на модификованој IEEE 13-bus дистрибутивној тест мрежи. IEEE 13 мрежа је модификована додавањем вјетроелектрана. У оквиру ове мреже моделована је и релејна заштита ветроелектране. Симулиран је трополни кратак спој са земљом и приказан је рад релејне заштите током кратких спојева.*
Кључне речи: *IEEE 13-bus тест мрежа, вјетроелектрана, релејна заштита, напон, струја*

Abstract – *This paper presents the operation of a wind power plant and its associated protection equipment, as well as a simulation conducted on a modified IEEE 13-bus distribution test network. The IEEE 13-bus network was adapted by incorporating wind power plants. Within this network, the relay protection system of the wind power plant was modeled. A three-phase fault to ground was simulated, and the performance of the relay protection during the fault conditions was analyzed and discussed.*

Keywords: *IEEE 13-bus test grid, wind power plant, relay protection, voltage, current*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Александар Станисављевић, вандредни професор

1. УВОД

Глобални еколошки проблеми и проблеми енергетског дефицита се данас у свијету посматрају као јединствен проблем добијања чисте енергије у складу са принципима одрживог развоја. Од свих обновљивих извора енергије највећи технолошки напредак и највећи тренд изградње у свијету у посљедњих 20 година имају вјетроелектране [1].

Тема овог рада јесте заштита вјетроелектрана у дистрибутивним мрежама микропроцесорском заштитом чија је функција да штите роторе вјетрогенератора, трансформаторе, изводе и многе друге дијелове вјетроелектрана. У овом раду, биће приказане предности које оваква заштита уноси у вјетро паркове и електроенергетске системе. Основни мотиви за примјену микропроцесорских заштитних уређаја јесу једноставна подешавања путем интуитивних софтверских алата.

У раду се објашњава како се примјењује заштита и шта је оно на шта треба да се обрати пажња при примјени заштите. Описани су стандарди који се примјењују при реализацији релејне заштите, као и могућности које заштита пружа кориснику.

У другој глави представљен је историјат и принцип рада вјетроелектрана. У трећој глави биће представљена енергија вјетра. У четвртој глави представљени су типови вјетротурбина те механичке карактеристике модерних вјетротурбина велике снаге. У петој глави описане су опште карактеристике микропроцесорске заштите, њен историјски развој, принцип рада, као и врсте заштита које се најчешће користе. Описан је и начин заштита вјетроелектрана као и правила прикључења вјетрогенератора на мрежу. Шеста глава представља симулацију у Матлаб Симулинку и резултате. Последње двије главе су Закључак и Литература.

2. ВЈЕТРОЕЛЕКТРАНЕ

Први писани трагови примене вјетроелектрана помињу се још 200. године п.н.е. и односе се на вјетрењаче коришћене за мљевење жита у тадашњој Персији. Почетком 12. вијека вјетрењаче се појављују у Европи у модификованом облику са хоризонталном осовином, слика 1 [1].

Слика 1. Древна вјетротурбина за мљевење жита [1]

Прву вјетротурбину која је коришћена за генерисање електричне енергије направио је 1891. године Данац Пол Ла Кур (Poul la Cour, 1846–1908). Енергетска криза из 1973. године, а касније и све већи еколошки проблеми везани за сагоријевање фосилних горива, поново популаризују обновљиве изворе енергије и почетком деведесетих година вјетрогенератори доживљавају ренесансу. Европска унија је 2007. године донела закон да 20% све енергије треба да буде из обновљивих извора до 2020. године. Очекује се да

ће енергија вјетра до 2050. године бити доминантан извор електричне енергије у свијету [2].
Кинетичка енергија вјетра се трансформише у механичку енергију помоћу вјетротурбине. Брзину обртања вјетротурбине (која износи десетак обртаја у минуту) обично је потребно прилагодити захтијеваној брзини обртања генератора. За то се користи механички мултипликатор.
Највише инсталисаних производних капацитета електричне енергије у ЕУ у посљедњих 20 година је у вјетроелектранама [1].

3. ЕНЕРГИЈА ВЈЕТРА

Вјетар је облик енергије који представља усмјерено кретање ваздушних маса. Настаје као посљедица разлика у атмосферским притисцима, које су узроковане неједнаким загријавањем ваздушних маса. Разликују се глобални или геострофски вјетрови и локални или површински вјетрови. С обзиром на то да вјетар представља усмјерено кретање ваздушних маса он посједује одређену кинетичку енергију, која је сразмјерна маси и квадрату брзине којом струји та маса ваздуха.

$$P' = \frac{1}{2}\rho \cdot V^3. \qquad (3.7)$$

Снага вјетра је пропорционална трећем степену брзине вјетра, што значи да се и врло мале варијације брзине вјетра битно одражавају на промјену његове снаге. Јака зависност између снаге и брзине вјетра има низ битних посљедица на пројектовање вјетроелектрана, како у погледу захтијеване тачности мјерења брзине вјетра, тако и у погледу захтијеваних експлоатационих карактеристика вјетроагрегата [5].

4. ВЈЕТРОТУРБИНЕ

Кинетичка енергија вјетра се трансформише у механичку енергију обртног кретања помоћу вјетротурбине. Постоје различите конструкције вјетротурбина. Циљ је да се постигне што већи степен искоришћења и стабилан рад у што ширем опсегу брзина вјетра. Развој вјетротурбина је још увијек интензиван [1].
Генерално, вјетротурбине се дијеле на вјетротурбине са:

- вертикалном осовином,
- хоризонталном осовином.

Код вјетротурбина са вертикалном осовином вјетар струји нормално на осу ротације, па се оне не морају усмјеравати према смјеру дувања вјетра. Код њих се генератор поставља у подножју турбине, те нису потребни јаки торњеви, као код турбина са хоризонталном осовином. Познате су: Дариусова, Савонијусова и Х вјетротурбина [1].
Вјетротурбине са хоризонталном осовином се данас доминантно користе, како за велике, тако и за мале снаге. Могу бити постављене уз и низ вјетар. Вјетротурбине постављене низ вјетар се саме прилагођавају смјеру вјетра и не захтијевају посебне механичке системе за закретање према смјеру вјетра. За урбане градске услове вјетроагрегати су и даље врло мало примењиви, прије свега због буке и опасности за околину због могућег разлетања турбине усљед хаварије или проблема хватања леда на лопатице, којег центрифугалне силе могу откинути и при нормалном погону вјетротурбине. Ипак, у посљедње вријеме се интензивно развијају концепти малих турбина (са хоризонталном и вертикалном осовином) који су прихватљиви и за урбане средине [1].

5. РЕЛЕЈНА ЗАШТИТА ВЈЕТРОЕЛЕКТРАНА

Развој микропроцесорске заштите је почео крајем 60-тих и почетком 70-тих година. До краја 80-тих година микропроцесорске заштите су постале високо поуздане и сигурне. Средином и крајем 90-тих година цијена је смањена на испод 10% у односу на исти класични релеј (заштиту), при чему је микропроцесорском заштитом увијек обезбјеђена свеобухватнија и квалитетнија заштита [4].
Најчешће је случај да се микропроцесор користи као база за функционално обједињавање више врста релеја, као и функција које се срећу у оквиру заштитног система.
У раном периоду употребе вјетроелектрана, вјетротурбине су се тренутно искључивале са мреже уколико би напон мреже опао испод 80 % од номиналне вриједности напона. Вјетротурбине су биле осјетљиве на пропаде напона, а при наведеном начину искључивања генератора, нарушава се стабилност ЕЕС. Почетком 2003. године, ријешен је наведени проблем тренутног искључивања генератора са мреже уколико пропад напона траје релативно кратко, односно, користи се ”нисконапонска вожња”, односно, LVRT (*eng. low voltage ride through* - врло често се користи и израз FRT - *eng. fault ride through*) карактеристика искључења генератора [6]. Велики број држава у свијету има дефинисана правила о погону преносних и дистрибутивних мрежа. У ова правила се убрајају ЛВРТ захтјеви који се односе на то да вјетропарк остане у погону и при сниженим вриједностима напона. У наставку текста размотрени су њемачки, ирски и дански LVRT захтјеви за прикључење вјетропарка на мрежу.
На слици 2. дати су њемачки LVRT захтјеви. По Њемачком правилнику, вјетропарк може остати прикључен на мрежу 150 ms, чак у случају да напон на мјесту прикључења падне на вриједност од нула волти.

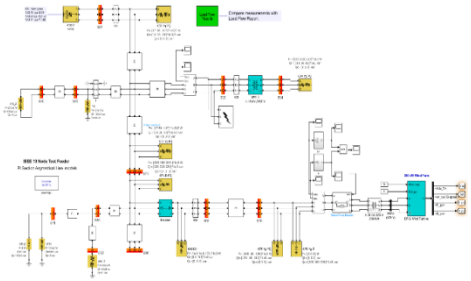
Слика 2. LVRT захтјеви правилима о раду дистрибутивних мрежа Њемачке [7]

По ирском правилнику на мјесту прикључења на мрежу, напон вјетропарка ни у једном тренутку не смије пасти испод 15 % од номиналне вриједности. У супротном долази до искључења [8].

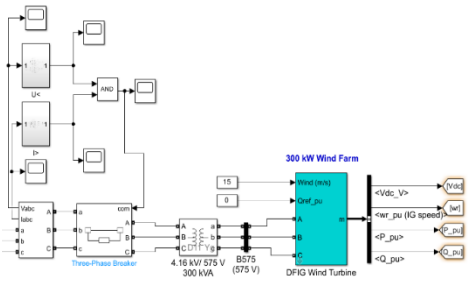
Код данских захтјева када напон на мјесту прикључења вјетропарка опадне до 15% номиналног напона, тада вјетропарк остаје прикључен на мрежу првих 100 ms. За временски период од 100 ms до 1000 ms, вријеме останка вјетропарка у погону расте линеарно са повећањем напона од 15% до 75% номиналног напона. Ако се напон повећа изнад 75% номиналног напона, послије 10 секунди, вјетропарк остаје трајно у погону [9].

6. РЕЛЕЈНА ЗАШТИТА ВЈЕТРОЕЛЕКТРАНА

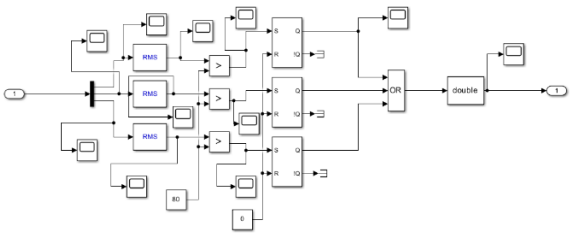
Симулиран је трополни кратак спој са земљом у чвору 633.



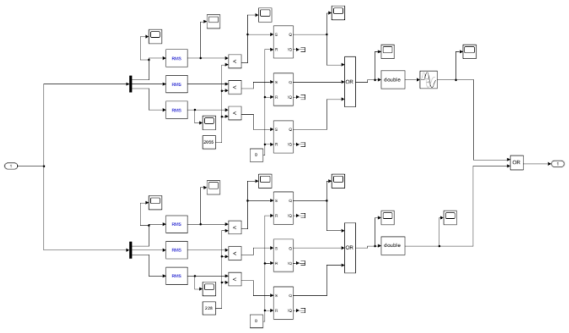
Слика 3. Модел мреже и вјетроелектране



Слика 4. Модел релејне заштите и вјетроелектране

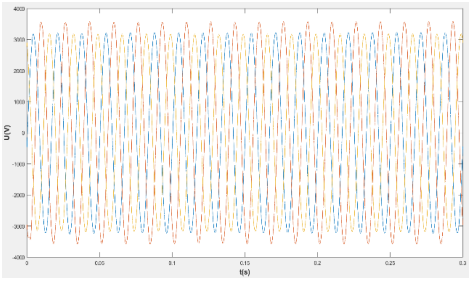


Слика 5. Струјни релеј



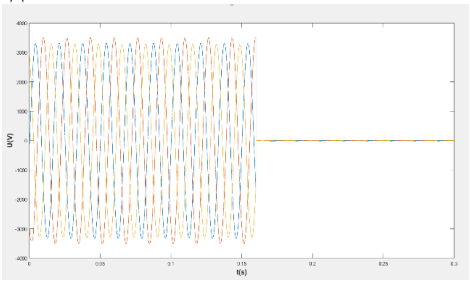
Слика 6. Напонски релеј

На овим сликама је приказан струјни и напонски релеј. У релејима се налази PMC блок одакле можемо да видимо ефективну вриједност струје и напона. Струјни релеј је подешен тако да у тренутку квара у било којој фази на излазу одмах даје логичку јединицу. Вриједност заштите је постављена на 80 A, а вријеме реаговања ове заштите је тренутно. Напонски релеј је подешен по LVRT карактеристици и има два степена дјеловања заштите. Први случај је да у тренутку квара, када напон падне на 90% од ефективне вриједности имамо временско затезање од 0,02 s и релеј на излазу даје логичку јединицу. Други случај је ако напон падне на 10% од ефективне вриједности релеј тренутно реагује. Коначан услов је да добијемо логичку јединицу из оба релеја и тада прекидач отвара своје контакте.



