ISSN 0042-8469

VOJNOTEHNIČKI glasnik

NAUČNI ČASOPIS
MINISTARSTVA ODBRANE
REPUBLIKE SRBIJE

MILITARY TECHNICAL COURIER

SCIENTIFIC PERIODICAL
OF THE MINISTRY OF DEFENCE
OF THE REPUBLIC OF SERBIA

3

UDC 623 + 355/359

GODINA LVIII JUL-SEPTEMBAR 2010.

MINISTARSTVO ODBRANE REPUBLIKE SRBIJE

MEDIJA CENTAR „ODBRANA“

DIREKTOR
Slavoljub M. Marković, potpukovnik

ODSEK ZA IZDAVAČKU DELATNOST

GLAVNI UREDNIK
Dragana Marković

ODGOVORNI UREDNIK
mr *Nebojša* Gaćeša, potpukovnik
e-mail: nebojsa.gacesa@mod.gov.rs
tel.: 011/3349-497

Adresa redakcije:
VOJNOTEHNIČKI GLASNIK,
Braće Jugovića 19, Beograd
e-mail: vojnotehnicki.glasnik@mod.gov.rs
http://scindeks.nb.rs/journaldetails.aspx?issn=0042-8469

Pretplata: e-mail: pretplata@odbrana.mod.gov.rs;
tel.-fax: 3241-009; tekući račun: 840-49849-58
Rukopisi se ne vraćaju
Časopis izlazi tromesečno

Štampa: Vojna štamparija – Beograd, Resavska 40b

S A D R Ž A J

C O N T E N T S

NAUČNI ČLANCI

ELEKTROMAGNETNI TOP – ISTRAŽIVAČKI PROJEKAT ILI USKORO U UPOTREBI?

Bakić P. *Selena*, J. P. Jugoimport-SDPR, Beograd
Paligorić L. *Anastas*

UDC: 623.421::621.318.3
623.421:537.862

Sažetak:

Više od jednog veka istraživači u mnogim zemljama sveta bave se istraživanjem i razvojem elektromagnetnog (EM) topa koji bi bio u mogućnosti da lansira projektil vrlo velikim brzinama. U publikovanoj stručnoj literaturi veći broj radova odnosi se na teorijska razmatranja pojedinih fenomena električnog pogona projektila i na hardverska rešenja električnih uređaja i komponenata, a manje su dostupni javnosti radovi koji se odnose na borbenu upotrebu, koncepciju rešenja i mogućnosti primene takvog oružja u borbenim sistemima vojske. U radu se ukazuje na osnovne probleme projektovanja takvog sistema naoružanja i saopštavaju se informacije na osnovu kojih se može proceniti da li će, kada i na kakvoj platformi EM top biti uveden u operativnu upotrebu.

Ključne reči: *artiljerijsko oruđe, konvencionalni top, elektromagnetni top, EM top, šinski EM top, solenoidni EM top, elektrotermički top, tenkovski EM top, brodski EM top, generator, kondenzator, kompulzator, APDSFS projektil, KE projektil, razorni projektil.*

Uvod

U članku je prikazano aktuelno stanje razvoja elektromagnetnih topova (EM topovi) i izneto mišljenje o temi koja duže od jednog veka intrigira pronalazače i projektante, a uzbuđuje zaljubljenike u naoružanje: da li će i kada EM top napustiti laboratorije i biti primenjen u praksi – kao naoružanje nekog od borbenih sistema kopnene vojske (vatrene podrške, protivo-

bakic.selena@gmail.com

klopne borbe, protivvazdušne odbrane) i mornarice (dejstvo po ciljevima na vrlo velikim daljinama) ili će, možda, predstavljati jednu od komponenti svemirskog oružja u nekom od „štitova“ potencijalnih sukobljenih strana (što nije predmet ovog rada)? U radu se razmatra samo aspekt stvaranja uslova za lansiranje projektila zahtevanom brzinom, bez upuštanja u domene dinamike sistema pri lansiranju i efikasnosti dejstva projektila na cilju.