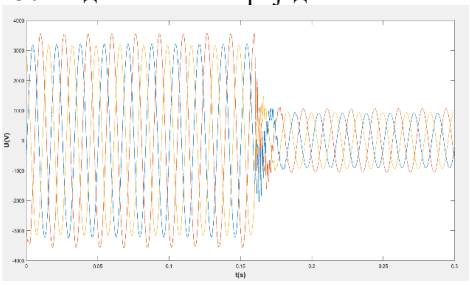
Слика 7. Напон на мјесту прикључења електране

На слици 7. приказана су мјерења напона на мјесту прикључења електране на мрежу прије квара. Видимо да су напони симетрични и да достижу вриједности од 3000 V до 3500 V.



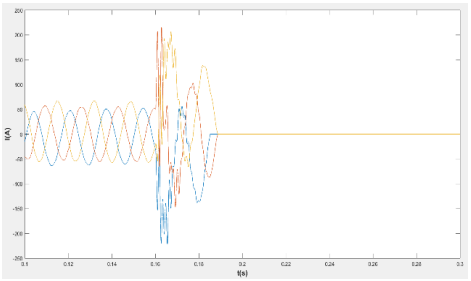
Слика 8. Напон на мјесту квара

На слици 8. видимо напон на мјесту квара. До квара је дошло у 0.16-oj секунди гдје видимо да је напон пао на нулту вриједност. На следећој слици приказан је напон на мјесту прикључења електране у тренутку квара. Са слике је уочљиво да је вриједност напона након квара пала на 30% од номиналне вриједности напона.

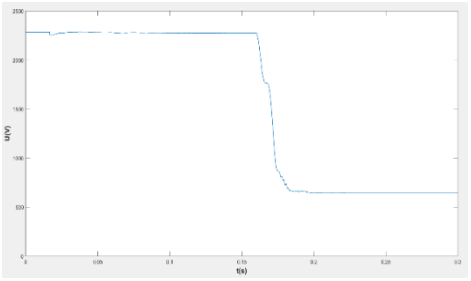


Слика 9. Напон на мјесту прикључења електране у тренутку квара

На наредној слици видимо да струја на мјесту прикључења електране у тренутку квара почиње да расте и достиже вриједности од око 200 A.

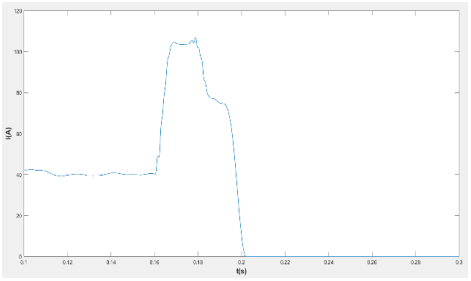


Слика 10. Струја на мјесту прикључења електране у тренутку квара



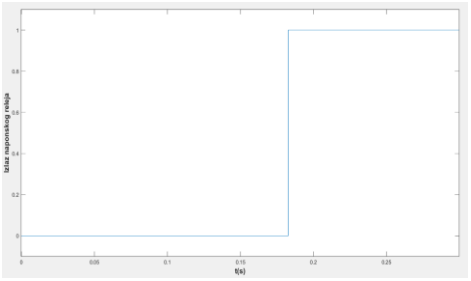
Слика 11. РМС напона

Ефективна вриједност напона је око 2300 V. У тренутку квара напон пада на вриједност од 650 V.

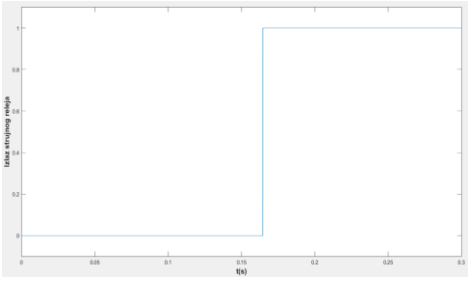


Слика 12. РМС струје

На слици 12. видимо да је ефективна вриједност струје око 40 А. Струјна заштита је постављена тако да дјелује на два пута већу вриједност од номиналне струје. Видимо да струја достише вриједност од 80 А у 0,16-ој секунди.



Слика 13. Излаз напонског релеја



Слика 14. Излаз струјног релеја

На овим сликама видимо излазе напонског и струјног релеја. Лако је уочљиво да напонски релеј има временско затезање од 0,02 s, након чега долази до реаговања заштите.

7. ЗАКЉУЧАК

У овом раду представљене су ветроелектране, као и начини рада заштитне опреме. Описане су основне шеме релејне заштите које се користе и у савременим системима за конверзију енергије вјетра. Описана је структура мреже вјетропарка, као и конфигурациија релејне заштите која се користи у дистрибутивној мрежи. Детаљно је описана релејна заштита вјетропарка и потенцијални изазови. Испитано је понашање система у случају трополног кратког споја са земљом са прикљученом вјетроелектраном на постојећу дистрибутивну мрежу. Квар је постављен на једној локацији и посматрани су напони и струје на мјесту квара и на мјесту прикључења електране на мрежу. Иако је квар удаљен од наше електране, лако је уочљиво да долази до већег пада напона на самом мјесту прикључења. За разматрани случај наглашена је потреба електричне заштите ротора да усљед кракторајног пада напона искључује вјетрогенератор са мреже, усљед чега може доћи до каскадог искључивања осталих генератора у ЕЕС. Уз кооперацију релејне заштите вјетрогенератора са LVRT захтјевима мреже ријешен је проблем стабилности и некоректног дјеловања заштите при краткотрајним падовима напона, што је описано у симулацији модела, И модел је радио у складу са LVRT. Како се повећава продор ветроелектрана у наш систем, изазови и заштитна разматрања се настављају развијати.

8. ЛИТЕРАТУРА

[1] ЖељкоР. Ђуришић „Вјетроелектране“, Академска мисао, Београд, 2019.

[2] Wind Energy Handbook, Second edition, Tony Burton, Wind Energy Consultant, Powys, UK, 2011.

[3] Wind Turbine Technology, Fundamental Concepts of Wind Turbine Engineering Second Edition, David A. Spera, 2009.

[4] Д. Бекут, „Релејна заштита“, Факултет техничких наука, Нови Сад, 2009.

[5] Wind Energy Explained, Theory, Design and Application, Second Edition, J.F. Manwell, J.G. McGowan, A.L. Rogers, USA, 2009.

[6] Tamer A. Kawady, Naema M. Mansour and Abdel-Maksoud I. Taalab, “Wind Farm Protection Systems: State of the Art and Challenges”, 2010, dostupno na: https://www.researchgate.net/publication/221907529_Wind_Farm_Protection_Systems_State_of_the_Art_and_Challenges.

[7] BDWE Bundesverband der Energie und Wasserwirtschaft e.V.: "Guideline for generating plants’ connection to and parallel operation with the medium- voltagenetwork", 2008.

[8] Distribution System Operators – ESB Networks, ‘Irish Distribution Code’, 2015.

[9] M. Tsili, S. Papathanassiou: "A Review of Grid Code Technical Requirements for Wind Farms", IET Renew. Power Gen., 2009, Vol. 3, No. 3, pp. 308–332, 2009.

Кратка биографија:

Немања Радић рођен је 1998. године у Добоју. Средњу школу – Гимназију Јован Дучић завршио је у Добоју 2017. године. Факултет техничких наукаписао је школске 2017/2018. године. На студијама се определио за смер Електроенергетика – Електроенергетски системи где је и дипломирао 2022. године Мастер студије уписао је 2022/2023 школске године.
Контакт: nradic11@gmail.com

Александар М. Станисављевић рођен је у Београду 1988. год. Дипломирао је и одбранио мастер рад на Факултету техничких наука у Новом Саду, 2011. и 2012. год., респективно. Од 2012. год. је на Факултету техничких наука као истраживач приправник. На истом факултету, одбранио је докторску дисертацију 2019. год. где је затим изабран је у наставно звање доцента. Од 2024. године је у звању вандредни професор.

Зборник радова Факултета техничких наука, НовиСад

УДК: 621.39
ДОИ: https://doi.org/10.24867/34BE38Lukac

Анализа и експериментална реализација система оптичких бежичних комуникација

Analysis and Experimental Implementation of Optical Wireless Communication systems

Немања Лукач, *Факултет техничких наука, Нови Сад*

Студијски програм – ЕНЕРГЕТИКА, ЕЛЕКТРОНИКА И ТЕЛЕКОМУНИКАЦИЈЕ

Кратак садржај – *У раду је представљена анализа и експериментална реализација оптичких бежичних комуникација са посебним освртом на примену видљиве светлости као преносног медијума. Рад је фокусиран на реализацију једноставног VLC система заснованог на OOK модулацији, коришћењем SDR уређаја USRP за физички слој комуникације и GNU Radio алата за генерисање и обраду сигнала.*
Кључне речи, *VLC, Интернет ствари USRP, GNU Radio*

Abstract – *This paper presents an analysis and experimental implementation of an Optical Wireless Communication system, with a specific focus on the application of Visible Light Communication as a transmission medium. Paper focuses on the implementation of a simple VLC system based on OOK modulation, using the USRP SDR device for the physical communication layer and the GNU Radio tool for signal generation and processing.*

Keywords: *VLC, Internet of Things, USRP, GNU Radio*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је била др Милица Петковић, доцент.

1. УВОД

Растућа потражња за капацитетом мобилних мрежа, коју покрећу апликације Интернета ствари (енг. *Internet of Things* – IoT) и проширена/виртуелна реалност (AR/VR), резултовала је потребом за развојем 5G и будућих 6G мрежа. 6G бежични комуникациони системи се очекују да подрже апликације Интернета свега (енг. *Internet of Everything* – IoE) и омогуће интеграцију различитих мрежа, укључујући копнене и некопнене. Технологија оптичких бежичних комуникација (енг. *Optical Wireless Communications* – OWC) представља економичну и перспективну допуну постојећим радиофреквентним (енг. *Radio Frequency* - RF) бежичним системима услед експоненцијалног пораста интернет саобраћаја. У овом раду извршена је практична имплементација једног система базираног на видљивој светлости (енг. *Visible Light Communication* – VLC) и његова анализа.

2. OWC КОМУНИКАЦИЈЕ

Као допуна постојећим RF бежичним системима, OWC технологија представља економично и перспективно решење за пренос података великог протока (до 30 Gb/s), које има потенцијал да постане један од водећих кандидата за наредну генерацију широкопојасног бежичног приступа, са циљем превазилажења изазова „последње миље“ и „последњег крака“ у приступним мрежама [1]. Овај потенцијал произилази из низа предности OWC технологије, као што су: одсуство потребе за лиценцирањем спектра; готово неограничена ширина спектра, што омогућава изузетан капацитет и подршку апликацијама високих брзина попут VLC чија је ширина спектра знатно већа од RF опсега; могућност остваривања домета од неколико метара до чак 5 km; енергетска ефикасност и еколошка прихватљивост захваљујући малој потрошњи енергије, смањеној интерференцији и отпорности на фединг; висока скалабилност и могућност реконфигурације; повећан ниво безбедности и приватности, јер је оптички сноп ограничен унутар одређеног простора, што смањује ризик од прислушкивања. Ове технологије су комплементарне традиционалним RF решењима и заједно чине основу за хетерогене комуникационе мреже будућности, омогућавајући висококвалитетне сервисе и апликације [2].

3. ПОДЕЛА OWC

OWC је кључна технологија за испуњавање експлозивно растућих захтева за капацитетом и брзином преноса података у еволуцији 5G и 6G комуникационих система. Четири главне OWC технологије, VLC, светлосна комуникација (енг. *Light Fidelity* – LiFi), оптичке комуникације путем камера (енг. *Optical Camera Communication* – OCC) и оптичка комуникација слободним простором (енг. *Free Space Optical communication* – FSO), представљају перспективна решења која могу испунити захтеве 5G/6G комуникационих система. Са аспекта инфраструктуре, оне се међусобно разликују по врсти

предајника, пријемника и комуникационом медијуму [3].
VLC користи LED диоде као предајнике у нерегулисаном спектру видљиве светлости (380–780 nm), нудећи изузетно велики пропусни опсег и потенцијал за брзине реда терабита по секунди у затвореном простору [3].
LiFi педставља напредну VLC технологију фокусирану на успостављање двосмерних мрежних решења за више корисника у затвореном простору, пружајући брз и сигуран приступ за системе у 6G ери [3].
OCC користе стандардне камере (попут CMOS камера у паметним телефонима) као пријемнике за хватање сигнала емитованих помоћу LED диода, што је економично, али ограничава брзину преноса због фреквенције кадрова [3].
FSO користи инфрацрвене (IR) ласере као предајнике за успостављање висококапацитетних линкова на великим даљинама, што га чини кључним за терестријалне везе и комуникацију између сателита [3].