Neposredan povod za razmatranje statusa razvoja i mogućnosti upotrebe EM topa bio je članak „Karakteristike trzanja elektromagnetnog topa“, objavljen u VTG broj 4, 2009 [1]. Već sam naslov rada je stručno intrigantan, jer najavljuje razmatranje pojave koja nije bitno svojstvo EM topa. Naime, sam princip dejstva rada EM topa ne uvodi u sistem značajniji impuls trzanja, te se može zaključiti da je dužina trzanja EM topa zanemarljivo mala. Stoga, sasvim je logično pitanje svrsishodnosti razmatranja pojave koja ne utiče na mogućnost praktične primene EM topa! Pri tome se u [1], bez ikakve analize i poređenja funkcije i dejstva na cilju, konstatuje da EM top ima značajne prednosti u odnosu na konvencionalni (klasičan) top.[1] Sem toga, u radu se upoređuju trzanja EM topa i konvencionalnog topa (uvođenjem u razmatranje impulsa trzanja i analizom primene i efikasnosti gasne kočnice) na netipičan i teorijski nedovoljno korektan način.[2]

Navedena stručna intrigantnost rada [1] bila je povod za detaljnije analize većeg broja radova koji su objavljeni o EM topovima. Deo teksta u uvodnom delu rada [1] preuzet je iz članka *„Savremeni uređaji za ispaljivanje projektila velikim i vrlo velikim brzinama“*, koji je objavljen u časopisu *Naučno-tehnički pregled* pre više od 20 godina [2]. Internet pretraživanje pokazuje da je ostatak rada skoro doslovan prevod članka *„Comparison of the recoil of conventional and electromagnetic cannon“*, objavljenog u časopisu *Shock and Vibration* 2001. godine [3]. Iz članka [3] preuzete su i slike (6 od

[1] Primera radi, nisu tačni navodi koji se odnose na: konstrukciju i izradu sklopa cevi i punjača (jer će ti sklopovi kod EM topa biti složeniji i skuplji); tvrdnju da EM top nema plamen na ustima cevi pri lansiranju projektila (naprotiv, EM top ima plamen na ustima cevi, a i druge pojave detektuju položaj topa); navodnu prednost što EM top ne treba da ima sklop protivtrzajućeg uređaja (taj sklop klasičnog topa je jednostavniji i jeftiniji u odnosu na složene, masivne, zapreminski velike i ekstenzivno skupe mašine koje su potrebne EM topu da se stvori mehanička energija i izvrši njena konverzija u električnu energiju); tvrdnju o malom broju stručnih radova o EM topovima (ona je netačna, jer je u poslednjih dvadeset godina objavljeno više od 100 veoma kompetentnih članaka o EM topovima).

[2] Tvrdnja da EM top nema zadnjak i zatvarač nije tačna. Zbog prenošenja struje sa jedne na drugu šinu pomoću armature sa plazmom, EM top mora da ima i zadnjak i zatvarač, da bi se „uhapsila“ plazma i usmerila ka ustima cevi (čime se izazivaju oštećenja unutrašnjosti cevi veća nego kod klasičnog topa), te je predložen izraz za impuls trzanja diskutabilan. Nije prihvatljivo da se funkcija, efikasnost i veličina udarnog talasa gasne kočnice topa 155 mm simulira na topu 20 mm, pre svega zbog velike razlike u količini i vremenu isticanja barutnih gasova, a time i u dinamici strujanja i isticanja gasova. Efikasnost gasne kočnice ne može biti veća od 100%. Ona u najboljim konstrukcijama može da bude do 70%, ali se pri tome formira veliki natpritisak barutnih gasova oko oruđa. Nelogično je poređenje klasičnog i EM topa pri početnim brzinama do 2500 m/s, jer su te brzine više od 2,5 puta veće od početnih brzina projektila koji se ispaljuju iz oruđa 155 mm M198 i M109. Sve ove primedbe odnose se i na rad [3] koji je, nesumnjivo, bio osnova za formiranje teksta [1].

ukupno 7), pa čak i literatura koju navodi autor rada [3]. Nije jasno zašto autori članka [1], objavljenog u VTG-u, nisu citirali dva osnovna izvora za svoj tekst, a pri tome su preuzeli odgovornost za stručni kvalitet rada!