4. GNU RADIO

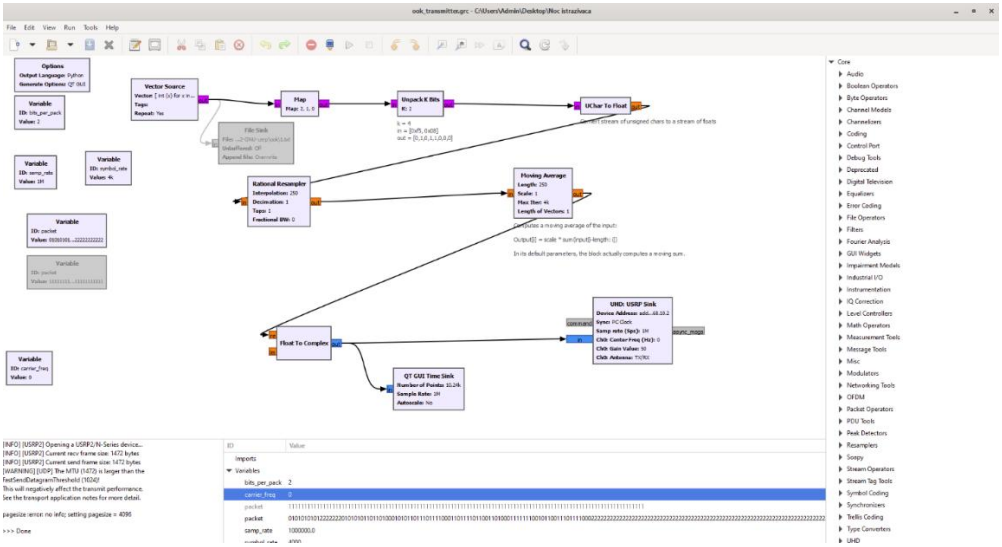
GNU Radio је програм који пружа блокове за обраду сигнала ради имплементације софтверски дефинисаних радио система (енг. *Software Defined Radio* – SDR). У пракси, то значи да корисник не мора да дизајнира све хардверске компоненте (као што су интегрисана кола за демодулацију, филтрирање или синхронизацију). Уместо тога, системи могу да се реализују софтверски, на комерцијално доступним рачунарима, уз евентуалну подршку периферијског RF хардвера. Ова флексибилност омогућава истраживачима, академској заједници и хобистима да прототипирају комуникационе системе, мере перформансе, интегришу нове модулације или канале, и на тај начин резултује у бржем развоју и експериментисању него код класичних радио решења. Архитектонски, GNU Radio нуди модуларни приступ: корисник гради „*flowgraph*“, граф блокова који представљају филтере, демодулационе јединице, модулације, визуелне слајсове и друге елементе обраде сигнала. GNU Radio такође подржава два главна режима: режим са хардвером и режим без хардвера (симулациони). На пример, може да се искористи за изучавање LiFi/VLC комуникација, интеграцију са 5G/6G протоколима, реализацију нових модулационих шема, мерење перформанси канала, тестирање прототипова у лабораторијама и слично [4].

5. ОПРЕМА

За реализацију практичне симулације VLC комуникације коришћена је комбинација специјализованог хардвера и софтверског алата GNU Radio, који је служио за обраду и управљање сигналом. Централни хардверски елемент био је USRP (енг. *Universal Software Radio Peripheral* - USRP), SDR уређај који функционише као пријемник и предајник, садржи D/A и A/D конверторе и повезује се са рачунаром путем Ethernet кабла. На предајној страни коришћена је LED лампа произвођача *Thorlabs* (модел M780LP1, 780 nm, 800 mW) са носачем SM1U25-A, чијим излазним светлосним сигналом је управљао мануелни драјвер (*Thorlabs*), омогућавајући ручну контролу модулације у струјном опсегу од 200 mA до 1200 mA. На пријемној страни, светлосни сигнал прихвата фотодетектор, такође произвођача *Thorlabs*, који је повезан са USRP-ом и омогућава механичко подешавање добитка (*gain*) израженог у децибелима.

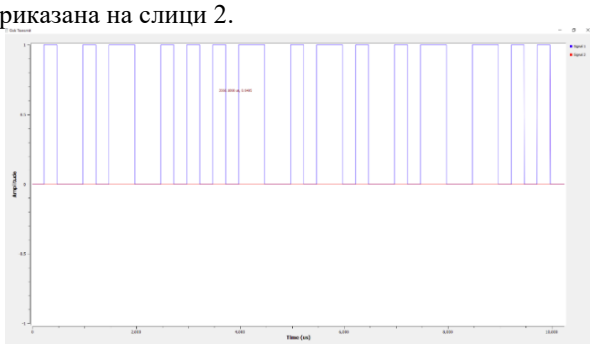
5.1. ПРЕДАЈНИК

Предајник користи GNU Radio као логички део система који говори SDR-у које инструкције треба да изврши. Користи USRP као уређај који служи за пренос података као и LED лампу која шаље сигнал ка пријемнику. USRP се повезује са рачунаром преко Ethernet порта. Такође имамо и драјвер који је повезан са USRP-ом и LED лампом. Блок шема предајника дата је на слици 1.



Слика 1. Блок шема предајника у GNU Radio-у

Блок „*Options*“ дефинише метаподатке пројекта (наслов, аутор, ID) и омогућава генерисање кода у Python-у. Параметар „*Generate Options*“ подешен је на QT GUI за графички приказ тока извршавања.
Блокови „*Variable*“ чувају кључне системске промењљиве без графичког интерфејса, као што су „*samp_rate*“, „*symbol_rate*“, „*bit_per_pack*“, „*packet*“ и „*carrier_freq*“.
Блок „*Vector Source*“ генерише низ правоугаоних импулса, представљајући секвенцу нула и јединица која се континуирано понавља. OOK модулација је имплементирана представљањем бинарних вредности различитим ширинама импулса.
Блокови „*Map*“ и „*Unpack K Bits*“ служе за пресликавање података и издвајање појединачних битова.
Блок „*UChar To Float*“ конвертује податке из типа карактер (*char*) у реалне бројеве (*float*).
Rational Resampler мења брзину одабирања улазног сигнала помоћу FIR филтра.
Блок „*Moving Average*“ израчунава просек улазних података.
Блок „*Float To Complex*“ врши конверзију реалних вредности (*float*) у комплексне (*complex*) ради припреме сигнала за USRP обраду.
Кључни блок је „*UHD: USRP Sink*“, који прослеђује узорковани сигнал ка USRP уређају за емитовање. Добитак (*gain*) је подешен на 50, а antena на TX/RX порт.
Блок „*QT GUI Time Sink*“ омогућава визуелну анализу емитоване секвенце у временском домену и она је приказана на слици 2.

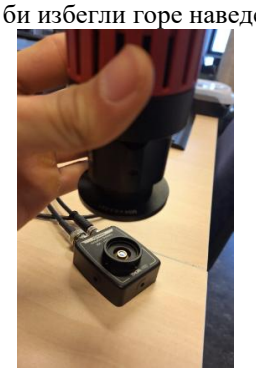


Слика 2. Изглед послатог сигнала

Правоугаони импулси шаљу се са предајника уз помоћ SDR, драјвера и LED лампе. LED лампа треба да генерише довољно јаку светлост коју ће фотодетектор на пријемнику примити и прочитати. Пријемник треба да ове сигнале реконструише што тачније могуће.

5.2. КОМУНИКАЦИЈА

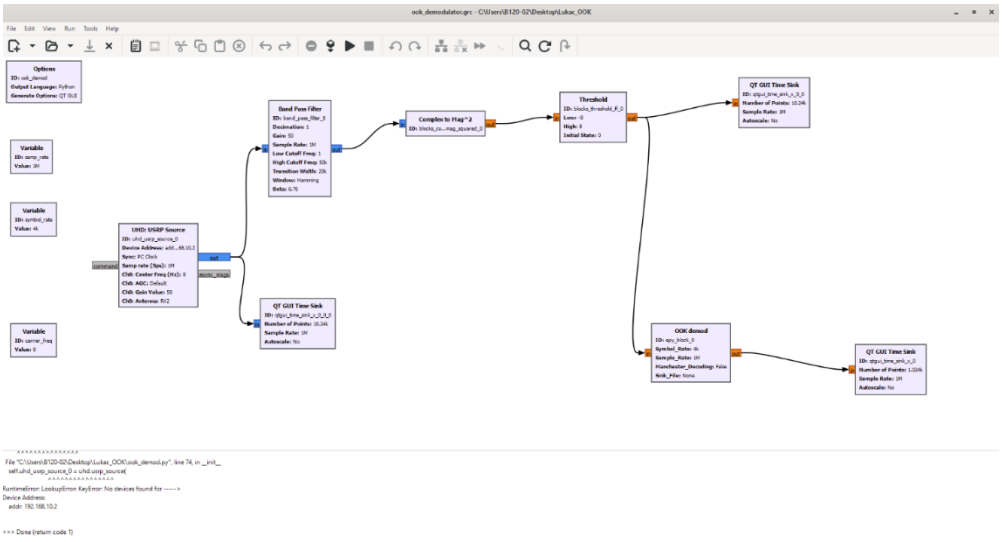
Слика 3 илуструје комуникацију између фотодетектора и LED лампе. Највећи изазов ове комуникације је наћи право растојање између ова два уређаја. Ако су преблизу, фотодетектор неће бити у могућности да прими послати сигнал и добиће се само шум, док ако су предалеко сигнал на фотодетектору биће преслаб и нећемо моћи успешно да рекоунструишемо послати сигнал. Такође велики проблем овог типа комуникације је спољашњи шум (светлост у просторији) који може дати погрешне вредности. Жељено растојање је свега неколико центиметара, да би избегли горе наведене проблеме.



Слика 3. Приказ комуникације LED лампе и фотодетектора

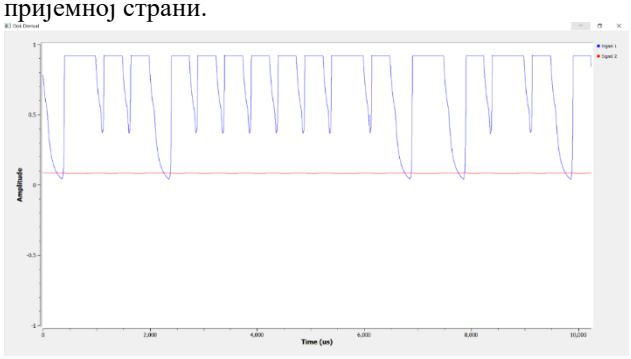
5.3. ПРИЈЕМНИК

Пријемник је реализован на сличан начин као и предајник, с тим што уместо LED лампе и драјвера имамо фотодетектор. Блок шема пријемника дата је на слици 4.



Слика 4. Блок шема пријемника у GNU Radio-у

Блокови „*Options u Variable*“ имају идентичну улогу као код предајника.
Блок „*UHD: USRP Source*“ прима сигнал са USRP хардвера. Добитак је подешен на 50, а antena на RX2 порт.
Блок „*Band Pass Filter*“ пропушта фреквенције унутар одређеног опсега. Користи FIR филтар са *Hamming* прозором, а добитак је постављен на 50.
Блок „*Complex to Mag^2*“ израчунава квадрат величине (*magnitude*) сваког комплексног узорка.
Блок „*Threshold*“ тестира улазни сигнал у односу на горњу (*high*) и доњу (*low*) вредност прага. Кључан за смањење шума и бољу реконструкцију сигнала, чиме се излаз подешава на један или нула.
Блок „*OOK Demod*“ врши демодулацију сигнала како би се на излазу добио сигнал што ближи послатом. *Manchester* декодовање је постављено на *False*.
На слици 5. приказан је реконструисан сигнал на пријемној страни.



Слика 5. Изглед рекоунстрисаног сигнала

Праг помаже у склањању дела шума и због тога имамо доста добру реконструкцију примљеног сигнала из ког можемо јасно видети када је послата јединица а када нула. Највећи изазов представља проналажење одговарајућег одстојања између LED лампе и фотодетектора.

6. ЗАКЉУЧАК

Експериментална реализација је потврдила могућност поузданог преноса података путем VLC технологије користећи GNU Radio и расположиву опрему, доказујући применљивост OWC метода у контролисаним условима. Међутим, уочена су значајна ограничења. Растојање представља највеће ограничење за стабилну комуникацију и ограничено је на неколико центиметара. Фотодетектор је такође показао осетљивост на засићење при малом растојању. Значајан је утицај амбијенталног осветљења, што доводи до повећаног шума и деградације сигнала. Ова ограничења указују на потребу за даљом оптимизацијом пријемног дела система и применом метода за побољшање отпорности на шум, али постигнути резултати потврђују да OWC технологије имају значајан потенцијал за будуће комуникационе системе, посебно у погледу високе пропусности, безбедности и отпорности на електромагнетне сметње.

7. ЛИТЕРАТУРА

[1] D. Borah, A. Boucouvalas, C. Davis, S. Hranilovic, and K. Yiannopoulos, “A review of communication-oriented optical wireless systems,” EURASIP J. Wireless Commun. Netw. vol. 1, no. 1, pp. 91:1–91:28, Mar. 2012.

[2]A. Mahdy and J. S. Deogun, “Wireless optical communications: A survey,” in Proc. IEEE WCNC, 2004, pp. 2399–2404.

[3] Z. Ghassemlooy , S. Arnon, M. Uysal, Z. Xu, and J. Cheng, “Emerging Optical Wireless Communications-Advances and Challenges”, J. Sel. Areas Commun., vol. 33, no. 9, pp. 1738–1749, 2015.

[4] Интернет страница: https://wiki.gnuradio.org/index.php?title=What_Is_GNU_Radio (приступљено у октобру 2025.)

Кратка биографија:

Немања Лукач рођен је у Новом Саду 2001. год. Дипломски рад на Факултету техничких наука одбранио је 2024. год. из области Информационо-комуникационе технологије. Од 2025. год. је запослен у звању сарадника у настави, на Катедри за телекомуникације и обраду сигнала, Департман за енергетику, електронику и телекомуникације.
Контакт:
nemanjalukac01@gmail.com

Зборник радова Факултета техничких наука, Нови Сад

УДК: 621.31
ДОИ: https://doi.org/10.24867/34BE39Stajsic

Утицај конфигурације намотаја на хармонијски састав индукованог напона хидрогенератора

Influence of winding configuration on the harmonic composition of the induced voltage of a hydrogenerator

Сергеј Стајшић, Дејан Јеркан, *Факултет техничких наука, Нови Сад*

Студијски програм – Енергетика, електроника и телекомуникације

Кратак садржај – *У раду је анализиран утицај конструкције намотаја на хармонијски састав индукованог напона хидрогенератора. Детаљно је приказана конструкција хидрогенератора, као и основни појмови који се односе на намотаје, магнетопобудну (МПС) и електромоторну силу (ЕМС). Разматрана је метода коначних елемената која се користи за анализу магнетских појава у машини, као и појам виших хармоника и њихових показатеља. Спроведена је анализа машине код које се у спектру индукованог напона јављају нежељени хармоници, након чега је предложена корекција корака намотаја статора. Извршене симулације показале су да предложена измена доводи до побољшања магнетског састава и радних перформанси машине.*

Кључне речи: *Хидрогенератор, метода коначних елемената, електромоторна сила, magnetopobudna sila, намотаји, хармонијско изобличење,*

Abstract – *This paper analyzes the influence of winding design on the harmonic composition of the induced voltage in a hydrogenerator. The construction of the hydrogenerator is presented in detail, along with the fundamental concepts related to windings, magnetomotive force (MMF), and electromotive force (EMF). The finite element method is applied to analyze magnetic phenomena in the machine, as well as the occurrence and indicators of higher harmonics. A case study was conducted on a machine exhibiting undesired harmonic components in its voltage spectrum. A correction of the stator winding pitch was proposed, which improved the machine's harmonic response. The effectiveness of the proposed modification was verified through simulation results.*

Keywords: *Hydrogenerator, Finite elements method, electromotoive force, magnetomotive force ,windings, harmonic distortion*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Дејан Јеркан, вандредни професор

1. УВОД

Хидрогенератори (ХГ) представљају окосницу производње електричне енергије у многим електроенергетским системима (ЕЕС) широм света. Њихова примарна улога је конверзија механичке енергије хидрауличне турбине у електричну енергију, а одликује их поузданост, дуг радни век и, у односу на друге технологије, знатно боља флексибилност за брзо покретање и регулацију снаге.

Слика 1. Ротор хидрогенератора

Иако су ХГ пројектовани за рад у идеалном синусном режиму, услед неидеалности магнетног кола (жлебови у статору и ротору) и засићења феромагнетног материјала, долази до деформације магнетског поља и, последично, појаве виших хармоника у индукованом напону. Ово хармонијско изобличење нарушава квалитет електричне енергије и изазива низ негативних појава.

Кључно је да се нежељена појава, која се квантификује преко укупне хармонијске дисторзије (THD), минимизује.

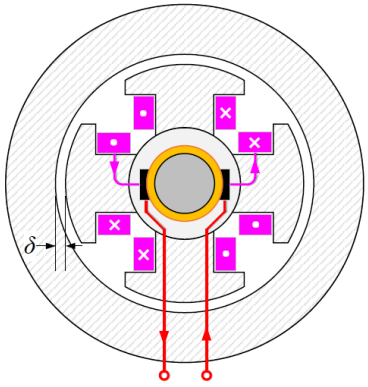
Циљ овог рада је да се детаљном анализом, применом софтвера који имплементира методу коначних елемената, испита утицај скраћења навојног корака на хармонијски састав индукованог напона хидрогенератора. Разматрају се резултати симулација машине код које се јавља хармонијско изобличење, након чега се предлаже и доказује корекција која доводи до побољшања квалитета индукованог напона.

2. ХИДРОГЕНЕРАТОРИ

2.1. Конструкција

Статор свих машина наизменичне струје конструише се од ламинираног феромагнетног језгра са жлебовима, што је неопходно ради смањења губитака услед вртложних струја. У жлебове се смештају активни проводници статорског намотаја.

Хидрогенератори, као синхроне машине, користе ротор са истакнутим половима и великим пречником, прилагођен малим брзинама обртања хидрауличних турбина. Због тога морају имати велики број полова да би постигли стандардну мрежну фреквенцију. Ротор садржи побудни намотај (за стварање магнетног поља) и пригушни намотај (за стабилизацију при поремећајима).



Слика 2. Синхрона машина са истакнутим половима [3]

Намотај статора је најчешће трофазни и расподељен (проводници су у већем броју жлебова), јер се тиме постиже да резултујућа магнетопобудна сила (МПС) буде што ближа идеалном синусоидалном облику. Поред расподеле, кључна техника је скраћивање навојног корака (тетивно намотавање). Коришћење ових техника доводи до смањења укупне индуковане електромоторне силе (ЕМС), што се у прорачунима корегује увођењем навојних сачиниоца:

1. Тетивни навојни сачинилац – описује смањење ЕМС услед скраћивања корака.
2. Појасни навојни сачинилац – описује смањење ЕМС због просторне расподеле намотаја у више жлебова.

Оба сачиниоца, у комбинацији, одређују укупни навојни сачинилац потребан за прецизан прорачун стварне ЕМС машине.

2.2. МПС расподељеног намотаја

Код машина наизменичне струје, није прихватљива правоугаона расподела магнетопобудне силе (МПС), јер би такав облик изазвао појаву правоугаоне електромоторне силе (ЕМС) у проводницима статора, што није пожељно у пракси. Циљ је да облик ЕМС што више одговара синусоидном (простопериодичном).

Да би се то постигло, намотај се распоређује у већи број жлебова по унутрашњем ободу статора, што резултује расподељеним намотајем. Услед овакве конструкције, расподела МПС више није правоугаона већ добија степеничаст облик који се приближава синусоидном и назива се квазихармонична расподела.

Вредност магнетопобудне силе у појединим тачкама обода одређује се **Амперовим законом**, интегрисањем магнетног поља дуж затворених контура које обухватају различит број ампернавојака. На тај начин се добија просторна расподела МПС, која представља основу за анализу поља у машини.

Квазихармонична расподела магнетопобудне силе $F(\vartheta)$је периодична функција по угловној координати ϑ, па се може развити у Фуријеов ред:

$$F(\vartheta) = F_1 \sin(\vartheta) + F_3 \sin(3\vartheta) + F_5 \sin(5\vartheta) + \cdots \quad (1)$$

где су $F_1, F_3, F_5, \ldots$амплитуде појединих хармоничних компоненти.

Амплитуда хармоника вишег реда опада са редом ν, приближно као $1/\nu$, што значи да највећи утицај на облик МПС и ЕМС имају нижег реда хармоници (најчешће трећи, пети и седми). Управо ови хармоници представљају главни извор одступања од идеално синусног таласа индукованог напона, због чега се у конструкцији намотаја предузимају мере за њихово потискивање (попут скраћења корака намотаја или одговарајућег распореда проводника).

2.3. Расподела индукције и флукс по полу

Магнетски флукс Ф представља укупан број линија магнетне индукције које пролазе кроз дату површину. У ротационим машинама, због хармонијске расподеле индукције по обиму, проводници под једним полом налазе се у пољу различитог интензитета индукције B. Због тога се уводи средња вредност магнетне индукције B_{sr}, на основу које се дефинише флукс по полу:

$$\Phi_p = S_p \cdot B_{sr} = \tau_p \cdot l \cdot B_{sr} \quad (2)$$

где је τ_pполни корак, а lефективна дужина гвожђа.

Ако је расподела индукције синусоидна, флукс по полу може се изразити и преко максималне индукције B_m:

$$\Phi_p = S_p \cdot B_{sr} = \tau_p \cdot l \cdot B_{sr} \quad (3)$$

Ова величина представља кључни параметар за израчунавање ефективне вредности индукованог напона једне фазе:

$$E = 4{,}44 \cdot f \cdot N_a \cdot k_n \cdot \Phi_p \quad (4)$$

где је f фреквенција, N_a број навојака по фази, а k_nукупни навојни сачинилац.

Услед конструкције полова ротора, расподела магнетне индукције B у ваздушном зазору није идеално простопериодична. Та нехармонична расподела може се представити као сума основне хармоничне компоненте и низа виших хармоника, од којих сваки индукује одговарајућу компоненту електромоторне силе (ЕМС) у проводницима статора.

Најчешће примењив метод за побољшање облика индукованог напона и елиминацију нежељених хармоника јесте скраћење корака секције. Принцип је следећи: хармоник реда ν елиминише се када се навојни корак скрати према односу

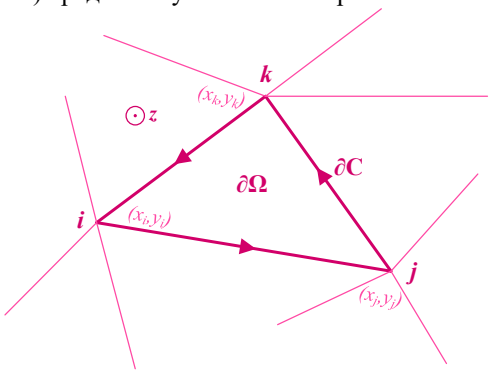
$$\frac{y}{\tau_p} = 1 - \frac{1}{\nu} \quad (5)$$

3. МЕТОДА КОНАЧНИХ ЕЛЕМЕНАТА

Метода коначних елемената, позната и као Finite Element Analysis (FEA), је нумеричко-графичка метода која се користи за прецизно решавање електромагнетских поља у доменима сложене геометрије, као што су савремене ротационе електричне машине.

Метода коначних елемената се заснива на Максвеловим једначинама које описују електромагнетно поље. За потребе анализе електричних машина, поље се најчешће посматра као квазистатичко (занемарује се утицај померајне струје), а за даљу формулацију се уводе потенцијали (магнетски вектор потенцијал А).

Суштина методе је у томе што се цела област од интереса (нпр. попречни пресек електричне машине) дели на мноштво мањих, дисјунктних делова који се називају коначни елементи (најчешће троуглови). Уместо решавања комплексних диференцијалних једначина у целом континуалном домену, методом коначних елемената се решава вредност електромагнетских величина (првенствено магнетског вектор потенцијала) само у чворовима (теменима) ових елемената. Вредност унутар самог елемента се затим добија једноставном интерполацијом (најчешће линеарном) вредности у његовим чворовима.



Слика 3. Коначни елемент у облику троугаоног сегмента [2]

Овим поступком, континуални проблем се претвара у систем алгебарских једначина који се може решити на рачунару.

4. ВИШИ ХАРМОНИЦИ У ЕЛЕКТРОЕНЕРГЕТСКИМ СИСТЕМИМА

Савремени електроенергетски системи све више су изложени појави сложеноперидичних радних режима услед масовне примене уређаја енергетске електронике, који уносе значајне нелинеарности у систем. Присуство виших хармоника у напонима и струјама доводи до изобличења таласних облика, смањења енергетске ефикасности и појаве различитих негативних ефеката као што су прегревање трансформатора, мотора и неутралних проводника, поремећаји у раду мерних инструмената и заштитних уређаја, као и интерференције са телекомуникационим сигналима.

Квалитет електричне енергије уско је повезан са степеном одступања таласних облика напона и струја од идеалних синусоидних. За квантитативно оцењивање изобличења користе се стандардизовани показатељи као што су укупна и индивидуална хармонијска дисторзија (THD, HD), крест фактор и фактор снаге λ. Ови параметри дефинисани су међународним стандардима (попут IEEE-519) и омогућавају праћење утицаја хармоника на квалитет напајања.