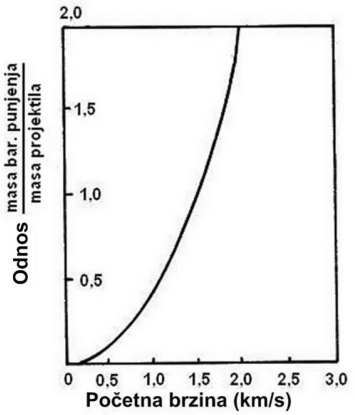
Težnja autora ovoga rada je da se, ne ulazeći u polemiku o etičkim normama i drugim kodeksima sa onima koji ne uvažavaju opšteprihvaćene kriterijume i pravila, čitaocima stave na uvid relevantni tehnički podaci i stručne analize koje se odnose na aktuelni trenutak projektantskih i tehnoloških napora u oblasti elektromagnetnog lansiranja projektila i odgovarajuće procene opravdanosti i prihvatljivosti upotrebe oruđa zasnovanih na tom principu u borbenim sistemima različite namene.

Tendencije u razvoju pogona i projektila klasičnih oruđa

U svojoj skoro milenijumskoj istoriji vatreno oružje, čiji je kraljevski reprezent top, razvijalo se korišćenjem baruta kao pogonskog sredstva za lansiranje projektila. Projektanti su pažljivo pratili zahteve korisnika, pa su, zahvaljujući novim proizvodnim tehnologijama i tehničkim inovacijama (koje se odnose na oruđa/lansere, projektile i barute), povećavali domet artiljerijskih oruđa opšte vatrene podrške, odnosno probojnost protivoklopnih i tenkovskih topova. Istraživanja koja su vršena u kanadskom centru za odbrambena istraživanja,[3] američkom balističkom institutu u Aberdinu[4] i francusko-nemačkom institutu u Saint Louisu[5] (sedamdesetih godina prošlog veka) pokazala su da, čak i ako bi se postigao veći napredak u fizičko-hemijskim svojstvima baruta, realizacija topova (pogodnih za operativnu upotrebu) sa početnim brzinama projektila većim od 2000 m/s nije prihvatljiva zbog velikih dimenzija i masa barutnih punjenja [2]. Na slici 1 prikazan je dijagram eksponencijalnog porasta odnosa mase barutnog punjenja i mase projektila u funkciji početne brzine, sačinjen na osnovu napred navedenih istraživanja. Uočava se da je za brzinu 1650 m/s taj odnos 1, a za brzinu 2000 m/s već 2. Primera radi, iz danas vrlo naprednog rešenja južnoafričke samohodne top-haubice 155 mm G-6 (balistički sistem sa cevi dužine 52 kalibra, zapremina barutne komore 25 litara), razornimm projektilom ERFB-BT nominalne mase 44 kg, najvećim barutnim punjenjem mase 21 kg (6 modularnih punjenja M64) i početnom brzinom od 995 m/s postiže se domet 38 400 m. Projektilom ERFB-BB, nominalne mase 45,5 kg, istim barutnim punjenjem mase 21 kg i početnom brzinom 1015 m/s, postiže se

[3] Opit je vršen iz eksperimentalnog topa 81,3 mm sa cevi dužine 50 kalibara. Sa odgovarajućim barutnim punjenjem i pritiskom od 4140 bara ostvarena je početna brzina projektila 2423 m/s [4].
[4] Korišćenjem produžene varijante cevi tenkovskog topa 120 mm M256 i projektila smanjene mase dobijena je početna brzina od 2790 m/s [4].
[5] Ostvarena je početna brzina od 3000 m/s [4].

domet 50 150 m. Navedeni podaci za odnos masa barutnog punjenja i projektila i ostvarenu početnu brzinu odgovaraju dijagramu sa slike 1. Ako bi se tražilo povećanje brzine na oko 2000 m/s, masa barutnog punjenja trebalo bi da bude oko 90 kg, što bi zahtevalo da zapremina barutne komore bude veća od 110 litara (odnosno 4,5 puta veća nego u realizovanom rešenju oruđa G-6). Očigledno je da takvo balističko rešenje nije prihvatljivo za operativnu upotrebu oruđa vatrene podrške.



Slika 1 – Dijagram porasta odnosa mase barutnog punjenja i mase projektila u funkciji porasta početne brzine

Za razliku od oruđa podrške, koja uglavnom koriste razorne projektile, protivoklopni i tenkovski topovi prvenstveno koriste projektile koji treba da probiju oklop (kupole ili tela) protivničkog borbenog vozila ili zidove protivničkih utvrđenja na daljinama do 2000 m. Za izvršenje tih zadataka, pored projektila punjenih eksplozivom i sa specijalnim funkcijama dejstva (kumulativni mlaz, Hopkinson efekat), koriste se i projektili koji dejstvuju kinetičkom energijom udara (u daljem tekstu KE projektil) u tvrdu prepreku, tj. pancirnu ploču oklopnog vozila. U poslednje tri decenije prošlog veka sve vodeće tehnološke zemlje sveta vrlo intenzivno su razvijale municiju na bazi kinetičke energije, jer ona ima dopunsku prednost – nije osetljiva na elektronsko ometanje, što je slučaj sa kumulativnim projektilima (HEAT) čija je „slaba tačka“ elektronika u upaljaču. Najviše uspeha imali su Rusi i Amerikanci. Tako su za topove tenkova zapadnih zemalja razvijeni potkalibarni projektili 105 mm i 120 mm, a za tenkove istočnih zemalja potkalibarni projektili[6] 100 mm i 125 mm tipa APDSFS. KE pro-

[6] Glavni delovi sklopa potklalibarnog projektila su: obloga, penetrator (jezgro) i krilni stabilizator. Po izlasku projektila iz cevi obloga se odvaja, a ka cilju leti penetrator sa stabilizatorom. Za projektile kalibra 120 mm do 125 mm prečnik penetratora je od 26 mm do 32 mm, da bi se ostvarila što veća specifična energija udara.

jektili prve generacije imali su penetrator od tvrdog metala, a penetratori projektila druge generacije izrađuju se od teškog metala – volframa ili osiromašenog uranijuma (kako bi se povećala specifična KE udara). Metak 125 mm jugoslovenske proizvodnje sa KE projektilom M88 prve generacije imao je karakteristike: početna brzina 1785 m/s, masa projektila 5,86 kg, masa barutnog punjenja 10,445 kg (uključujući i deo mase sagorljive čaure). Budući da odnos masa barutnog punjenja i projektila iznosi 1,783, a početna brzina 1785 m/s, može se konstatovati da se dijagram na slici 1 korektno može primeniti i na KE projektile.

Dobri poznavaoci projektovanja tenkovskih topova 120 mm i 125 mm (dužine sklopa cevi do 7,5 metara, mase do 3 tone, dopušteni pritisak barutnih gasova do 6400 bara, mali balistički vek cevi zbog velikog habanja cevi pri gađanju KE projektilom – oko 8 grama pri ispaljenju jednog metka, a pri tome cena sklopa cevi čak do 160 000 eura) znaju da svako dalje (a pri time neznatno) povećanje već postignutih početnih brzina zahteva znatno povećanje mase, gabarita i cene cevi, čime se kompromituje mogućnost njihove operativne upotrebe. Dostignuti konstrukcioni i tehnološki nivo tenkovskih topova 120 mm i 125 mm i njihove municije prikazan je u tabeli 1.