Табела 1. Неки индикатори квалитета електричне енергије

Индикатор	Дефиниција	Главна примена
Укупна хармонијска дисторзија (THDU, THDI)	$\sqrt{\frac{\sum_{n=2}^{\infty} U_n^2}{U_1^2}}, \sqrt{\frac{\sum_{n=2}^{\infty} I_n^2}{I_1^2}}$	Описивање нивоа виших хармоника, стандарди
Индивидуална хармонијска дисторзија (HD U_n, HD I_n)	$\frac{U_n}{U_1}, \frac{I_n}{I_1}$	Описивање нивоа виших хармоника, стандарди
Фактор снаге (PF,λ)	$\frac{P_{tot}}{\lvert U_{eff}\rvert\lvert I_{eff}\rvert}$	Наплате реактивне и хармонијске снаге

5. СИМУЛАЦИЈЕ НА РАЗВИЈЕНОМ МОДЕЛУ

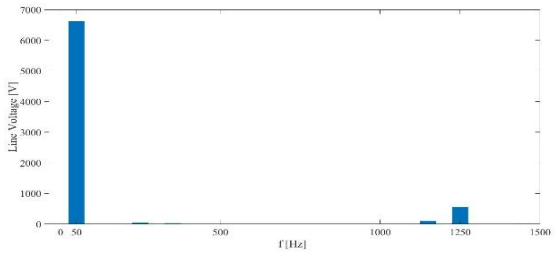
У овом поглављу ће се извршити анализа утицаја корекције статорског намотаја, односно скраћења навојног корака, на хармонијско изобличење индуковане електромоторне силе (ЕМС) у режиму празног хода. Као основа за анализу ће послужити модел хидрогенератора оригиналне конструкције и једна његова варијација изведена на нивоу симулационог модела, која представља модификацију намотаја са аспекта скраћења корака намотавања. Над моделима, креираним у програмском пакету Ansys, извршене су електромагнетске симулације којима се опонаша рад генератора у режиму празног хода при синхроној брзини обртања.

Табела 2. Каталошки подаци генератора

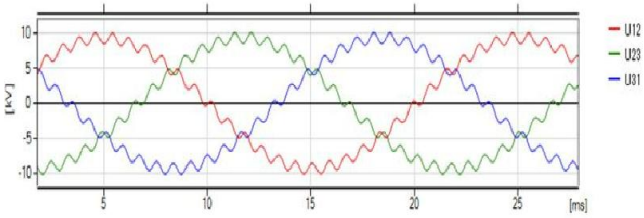
Подаци хидрогенератора	
Снага [kVA]	1583
Фреквенција [Hz]	50
Номинални напон [V]	6600
Номинална брзина обртања [rpm]	750
Број пари полова	4
Спољашњи пречник статора [mm]	1100
Дужина лим пакета [mm]	760
Број жлебова статора	96

Као одговор ових симулација добијају се вредности вектора магнетске индукције, које се користе за прорачун флуксних обухвата и хармонијског спектра индуковане ЕМС. На слици 4 приказан је хармонијски спектар индукованог линијског напона за модел

оригиналне конструкције хидрогенератора. Јасно се уочава доминантна компонента на основној фреквенцији (50 Hz), али и присуство значајне нежељене компоненте напона 25. хармоника (на фреквенцији 1250Hz).

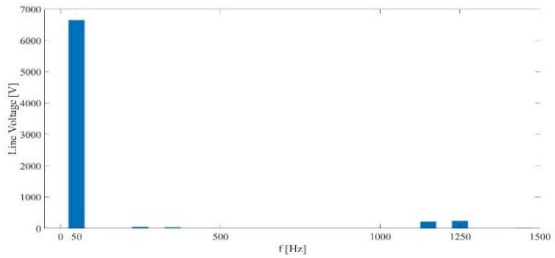


Слика 4. Хармонијски спектар индукованог линијског напона у режиму празног хода

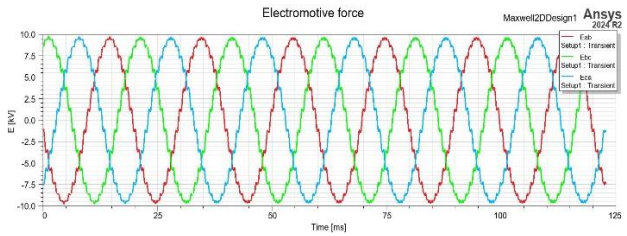


Слика 5. Таласни облик индукованог линијског напона у режиму празног хода

Да би се редуковала амплитуда 25. хармоника, предложено је кориговање корака намотавања статорског намотаја. Извршена је измена модела и симулација је поновљена. На слици 6 приказан је хармонијски спектар индукованог линијског напона за модел са коригованим кораком намотавања. Уочава се да је променом корака намотаја постигнута ефикасна редукција амплитуде 25. хармоника. Ова корекција је усклађена са теоријом о утицају тетивног навојног сачиниоца на више хармонике и представља конструкцијско решење за побољшање таласног облика индуковане ЕМС.



Слика 6. Хармонијски спектар индукованог линијског напона у режиму празног хода, након промене корака намотавања



Слика 7. Таласни облик индукованог линијског напона у режиму празног хода, након промене корака намотавања

6. ЗАКЉУЧАК

У овом раду детаљно је приказан утицај конструкције намотаја хидрогенератора на његове електромагнетне величине и квалитет индуковане електромоторне силе (ЕМС). Извршена је анализа хармонијског изобличења линијског напона, која је показала присуство значајног нежељеног 25. хармоника у режиму празног хода машине.

На практичном примеру, применом Методе коначних елемената у софтверском пакету Ansys, извршена је упоредна анализа оригиналне конструкције и модела са коригованим (скраћеним) кораком намотавања.

Установљен је директан и значајан утицај скраћења корака на редукцију амплитуде 25. хармоника. Овај конструктивни параметар показао се као кључно средство за побољшање чистоће таласног облика напона, што наводи на закључак да се о оптимизацији корака намотавања мора посебно водити рачуна у фази пројектовања и реконструкције синхроних машина, како би се задовољили критеријуми квалитета електричне енергије.

7. ЛИТЕРАТУРА

[1] С. Вукосавић, „*Електричне машине*“ , Универзитет у Београду, Електротехнички факултет, Академска мисао, Београд, 2010.

[2] Д. Јеркан, „*Динамички модел трофазне кавезне асинхроне машине заснован на методи коначних елемената*“, докторска дисертација, Факултет техничких наука, Нови Сад, 2016.

[3] Богдан М. Брковић, „*Основи електромагнетског прорачуна обртних машина за наизменичну струју*“, Универзитет у Београду, Електротехнички факултет, Катедра за енергетске претвараче и погоне, Београд, 2023.

[4] Веран Васић, „*Увод у електрине машине*“, Факултет техничких наука, Нови Сад, 2023.

[5] Radenko Wolf, „*Osnovi električnih strojeva*“, Školska knjiga zagreb, Zagreb, 1989.

[6] Нина Стефановић, „*Енергетски трансформатори у сложеноперiодичним режимима*“, мастер рад, Факултет техничких наука, Нови Сад, 2020.

Кратка биографија:

Сергеј Стајшић рођен је 2000. године у Сомбору. Факултет техничких наука уписао је школске 2019/2020. године. На студијама се определио за смер Електроенергетика – Енергетска електроника и електричне машине где је и дипломирао 2023. Године

Дејан Јеркан је ванредни професор на Факултету техничких наука у Новом Саду, на катедри за Енергетску електронику и претвараче. Област интересовања су му моделовање и дијагностика електричних машина као и метода коначних елемената.

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.38
DOI: https://doi.org/10.24867/34BE12Stefanov

MULTIFAKTORSKA AUTENTIFIKACIJA I KONTROLA PRISTUPA ZASNOVANA NA INTEGRACIJI SENZORA I BIOMETRIJE

MULTIFACTOR AUTHENTICATION AND ACCESS CONTROL BASED ON SENSOR INTEGRATION AND BIOMETRICS

Miljana Stefanov, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu predstavljen je dizajn multifaktorskog sistema za autentifikaciju i kontrolu pristupa, koji kombinuje senzore pokreta, biometriju i prepoznavanje glasa. Sistem omogućava dva nivoa verifikacije – PIN ili otisak prsta i prepoznavanje glasa – pre odobrenja pristupa ili aktiviranja alarma.*

Ključne reči: *Multifaktorska autentifikacija, verifikacija*

Abstract – *This paper presents the design of a multifactor authentication and access control system that combines motion sensors, biometrics, and voice recognition. The system provides two levels of verification – PIN or fingerprint, and voice recognition – before granting access or activating an alarm.*

Keywords: *Multifactor authentication, verification*

1. UVOD

Pojam bezbednosti je individualan i zavisi od potreba svakog pojedinca. Dok je nekima dovoljno da zaključaju vrata i ostave rezervni ključ komšiji, drugi se oslanjaju na napredna tehnološka rešenja. U prošlosti, kuće su čuvale životinje poput pasa, dok se danas sve više oslanjamo na moderne tehnologije i senzore. Vremenom, sa promenom društvenih i tehnoloških okolnosti, menja se i samo shvatanje termina "bezbednost".

Savremeni senzori omogućavaju praćenje doma u realnom vremenu i slanje obaveštenja u slučaju neuobičajene aktivnosti. Ovo rešenje doprinosi osećaju sigurnosti, kako u kućama tako i u stanovima, posebno za ljude koji nemaju želju ili mogućnost da drže životinje kao čuvare.

U ovom radu prikazan je primer implementacije sigurnosnog sistema za kontrolu ulaska u dom.

2. OPIS SISTEMA

Cilj ovog istraživanja je dizajn i implementacija sigurnosnog sistema za automatsko upravljanje vratima, koji omogućava višestepenu autentifikaciju korisnika.

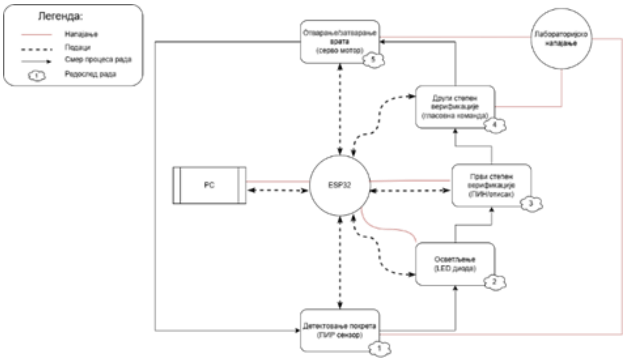
Fokus je na sigurnosti i efikasnosti kroz integraciju senzora i mikrokontrolera.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Jovan Bajić, vanr. prof.

Sistem omogućava pristup samo ovlašćenim korisnicima koristeći sledeće korake:

1. **Detekcija korisnika –** PIR senzor registruje pokret i aktivira LED diodu**.**
2. **Prvi stepen verifikacije** – Korisnik unosi PIN ili skenira otisak prsta.
3. **Drugi stepen verifikacije** – Aktivira se senzor za prepoznavanje glasa.
4. **Otvaranje vrata** – Ako su oba koraka uspešna, vrata se otvaraju; u suprotnom, aktivira se alarm i šalje obaveštenje preko Telegram aplikacije.
5. **Napajanje i kontrola** – Sistemom upravlja ESP32 mikrokontroler, dok laboratorijsko napajanje omogućava rad komponenti.

Blok šema koja se nalazi na slici broj 1, prikazuje strukturu sistema, uključujući linije napajanja, tok podataka i redosled aktivacije komponenti.



Slika 1. *Rezultati simulacije*

3. PREGLED KOMPONENTI SISTEMA

3.1. ESP32

ESP32 može označavati sam čip ili razvojnu ploču, koja je praktičnija za učenje i testiranje. Najčešće se koristi razvojne ploče, poput ESP32 DEVKIT DOIT, koje uključuju USB interfejs, regulatore napona i lako dostupne *GPIO* pinove. Izgled mikrokontrolera dat je na slici broj 2.

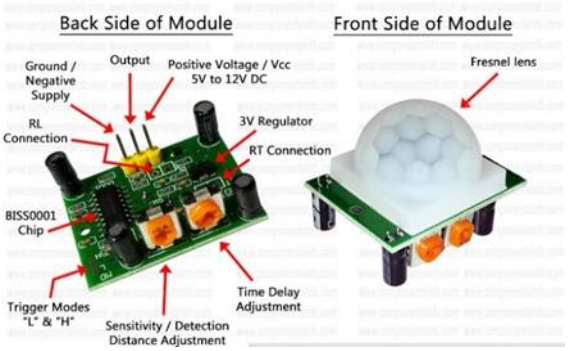
Slika 2. *ESP32 DEVKIT [1]*

Ovaj mikrokontroler ima dvostruko jezgro, integrisani *Wi-Fi* i *Bluetooth*, što ga čini idealnim za *IoT* projekte. Podržava različite komunikacione interfejse (*UART, SPI, I²C, PWM, ADC, DAC*) i omogućava efikasno upravljanje resursima. Njegova niska potrošnja energije (*deep sleep, light sleep režimi*) pogodna je za baterijski napajane uređaje.

ESP32 podržava razvojna okruženja poput *Arduino IDE*, *MicroPython* i *ESP-IDF*. Fleksibilni *GPIO* pinovi omogućavaju prilagođavanje projektima, uključujući promenu podrazumevanih *I²C* pinova (*GPIO* 21 – *SDA*, *GPIO* 22 – *SCL*). Zbog ovih karakteristika, ESP32 je jedno od najpopularnijih rešenja za automatizaciju, pametne uređaje i senzorske mreže.