Tabela 1

Osnovni podaci o tenkovskim topovima i njihovoj municiji sa KE projektilima

Zemlja	SAD/ Nemačka	Francuska	Rusija/Slovačka	Kina	Jugoslavija
Kalibar topa (mm)	120	120	125	125	125
Oznaka topa	Rh 120 /M256	CN120F1	2A46M	2A46M	2A46M
Dužina cevi (kalibara/mm)	L44 / 5280 L55 / 6600	L52 / 6240	L51 / 6375	L51 / 6375	L51 / 6375
Tip cevi	Glatka	Glatka	Glatka	Glatka	Glatka
Najveći pritisak barutnih gasova u cevi (bara)	6430	6425	5200	5400	5200
Masa sklopa projektila sa jezgrom od volframa (kg)	8,35 (oznaka DM 53)	6,2	7,05	7,44	5,68 (oznaka M88)[7]
Masa jezgra (penetratora) (kg)	4,6	4,4		4,03	3,6
Početna brzina (m/s)	1670 (iz L44) 1750 (iz L55)	1780	1700	1740	1785
KE na ustima cevi (kJ)	12785	9822	10838	11263	9049
Probojnost (mm)[8]	640	640	560	560	350

[7] U konkretnom slučaju reč je o municiji prethodne generacije, u kojoj je jezgro (penetrator) od tvrdog metala.

Na osnovu podataka iz tabele 1 mogu se usvojiti sledeći zaključci bitni za kvalitet realizovanih rešenja najmoćnijih sistema tenkovskih topova i KE municije:

– energija KE projektila na ustima cevi je u granicama od 9 MJ do 13 MJ,

– penetrator najuspešnijih rešenja KE projektila ima masu oko 4 kg, prečnik je oko 30 mm, te je kontaktna površina sudara projektila sa ciljem oko $7 \cdot 10^{-4}$ m^2,

– pad početne brzine razmatranih KE projektila na daljini do 2000 m je oko 100 m/s, te je najveća brzina penetratora od volframa pri udaru u ploču oko 1650 m/s,

– udarna energija KE projektila klasičnog topa na cilj udaljen 2000 m je oko 5445 kJ, odnosno specifična energija udara je $770{,}7 \cdot 10^{+4}$ kJ/ m^2,

Realizovana rešenja tenkovskih topova i municije (tabela 1), uz napred navedena teorijska istraživanja, očigledno pokazuju da je upotreba baruta kao pogonskog goriva ograničena do dobijanja početnih brzina oko 1800 m/s. Stoga je nejasno zašto autori radova [3] i [1] upoređuju ponašanje konvencionalnog i EM topa pri brzinama projektila od 1800 m/s do 2500 m/s, imajući u vidu činjenicu da se barut ne koristi kao gorivo u tom rasponu brzina!

Alternativne mogućnosti povećanja početne brzine projektila jesu primena tečnog goriva ili lakog gasa (umesto baruta). Nažalost, rezultati dosadašnjih istraživanja nisu potvrdili mogućnost pouzdanog i bezbednog korišćenja tih goriva u konvencionalnim topovima(detaljnije o statusu upotrebe tih goriva u [2], [4] i [5]). Ovaj rad se bavi samo mogućnošću primene EM topa za postizanje vrlo velikih brzina lansiranja projektila.

Iz teorije sudara dva čvrsta tela poznato je da pri povećanju udarne brzine iznad 2000 m/s (pa sve do 3000 m/s) lokalni pritisak postaje veći od granice otpornosti (tečenja) materijala, te se tela u sudaru ponašaju po zakonima hidrodinamike. Pri vrlo velikim brzinama sudara (većim od 12 000 m/s) energija se tako brzo oslobađa da se tela u sudaru lokalno ponašaju po zakonima gasodinamike [7]. Više o teoriji sudara čitalac može da sazna u radovima [2] i [7].

Osnovni principi dejstva EM topova

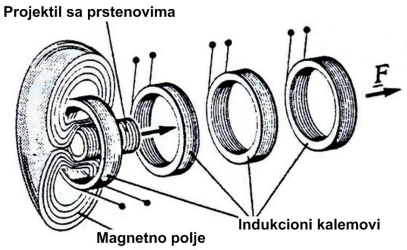
Prve ideje o oružju koje nazivamo EM top nastale su krajem XIX veka. Pre Prvog svetskog rata objavljeno je 45 patenata o EM topu.[9] Postoje dva tipa EM topova: najpre su realizovani laboratorijski modeli solenoidnog topa (Coil Gun), a kasnije efikasniji modeli šinskog topa (Rail Gun).

[8] Podaci o probojnosti potkalibarnog projektila sa jezgrom od teškog metala (volframa), koje deklarišu proizvođači, teško su proverljivi, ali se može prihvatiti da je realan zahtev da probija homogenu pancirnu ploču uslovne debljine $\geq$ 550 mm na daljini od 2000 m (vertikalno postavljenu na osu gađanja).

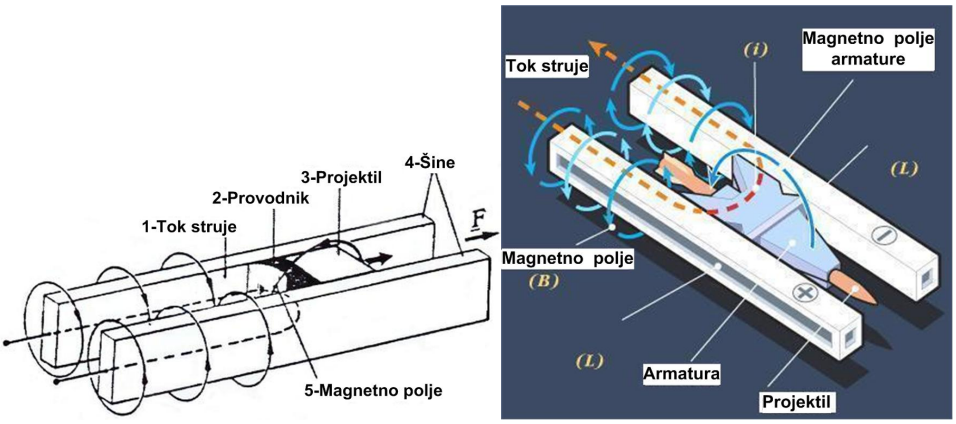
[9] Jedan od prvih datira iz 1901. godine. Autor je bio norveški profesor fizike Birkeland, a njegov solenoidni EM top je i danas izložen u norveškom Tehničkom muzeju u Oslu [2], [4].

Solenoidni top sastoji se od cevi oko koje su na određenim rastojanjima postavljeni indukcioni kalemovi. Sukcesivnim propuštanjem napona kroz kalemove formira se magnetno polje usled indukovanja struje u prstenovima na projektilu, te se formira potisna električna sila koja ubrzava projektil u cevi.

Šinski top[10] sastoji se od dve paralelne šine, između kojih klizi projektil. Da bi se iniciralo kretanje projektila kroz jednu šinu se propusti jednosmerna struja, zatim ona prolazi kroz armaturu[11] (provodnik, sa ili bez plazme) između šina i zatim se vraća kroz drugu šinu. Magnetno polje formirano oko šina u kombinaciji sa tokom struje stvara potisnu silu koja ubrzava armaturu sa projektilom. Za šira saznanja o principima, dejstvu i opremi EM topova čitaoci se upućuju na kumulativnu naučno-tehničku informaciju „Elektromagnetni topovi“ [4].



Slika 2 – Funkcionalna šema solenoidnog EM topa

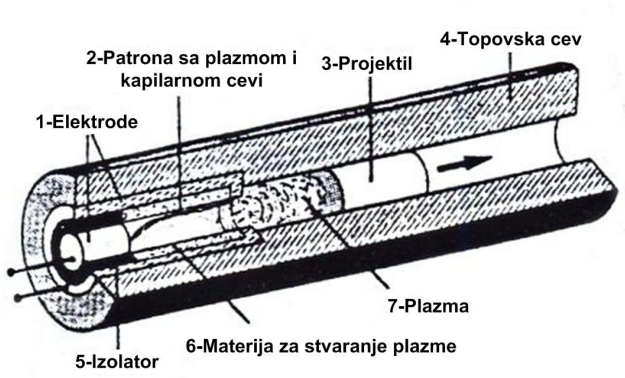


Slika 3 – Funkcionalna šema EM šinskog topa

[10] Pronalazač šinskog topa je francuz André Louis-Octave Fauchon-Villeplée, sa svoja tri patenta iz 1920. godine.