3.2. *PIR* senzor

PIR senzor detektuje infracrveno zračenje koje emituju sva tela na temperaturama iznad apsolutne nule. Sastoji se od piroelektričnog senzora, koji registruje promene u infracrvenom spektru i Frenelovih sočiva, koja povećavaju domet i širinu vidnog polja. Prikazan je na slici broj 3.



Slika 3. *Izgled PIR senzora sa donje i gornje strane [2]*

Što se tiče podešavanja senzora, postoje dva potenciometra. Jedan potenciometar vezan je za osetljivost. Ukoliko se pomera u smeru kazaljke na satu onda se povećava osetljivost, suprotno se smanjuje. Drugi potenciometar vezan je za vremensko odlaganje, odnosno koliko dugo izlaz ostaje u visokom stanju nakon detekcije (1s-3min). Postoje i dva režima rada, *single* i *multiple trigger mode.* U projektu je izabran *single trigger mode.*

U ovom projektu, *PIR* senzor detektuje prisustvo osobe ispred vrata i aktivira *LED* diodu za osvetljenje. Kada se pokret registruje, sistem prelazi na sledeći nivo verifikacije korisnika.

3.3. *OLED* displej

OLED displej ZJY096I0400WG11 je ekran dijagonale 0,96 inča sa *I²C* interfejsom i rezolucijom 128x64 piksela. Izgled datog displeja dat je na slici broj 4.

Slika 4. *Izgled OLED displeja [3]*

Zahvaljujući tome što svaki piksel samostalno emituje svetlost, ima visok kontrast i malu potrošnju energije. U ovom radu koristi se za prikaz informacija korisniku – kao što su status sistema i rezultati verifikacije – čime omogućava jasan uvid u tok procesa autentifikacije. Komunikacija sa ESP32 mikrokontrolerom ostvaruje se putem *I²C* protokola, korišćenjem samo dve linije: *SDA* (za podatke) i *SCL* (za taktnu sinhronizaciju).

3.4. Tastatura

U ovom sistemu, 4×4 membranska tastatura predstavlja jednu od dve ponuđene metode za prvi stepen verifikacije. Na slici broj 5 prikazan je izgled iskorišćene tastature sa pripadajućim rasporedom pinova

Slika 5. *Izgled 4x4 мастатура и распоред пинова [4]*

Zbog svoje otpornosti na vlagu, masnoću i mehaničku pouzdanost, odabrana je umesto osetljivih *touch* ekrana, koji u realnim uslovima mogu da dovedu do grešaka pri unosu. Tastatura funkcioniše po principu presecanja redova i kolona: kada korisnik pritisne taster, zatvara se kontakt između određenog reda i kolone, što mikrokontroler prepoznaje putem programske logike koja sekvencijalno aktivira izlazne linije i očitava ulazne. Na osnovu aktivnog spoja, određuje se koji je taster pritisnut i taj unos se dalje koristi u procesu autentifikacije.

3.5. Senzor za skeniranje otiska prsta

Senzor za otisak prsta koristi se kao alternativa tastaturi za prvi stepen verifikacije korisnika. Na slici broj 6 prikazan je izgled korišćenog senzora.

Slika 6. *Izgled senzora za skeniranje otiska prsta [5]*

U pitanju je optički skener koji snima otisak i upoređuje ga sa prethodno sačuvanim šablonima radi potvrde identiteta. Karakteriše ga brz odziv (manje od 1 sekunde), kapacitet od 162 otiska i nizak procenat grešaka pri prepoznavanju. U ovom radu povezan je sa ESP32 mikrokontrolerom putem *TTL* serijske komunikacije i omogućava sigurnu, brzu i jednostavnu biometrijsku autentifikaciju korisnika.

3.6. Senzor za prepoznavanje fraza

U završnoj fazi verifikacije koristi se senzor za prepoznavanje fraza, čime se sistemu dodaje drugi

sigurnosni sloj – glasovna potvrda identiteta. Ugrađeni modul omogućava *offline* rad, bez potrebe za internet konekcijom i prepoznaje do 17 korisnički definisanih komandi. Izgled datog senzora dat je na slici broj 7.

Slika 7. *Izgled senzora za prepoznavanja fraza [6]*

Dati senzor je povezan sa ESP32 mikrokontrolerom putem *I²C* protokola, što omogućava jednostavno proširenje sistema bez zauzimanja velikog broja pinova. Zahvaljujući integrisanom zvučniku, korisniku se pruža povratna audio informacija, dok kompaktnost i pristupačnost modula čine ga pogodnim za upotrebu u pametnim sistemima kontrole pristupa.

4. POVEZIVANJE KOMPONENTI

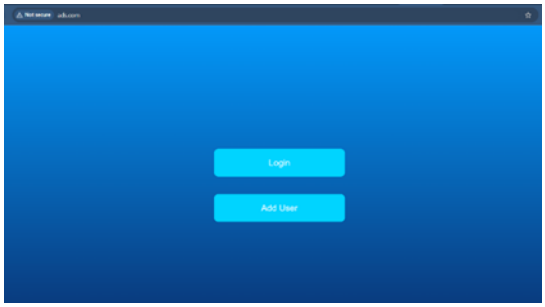
Za pravilno funkcionisanje sistema bilo je neophodno pažljivo definisati povezivanje svake komponente sa odgovarajućim *GPIO* pinovima na ESP32 mikrokontroleru. Sve komponente, uključujući senzore, tastaturu, displej i servo motor, imaju dodeljene pinove u skladu sa funkcionalnim zahtevima sistema. Posebno su konfigurisani *GPIO* 33 i *GPIO* 32 kao *SDA* i *SCL* linije za *I²C* komunikaciju, zahvaljujući fleksibilnosti ESP32 i biblioteci *Wire*, koja omogućava redefinisanje pinova. U tabeli 1 dat je pregled načina povezivanja iskorišćenih uređaja sa odgovarajućim *GPIO* pinovima.

Tabela 1. *Komponente i odgovarajući GPIO pinovi*

Uređaj	Pin na ESP32
Tastatura – redovi (R1, R2, R3, R4)	*GPIO* 13,12,14,27
Tastatura – kolone (C1, C2, C3, C4)	*GPIO* 26,25,15,2
***PIR* sensor**	*GPIO* 23
Servo motor	*GPIO* 18
Senzor otiska prsta (TX - RX)	*GPIO* 17 (RX2), *GPIO* 16 (TX2)
Senzor za prepoznavanje fraza (*I²C*)	*GPIO* 33 *(SDA), GPIO* 32 *(SCL)*
***OLED* displej (*I²C*)**	*GPIO 21 (SDA), GPIO 22 (SCL)*
***LED* dioda**	*GPIO* 5

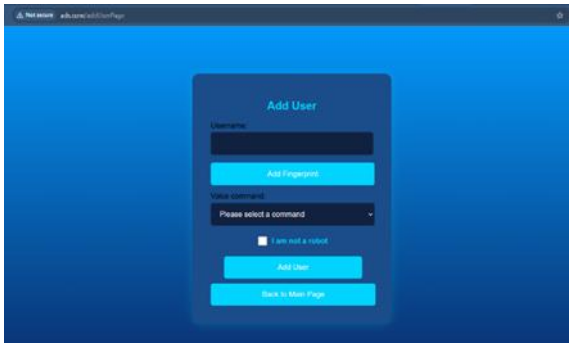
5. *WEB* STRANICA

Za potrebe upravljanja korisnicima i verifikacije identiteta, razvijen je jednostavan *web* interfejs koji omogućava lokalni pristup stranici putem *IP* adrese koju ESP32 dobija nakon povezivanja na mrežu. Pristupom početnoj stranici korisniku se nude dve osnovne opcije: prijava na sistem i kreiranje novog naloga i to je prikazano na slici broj 8.



Slika 8. *Glavni meni*

Na slici ispod, označenom pod brojem 9 prikazana je stranica za kreiranje naloga.

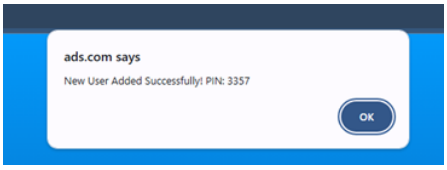


Slika 9. *Stranica za dodavanje novog korisnika*

Prilikom kreiranja naloga, korisnik unosi korisničko ime i registruje svoj otisak prsta kao jedan od načina verifikacije. Da bi unos bio validan, mora ispuniti određena pravila. Sistem automatski proverava da li već postoji korisnik sa unetim imenom i prikazuje poruku u slučaju neuspešnog unosa. Interfejs prikazuje sve faze registracije otiska prsta – od početnog očitavanja, preko validacije, do završetka procesa – uz jasan prikaz statusa i poruka korisniku. U sklopu registracije, korisnik bira i frazu iz ponuđene liste komandi koja se kasnije koristiti za glasovno prepoznavanje. Spisak fraza je dat na slici broj 10.

Slika 10. *Lista dostupnih komandi*

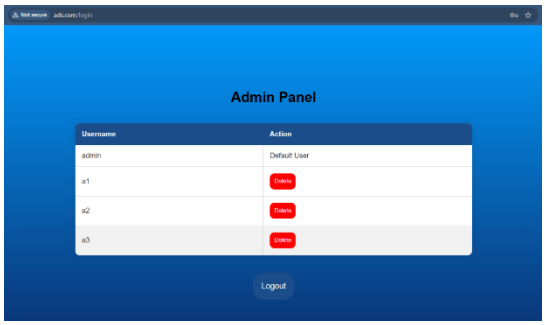
PIN se korisniku dodeljuje automatski nakon uspešne registracije, kako bi se obezbedila jedinstvenost i izbegle greške pri izboru. Kraj uspešne registracije prikazan je na slici broj 11.



Slika 11. *Uspešno dodat korisnik*

Pored opcije za kreiranje naloga, interfejs sadrži i deo za prijavu korisnika. Nakon uspešnog logovanja, korisnik biva preusmeren na odgovarajuću stranicu u zavisnosti od privilegija: administrativni panel za administratora ili korisnički prikaz za običnog korisnika.

Na administratorskoj stranici, prikazanoj na slici broj 12, prikazana je lista svih registrovanih korisnika sa mogućnošću njihovog brisanja. Ova funkcionalnost omogućava jednostavno upravljanje bazom korisnika.



Slika 12. *Izgled admin stranice*

Na korisničkoj stranici, prikazanoj na slici broj 13, vizuelno se prikazuje ponašanje sistema u realnom vremenu: kada *PIR* senzor detektuje pokret, ispisuje se vreme detekcije; kada se unosi *PIN* kod, unosi se i na ekranu; kada se aktivira *LED* dioda, pali se sijalica; a tokom rada servo motora, status vrata se menja. Ako su oba koraka verifikacije uspešno završena, servo motor automatski otvara vrata. U suprotnom, nakon tri neuspešna pokušaja, aktivira se alarm, a sistem korisniku automatski šalje obaveštenje o pokušaju neovlašćenog pristupa putem Telegram aplikacije. Na ovaj način, korisnički interfejs pruža jasnu i intuitivnu vizualizaciju toka autentifikacije i rada sistema, dok se bezbednosne informacije prenose u realnom vremenu.

Slika 13. *Izgled korisničkog interfejsa*

6. ZAKLJUČAK

Ovaj rad prikazuje multifaktorski sistem za autentifikaciju i kontrolu pristupa, zasnovan na pristupačnim komponentama i praktičnoj *web* aplikaciji koja omogućava uvid u rad sistema u realnom vremenu. U slučaju neovlašćenog pristupa, korisnik se automatski obaveštava putem Telegram aplikacije.

Poseban fokus je na mogućnostima daljeg razvoja sistema. Planirane nadogradnje uključuju opciju da korisnici samostalno menjaju korisničko ime i šifru, uz proveru da ime nije već zauzeto. Razmatra se i dodavanje provere već registrovanih otisaka prstiju, što bi omogućilo bolje upravljanje nalogom. Predložena je i mogućnost izmene glasovnih komandi, kao i proširenje liste dostupnih fraza. Pored toga, sistem bi mogao da komunicira i bez interneta, putem GSM modula za slanje SMS poruka ili automatski poziv hitnim službama u slučaju opasnosti. Kao moguće unapređenje sistema predlaže se dodavanje dodatnih senzora i aktuatora, što bi povećalo bezbednost ne samo vrata, već i celog objekta. Na taj način se otvara mogućnost razvoja sistema za sigurnost stambenih prostora.

7. LITERATURA

[1] https://randomnerdtutorials.com/getting-started-with-esp32/ (pristupljeno u oktobru 2025.)

[2] https://www.componentsinfo.com/hc-sr501-module-pinout-datasheet/ (pristupljeno u oktobru 2025.)

[3] https://www.az-delivery.de/en/products/0-96zolldisplay (pristupljeno u oktobru 2025.)

[4] https://lastminuteengineers.com/arduino-keypad-tutorial/ (pristupljeno u oktobru 2025.)

[5] https://learn.adafruit.com/adafruit-optical-fingerprint-sensor (pristupljeno u oktobru 2025.)