[11] Termin „armatura“ podrazumeva element koji provodi struju između dve šine. Može biti od čvrstog materijala ili je hibrid plazme i čvrstog materijala.

Mnogo kasnije, kada je postalo izvesno da su osnovni problemi EM topova formiranje potrebne električne energije na ustima cevi topa i njeno akumuliranje u mašinama prihvatljivih dimenzija, obimna istraživanja usmerena su na razvoj „hibridnih“ EM topova, najpre elektrotermičkog (ET) topa, a zatim elektrotermičko-hemijskog (ET-H) topa.[12]

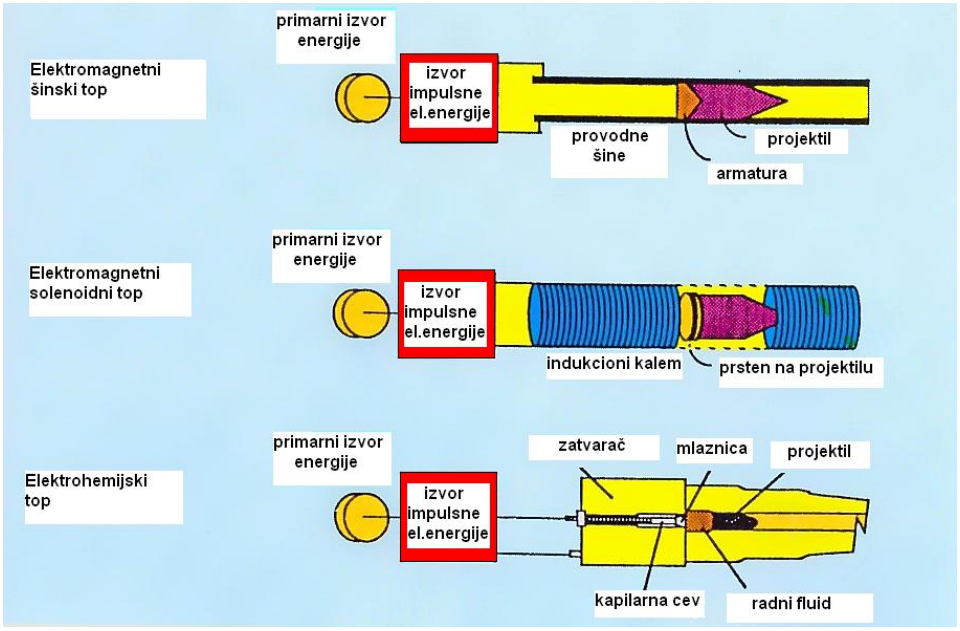


Slika 4 – Funkcionalna šema ET topa

ET top sastoji se od klasične topovske cevi sa elektrodama, komore sa plazmom, zadnjaka i ostalih delova oruđa. Struja se uvodi u fluid pomoću patrone (napunjenje plazmom) sa tankom niti u polietilenskoj kapilarnoj cevi. Pri prodoru strujnog talasa eksplodira kapilarna cev, što dovodi do stvaranja toplih polietilenskih para, a zatim plazma (pod vrlo visokim pritiskom i pri temperaturama preko 3000 K) ubrzava projektil do brzina znatno većih od 2000 m/s.

ET-H top je nastao tako što se veći deo pogonske energije dobio u procesu hemijske reakcije, te se od ET topa razlikuje po načinu korišćenja egzotermnih radnih fluida. Razvoj ET-H topova započet je u američkim firmama GDLS[13] i FMC[14] početkom osamdesetih godina prošlog veka. Obe firme su za razvoj svojih eksperimentalnih modela koristile američki tenkovski top M256 i kondenzator kao izvor električnog impulsnog napona. Sredinom osamdesetih godina u istraživačkom centru firme FMC patentiran je koncept razvoja ET-H topa oznake CAP,[15] a zatim su realizovani i ispitivani do sredine devedesetih godina modeli topova 105 mm i 120 mm, radi ocene mogućnosti njihove primene u tenkovima [9].