[6] https://wiki.dfrobot.com/SKU_SEN0539-EN_Gravity_Voice_Recognition_Module_I2C_UART#target_0 (pristupljeno u oktobru 2025.)

Kratka biografija:

Miljana Stefanov rođena je u Vršcu 2000. god. Master rad na Fakultetu tehničkih nauka iz oblasti Primenjena elektronika odbranila je 2025.god.
Kontakt:miljana.s2609@gmail.com

Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK:621.31
DOI: https://doi.org/10.24867/34BE14Papic

UTICAJ REGULACIJE POBUDE SINHRONOG GENERATORA NA DINAMIKU KRATKIH SPOJEVA

IMPACT OF SYNHRONOUS GENERATOR EXCITATION REGULATION ON SHORT-CIRCUIT DYNAMICS

Nikola Papić, Dejan Jerkan, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Predmet rada je analiza uticaja regulacije napona upravljanjem naponom pobude sinhronog generatora prilikom tropolnih kratkih spojeva u upetljanoj prenosnoj mreži. Dat je postupak i proračun tranzijenata tropolnog kratkog spoja, kao i analitički izraz za struju kratkog spoja pod uticajem regulacije napona upravljanjem pobude generatora. Nakon toga, prelazi se na simulacionu verifikaciju gde je detaljno objašnjen postupak izvedbe sinhronizacije i regulacije. Konačno, snimljeni su talasni oblici veličina od interesa prilikom kratkog spoja gde su potvrđena teorijska izlaganja, kojima je predviđena pojava većih vrednosti struja kratkog spoja primenom regulacije.*

Ključne reči: *Sinhroni generator, kratki spojevi, regulacija napona*

Abstract *The subject of this paper is the analysis of the influence of the network voltage regulation on the control of the excitation voltage of the synchronous generator in case of three-pole short circuits in the looped transmission network. The procedure and calculation of transients for a three-phase short circuit are presented, as well as the analytical expression for the short-circuit current under the influence of voltage regulation through generator excitation control. After that, it is moved on to simulation verification, where the process of implementation of synchronization and regulation is explained in details. Finally, the waveforms of interest during the short-circuit fault event were recorded, providing experimental validation of the theoretical background that short-circuit currents attain higher values when excitation-based voltage regulation is applied.*

Keywords: *Synchronous generator, short circuits, voltage regulation*

1. UVOD

U savremenim elektroenergetskim sistemima sinhrone mašine imaju ključnu ulogu, posebno u konvencionalnim elektranama koje su direktno povezane na visokonaponsku prenosnu mrežu. Najčešće se koriste u generatorskom režimu, kao osnovni proizvođači električne energije. U odnosu na druge vrste mašina koje mogu raditi kao generatori, prednost sinhronih generatora leži u mogućnosti podešavanja napona i upravljanja tokom reaktivnih snaga u sistemu, što je omogućeno nezavisnim sistemom pobuđivanja. Preduslov za njihovu eksploataciju jeste adekvatan postupak priključenja na mrežu. Priključenje sinhronog generatora na naizmeničnu elektroenergetsku mrežu bez prethodnog ispunjenja svih uslova za sinhronizaciju dovodi do izraženih električnih i mehaničkih naprezanja u samom generatoru, što može rezultovati ozbiljnim oštećenjima mašine. U okviru eksploatacije elektroenergetskog sistema (EES) neminovno se javljaju različiti poremećaji koji utiču na njegov stabilan rad.

Od svih poremećaja koji se mogu javiti u radu elektroenergetskih sistema, najveći izazov svakako predstavljaju metalni kratki spojevi, posebno onda kada nastanu neposredno na priključcima same mašine. Među različitim vrstama kratkih spojeva, tropolni kratak spoj izdvaja se kao najnepovoljniji, jer izaziva najveća i najsveobuhvatnija naprezanja u sistemu. Unutar ovog rada, između ostalog, obrađena je i teorija o regulaciji napona i teorija o sinhronizaciji generatora na mrežu. Pored toga, date su Parkove jednačine i operatorske induktivnosti kao način modelovanja sinhrone mašine pogodan za upravljanje. Izvedeni su izrazi za parametre sinhrone mašine i vremenske konstante za subtranzijentnu, tranzijentnu i ustaljenu sekvencu kratkog spoja.

2. MATEMATIČKI MODEL SINHRONE MAŠINE, PARAMETRI MAŠINE I VREMENSKE KONSTANTE

Početna forma sistema sastoji se od deset izraza, pri čemu se pet njih tiče jednačina naponske ravnoteže namotaja, a drugih pet jednačina njihovih fluksnih obuhvata, prikazanih na sledeći način:

$$u_d = R_s i_d + p\psi_d - \omega\psi_q \quad (1)$$
$$u_q = R_s i_q + p\psi_q + \omega\psi_d \quad (2)$$
$$u_f = R_f i_f + p\psi_f \quad (3)$$
$$0 = R_k i_D + p\psi_D \quad (4)$$
$$0 = R_k i_Q + p\psi_Q \quad (5)$$
$$\psi_d = L_d i_d + M_d i_f + M_d i_D \quad (6)$$
$$\psi_q = L_q i_q + M_q i_Q \quad (7)$$
$$\psi_f = M_d i_d + L_f i_f + M_d i_D \quad (8)$$
$$\psi_D = M_d i_d + M_d i_f + L_D i_D \quad (9)$$
$$\psi_Q = M_q i_q + L_Q i_Q \quad (10)$$

Imajući u vidu činjenicu da su za regulaciju od interesa isključivo upravljačke veličine, uvodi se motiv da se vrši svođenje matematičkog modela na jednostavniji model gde će figurisati promenljive od interesa koje su merljive u mašini. Rezultat ovog postupka uprošćavanja prerasta u sistem jednačina koje opisuju samo statorske namotaje po d i q osi, ali u kojima je kroz izraze operatorskih

NAPOMENA:
Ovaj rad proistekao je iz master rada, čiji mentor je bio dr Dejan Jerkan, vanr. prof.

induktivnosti dobijenih tokom postupka uprošćavanja sistema, ipak sadržan uticaj svih prisutnih namotaja. Ovakav sistem se naziva sistemom Parkovih jednačina i glasi:

$$u_d = R_s i_d + p\psi_d - \omega\psi_q \quad (11) \qquad \psi_d = L_d(p) i_d + G(p) u_f \quad (13)$$

$$u_q = R_s i_q + p\psi_q + \omega\psi_d \quad (12) \qquad \psi_q = L_q(p) i_q \quad (14)$$

Uvedene su tri nove veličine u matematički model:
$L_d(p)$ – podužna operatorska induktivnost, $L_q(p)$ – poprečna operatorska induktivnost i $G(p)$ – prenosna funkcija napona pobude.
Podužna i poprečna induktivnost, date u zavisnosti od Laplasovog operatora *p*, produkt su postupka uprošćavanja sistema jednačina (1)-(10). Induktivnosti se tada izražavaju relacijama u kojima firgurišu omski otpor (R_k, R_f) i rasipni (Λ_D, Λ_Q, Λ_f) parametri prigušnog i pobudnog namotaja, podužna i poprečna rasipna induktivnost statorskog namotaja, Λ_d i Λ_q, međuinduktivnosti M_d i M_q:

$$pL_d(p) = p\Lambda_d + pM_d \| (R_k + p\Lambda_D) \| (R_f + p\Lambda_f) \quad (15)$$

$$pL_q(p) = p\Lambda_q + pM_q \parallel (R_k + p\Lambda_Q) \quad (16)$$

Prilikom pojave naglih poremećaja u mašini, poput kratkih spojeva, dinamika odziva mašine je upravo dominatno određena ovim operatorskim induktivnostima.
Vremenski tok struja kratkog spoja karakterišu tri uočljiva stadijuma, koji se na osnovu oblika anvelope struje kvara mogu jasno raščlaniti. To su subtranzijentni, tranzijentni i ustaljeni period. Ovakva podela na intervale uzrokovana je konstrukcionim karakteristikama mašine sa isturenim polovima rotora i prigušnim namotajem. Naime, na samom početku kvara, ukupnoj impedansi mašine aktivno doprinose svi namotaji u mašini. Međutim, zbog izraženije vrednosti aktivne otpornosti prigušnog namotaja u poređenju sa otpornostima ostalih namotaja mašine, doprinos ovog namotaja u impedansi kratkog spoja najpre iščezava. Značajan uticaj prigušnog namotaja najbrže jenjava i time označava kraj subtranzijentnog, a početak tranzijentnog perioda. Aktivna otpornost pobudnog namotaja je i do 50 puta manja od prigušne, što uz ujedno i veliku sopstvenu induktivnost određuje da tranzijentni period vremenkog toka struje kvara traje značajno duže od subtranzijentnog. Sopstvena magnetna tromost pomenutih namotaja može se iskazati putem sledećih vremenskih konstanti:

$T_f = \frac{L_f}{R_f} = \frac{\Lambda_f + M_d}{R_f}$ – podužna vremenska konstanta pobudnog namotaja rotora (17)

$T_D = \frac{L_D}{R_k} = \frac{\Lambda_D + M_d}{R_k}$ – podužna vremenska konstanta prigušnog namotaja rotora (18)

Kao što je rečeno, strujama kvara statorskih namotaja doprinose svi namotaji mašine usled magnetskog sprezanja. Efekat ovog sprezanja je uvažen putem operatorskih induktivnosti $L_d(p)$ i $L_q(p)$. Stoga je vremenski tok struja kvara određen dinamikom svih međusobno spregnutih namotaja, tako da oni združeno određuju induktivnosti i vremenske konstante pomoću kojih se ta promena karakteriše.
Operatorske induktivnosti se mogu primenom teoreme o graničnim vrednostima tumačiti kao konstantne veličine tokom trajanja nekog od tri pobrojana segmenta (sub,tr,ust) Prema tome, subtranzijentnom tj. početnom periodu prelaznog procesa odgovara primena prve navedene granične teoreme čime se dobija tzv. subtranzijentna induktivnost L_d'':

$$L_d^n = L_d(t \to 0) = L_d(p \to \infty) = \Lambda_d + \left(M_d \left\| \left(\frac{R_k}{p} + \Lambda_D \right) \right\| \left(\frac{R_f}{p} + \Lambda_f \right) \right) = \Lambda_d + \left(M_d \| \Lambda_D \|_f \right). \quad (19)$$

Naredni je tranzijentni period koji za polaznu osnovu uzima izraz sličan prethodnom, ali bez učešća parametara vezanih za prigušni namotaj (Λ_f, R_f). Ovakav pristup je teorijski opravdan odnosnom vrednosti vremenske konstante prigušnog i pobudnog namotaja za koje važi $T_f \gg T_D$. Izraz za određivanje tranzijentne induktivnosti L_d', uz pobrujana ograničenja glasi:

$$L_d' = L_d(t \to 0) = L_d(p \to \infty) = \Lambda_d + (M_d \parallel \Lambda_f). \quad (20)$$

Po vremenskom toku poslednja, ustaljena induktivnost L_d, dobija se korišćenjem drugog graničnog uslova na sledeći način:

$$L_d = L_d(t \to \infty) = L_d(p \to 0) = \Lambda_d + \frac{1}{p}(pM_d \| R_k \| R_f) = \Lambda_d + M_d. \quad (21)$$

Analognim postupkom definišu se i poprečne induktivnosti subtranzijentnog i ustaljenog perioda, L_q'' i L_q :

$$L_q'' = L_q(t \to 0) = L_q(p \to \infty) = \Lambda_q + \left(M_q \parallel \left(\frac{R_k}{p} + \Lambda_Q \right) \right) = \Lambda_q + (M_q \parallel \Lambda_Q) \quad (22)$$

$$L_q = L_q(t \to \infty) = L_q(p \to 0) = \Lambda_q + M_q. \quad (23)$$

Poprečna operatorska induktivnost nije pod uticajem promene u tranzijentnom periodu zbog odsustva pobudnog namotaja po podužnoj osi, te stoga trivijalno sledi $L_q'' = L_q'$.
Vremenske kontante statorskih namotaja se mogu izvesti putem razlaganja na proste činioce izraza za operatorske induktivnosti:

$$L_d(p) = L_d \frac{(1+pT_d')(1+pT_d'')}{(1+pT_{d0}')(1+pT_{d0}')}; \quad (24)$$

$$L_q(p) = L_q \frac{1+pT_q''}{1+pT_{q0}''}; \quad (25)$$

gde su:

$$T_{d0}' = T_f + T_D \approx T_f = \frac{\Lambda_f + M_d}{R_f} \quad (26)$$

$$T_{d0}'' = \frac{\sigma_{fD} T_D}{1 + \underline{T_D}} \approx \sigma_{fD} T_D = \frac{\Lambda_D + (\Lambda_f \parallel M_d)}{R_k} \quad (27)$$

$$T_d' = \sigma_{df} T_f + \sigma_{dD} T_D \approx \sigma_{df} T_f = \frac{\Lambda_f + (\Lambda_d \parallel M_d)}{R_f} \quad (28)$$

$$T_d'' = \frac{\Lambda_D + (\Lambda_d \| \Lambda_f \| M_d)}{R_k} \quad (29)$$

Apostrof ′ se odnosi na konstante vezane za tranzijetni period prelaznog procesa, dok je dvosotruki apostrof " oznaka za subtranzijentni period. Dodatni indeks ”0” naglašava da je reč o konstantama koje ne uključuju statorske rasipne induktivnost, što asocinara na režim praznog hoda, dok su veličine bez indeksa vezane za režim kratkog spoja.

3. ANALITIČKI IZRAZ ZA STRUJU TROPOLNOG KRATKOG SPOJA

Analitički izraz za struju kratkog spoja glasi:

$$i_a(t) = -\sqrt{2}\cdot E \cdot \left(\begin{array}{c}\left[\frac{1}{X_d}+\left(\frac{1}{X'_d}-\frac{1}{X_d}\right)e^{-\frac{t}{T'_d}}+\left(\frac{1}{X''_d}-\frac{1}{X'_d}\right)e^{-\frac{t}{T''_d}}\right]\\ \cos(\omega t+\vartheta_0)\\ -\left[\begin{array}{c}\frac{1}{2}\left(\frac{1}{X''_d}+\frac{1}{X''_q}\right)e^{-\frac{t}{T_a}}\cos(\vartheta_0)\\ +\frac{1}{2}\left(\frac{1}{X''_d}-\frac{1}{X''_q}\right)e^{-\frac{t}{T_a}}\cdot\cos(2\omega+\vartheta_0)\end{array}\right]\end{array}\right) \quad (30)$$

Uvažavajući da je $X''_d \approx X''_q$ kod sinhronih mašina sa dobro dimenzionisanim prigušnim namotajem i $\vartheta_0 = 0$, jednačina za struju u vremenskom domenu glasi:

$$i_a(t) = -\left[\sqrt{2}\frac{E}{X_d}+\sqrt{2}E\left(\frac{1}{X'_d}-\frac{1}{X_d}\right)e^{-\frac{t}{T'_d}} + \sqrt{2}E\left(\frac{1}{X''_d}-\frac{1}{X'_d}\right)e^{-\frac{t}{T''_d}}\right]\cdot cos(\omega t) + \sqrt{2}\frac{E}{X''_d}e^{-\frac{t}{T_a}} \quad (31)$$

Gde je T_a aperodična vremenska konstanta i iznosi:

$$T_a = \frac{2X''_dX''_q}{\omega R_s\left(X''_d+X''_q\right)} \quad (32)$$

Proračuni struja trofaznog kratkog spoja u radijalnoj šemi mogu se izvesti primenom izraza izvedenih za kvarove neposredno na krajevima generatora, izmenjenim tako da obuhvataju uticaj impedanse elemenata mreže do mesta kvara. Deo prenosnog sistema, npr pri tački *C* sa slike 1, može se kod trofaznog kratkog spoja zameniti električnom šemom sa generatorom i ukupnom rednom impedansom mreže do mesta kvara:

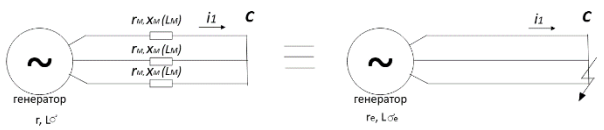
$$\bar{Z}_M = r_M + j\mathrm{X}_M \quad (33)$$

Impedansa $\bar{Z}_M$ predstavlja zbir rednih impedansi elemenata mreže do mesta kvara u tački *C*. Stvarni generator sa impedansom mreže se pri proračunima struje kratkog spoja može zameniti ekvivalentnim generatorom kao na slici 1 sa aktivnom otpornošću faza:

$$r_e = r + r_M \quad (34)$$

i induktivnošću rasipanja:

$$L_{\sigma e} = L_\sigma + L_M \quad (35)$$



Slika 1. *Ekvivalentni generator*

Struja kratkog spoja u radijalnoj šemi računa se preko izraza (30) napisanog za ekvivalentni generator:

$$i_a(t) = -\left[\sqrt{2}\frac{E}{X_{de}}+\sqrt{2}E\left(\frac{1}{X'_{de}}-\frac{1}{X_{de}}\right)e^{-\frac{t}{T'_{de}}} + \sqrt{2}E\left(\frac{1}{X''_{de}}-\frac{1}{X'_{de}}\right)e^{-\frac{t}{T''_{de}}}\right]\cdot\cos(\omega t)+\sqrt{2}\frac{E}{X''_{de}}e^{-\frac{t}{T_{ae}}}, \quad (36)$$

gde su:

$$X_{de} = X_d + \mathrm{X}_M;\quad X'_{de} = X'_d + \mathrm{X}_M;\quad X''_{de} = X''_d + \mathrm{X}_M, \quad (37)$$

dok su vremenske konstante:

$$T'_{de} = T'_{d0}\frac{X'_{de}}{X_{de}};\quad T''_{de} = T''_{d0}\frac{X''_{de}}{X'_{de}} \quad (38)$$

Vremenske konstante T'_{d0} i T''_{d0} ekvivalentnog generatora poklapaju se sa konstantama stvarnog generatora jer na njih ne utiču parametri statora. Uz pretpostavku da je $X''_{de} = X''_{qe}$, T_{ae} je , u skladu sa izrazom (32), jednaka:

$$T_{ae} = \frac{1}{\omega}\frac{X''_{de}}{R_s} \quad (39)$$

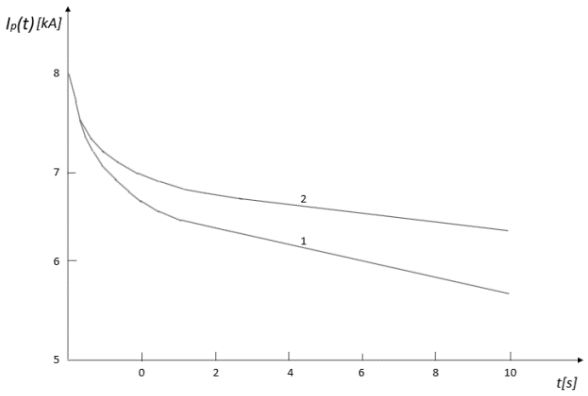
Promena napona pobude generatora usled dejstva regulacije pobude može se približno opisati izrazom:

$$\Delta U_f(p) = \frac{\Delta U}{p}\frac{1}{1+pT_B} \quad (40)$$

Sa $\Delta U_f(p)$ označena je Laplasova transformacija porasta napona pobude , sa ΔU podešeni maksimalni porast napona pobude, a T_B je vremenska konstanta sistema pobude. Efektivna vrednost naizmenične komponente struje kratkog spoja pri delovanju regulacije dobija se kada se odgovarajućem članu u izrazu (36) doda član prouzrokovan regulacijom:

$$i_a(t) = -\left[\sqrt{2}\frac{E}{X_{de}}[1+(k-1)F(t)] + \sqrt{2}E\left(\frac{1}{X'_{de}}-\frac{1}{X_{de}}\right)e^{-\frac{t}{T'_{de}}} + \sqrt{2}E\left(\frac{1}{X''_{de}}-\frac{1}{X'_{de}}\right)e^{-\frac{t}{T''_{de}}}\right]\cdot\cos(\omega t) \quad (41)$$

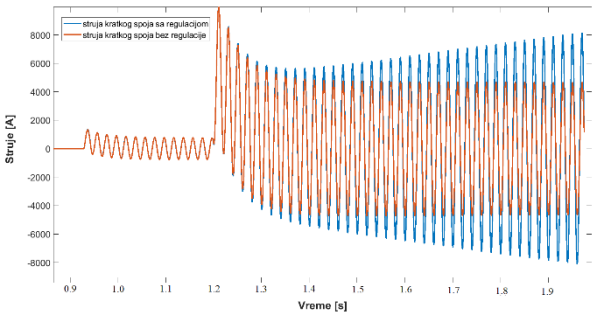
Faktor k obično ima vrednost do reda 2. Na slici 2 prikazan je vremenski tok efektivne vrednosti naizmenične komponente struje kratkog spoja u slučajevima sa i bez udarne regulacije pobude.



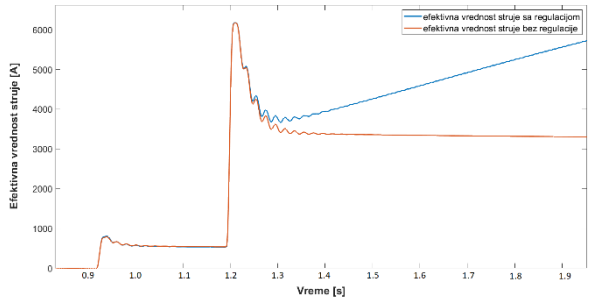
Slika 2. *Efektivna vrednost naizmenične struje, (1) bez regulacije, (2) sa regulacijom*

4. SIMULACIONA VERIFIKACIJA

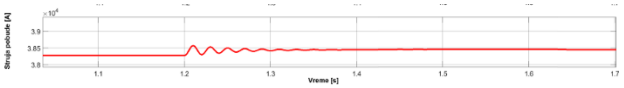
Unutar ovog rada korišćena je IEEE 5-BUS šema koja predstavlja standardizovani električni model pogodan za analizu u okviru Matlab&Simulink softverskog okruženja. Na jedan od čvorova prenosne upetljane mreže vezan je generator kome se reguliše napon pobude, a na mrežu se povezuje putem prekidača. U svrhu analize kratkih spojeva, prvenstveno je neophodna sinhronizacija generatora na mrežu, a zatim i implementacija regulacije napona, što je urađeno putem kaskadne regulacije, izbegavajući time potrebu za pronalaskom parametara PI–kontrolera. Nakon što se uspešno izvrši sinhronizacija i otpočne proces regulacije napona iz razloga što je napon mreže na mestu priključenja manji od zadanog nominalnog, stvara se kratak spoj u dubini prenosne mreže. Kao posledica kratkog spoja javljaju se velike vrednosti struja tropolnog kratkog spoja u mreži. Najbitniji rezultati simulacione verifikacije su talasni oblici struje tropolnog kratkog spoja sa i bez regulacije napona mreže putem generatora prikazani na slici 3, izdvojene promene efektivnih vrednosti struja u vremenu na slici 4, kao i struje pobude bez regulacije na slici 5 i sa regulacijom na slici 6. Imajući u vidu da kvar nastaje u trenutku $t = 1{,}2$ s, potvrđena je teorija da su vrednosti struja kvara pri regulaciji veće od onih bez regulacije.



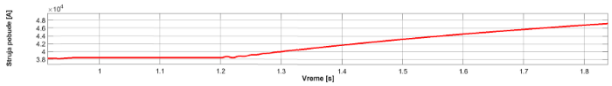
Slika 3. *Talasni oblici struja kratkog spoja sa (plava boja) I bez regulacije (narandžasta boja)*



Slika 4: Efektivne vrednosti struja kvara sa i bez regulacije u prenosnoj mreži



Slika 5. *Struja pobude bez regulacije prilikom kratkog spoja*



Slika 6. *Struja pobude sa regulacijom prilikom kratkog spoja*

5. ZAKLJUČAK

Simulacionom verifikacijom potvrđeni su teorijski analitički izrazi za struje kratkih spojeva sa i bez regulacije napona mreže. Potvrđeno je da su veće vrednosti struje kvara kada postoji regulacija napona u mreži. Sa jedne strane, ovo može predstavljati manu jer zbog većih efektivnih vrednosti dolazi do većih mehaničkih i termičkih naprezanja kako u mašini, tako i u prenosnim vodovima. Sa druge strane, povećanje efektivne vrednosti struje kratkog spoja ima prednost u smislu bržeg delovanja relejne zaštite u prenosnoj mreži, a samim tim i bržeg prepoznavanja i otklonjanja kvara.

6. LITERATURA

[1] Modelovanje električnih mašina, Vladan Vučković

[2] Adkins, B. и Harley, RG., 1975., *The general theory of alternating current machines: Application to Practical Problems*, Chapman and Hall.

[3] Concordia, C., 1951. *Synchronous machines, Theory and Performance*. New York: John Wiley & Sons, INC.

[4] Osnovi elektroenergetike, Vladimir C. Strezoski, Fakultet tehničkih nauka, Univerzitet u Novom Sadu

[5] Odabrana poglavlja iz visokonavonskih postrojenja, Jovan Nahman, Vladica Mijailović, Elektrotehnički fakultet, Akademska misao Beograd

Kratka biografija:

Nikola Papić rođen je u Novom Sadu 2000. god. Osnovne akademske studije završio je 2023. na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Energetska elektronika i električne mašine uz završni rad na temu „Modulacione tehnike za upravljanje trofaznim invertorom". Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Energetska elektronika i električne mašine odbranio je 2025.god. na temu „Uticaj regulacije pobude sinhronog generatora na dinamiku kratkih spojeva".

Dejan Jerkan je vanr. prof. na Fakultetu tehničkih nauka u Novom Sadu, na Katedri za Energetsku elektroniku i pretvarače. Oblast interesovanja su mu modelovanje i dijagnostika električnih mašina, kao i metoda konačnih elemenata.