[12] Početna istraživanja vršio je Nemac Muck 1945. godine, a tokom šezdesetih godina registrovani su prvi patenti za zagrevanje helijuma pomoću električnog luka u firmi GEC (General Electric corporation).
[13] GDLS – General Dynamics Land Systems.
[14] FMC – Ford Motor Corporation.
[15] CAP (Combustion Augmented Plasma – plazma pojačanog sagorevanja).



Slika 5 – Šematski prikaz rešenja EM topova:

Propao pokušaj naoružavanja tenka klasičnim topom 75 mm ARES – šansa za EM top

Ne ulazeći u detaljnije analize koncepcije rešenja tenkova, može se konstatovati da su krajem dvadesetog veka realizovana optimalna rešenja osnovnog borbenog tenka u tehnološki vodećim zemljama sveta (na osnovu raspoloživih tehnologija). Pri tome se došlo do zaključka da je dalje povećanje mase tenkova neprihvatljivo sa stanovišta borbene upotrebe, a dalje povećanje cena (za zapadne tenkove poslednje generacije ona je veća od 5 miliona eura) ekonomski neprihvatljivo. Pošto se masa tenka utvrđuje na osnovu željenog nivoa balističke zaštite i energije projektila na ustima cevi, početkom osamdesetih godina prošlog veka došlo se na ideju da se umesto kupole naoružane topom velikog kalibra ugradi automatski oružni sistem manjeg kalibra, koji može da obezbedi lansiranje projektila sa istom ili većom kinetičkom energijom. Tako je kompanija Paccar u okviru projekta ELKE (*ELevated Kinetic Energy*) ugradila spolja, na gornju ploču oklopnog tela, automatski top 75 mm ARES sa novom generacijom KE projektila [6], sa ciljem da se smanji ukupna masa tenka i da udarna energija projektila na cilju bude prihvatljiva. Ipak, operativna ispitivanja prototipa ukazala su na borbene nedostatke zbog kojih korisnici nisu prihvatili predloženi koncept rešenja (nezaštićena i podignuta silueta automatskog topa bila je „laka“ meta za dejstvo naoružanja protivnika, komandir nije imao mogućnost

kružnog osmatranja, optoelektronska panoramska sprava nije zadovoljila, složeno rešenje automatskog punjača i potreba uvođenja daljinske komande su ekstenzivno povećali cenu). Napuštanjem koncepta ELKE pojavila se (možda) poslednja šansa za eventualnu afirmaciju EM topa.

Definisanje zahteva za projektovanje tenkovskog EM topa

Bitna i osnovna razlika konvencionalnog i EM topa je princip dejstva. Konvencionalni top je, u osnovi, toplotna mašina u kojoj hemijska energija baruta u procesu sagorevanja oslobađa toplotu u zatvorenom prostoru barutne komore i formira pritisak barutnih gasova, te se potiskivanjem projektila u cevi toplotna energija transformiše u mehaničku energiju. Cilj dobrog balističkog projektovanje jeste da projektil napusti usta cevi sa što većom kinetičkom energijom. Koeficijent korisnosti toplotne energije baruta u konvencionalnom topu je oko 28% do 35%.[16]

Princip rada EM topa je složeniji i svodi se na sledeću šemu transformacije primarne energije u mehaničku energiju projektila (razmotren je slučaj ugradnje EM topa u tenk):

– toplotna energija dizel goriva ili kerozina u dizel motoru ili gasnoj turbini pretvara se u mehaničku energiju; koeficijent korisnosti dizel motora je oko 40%, a gasne turbine oko 30%;

– mehanička energija dizel motora (ili gasne turbine) transformiše se u impulsnu električnu energiju (za kasnije formiranje magnetnog polja) pomoću homopolarnog generatora jednosmerne struje ili pomoću kompulzatora[17]; koeficijent korisnosti generatora je 80% do 90%;

– za akumuliranje električne energije (potrebne za ispaljivanje većeg broja projektila) koriste se kondenzatori, induktori ili akumulatori, zavisno od rešenja EM topa; poželjno vreme za ponovno popunjavanje potrošene energije je do 5 minuta;

– u EM topu (odgovarajuće konstrukcije) formira se jednosmerna struja kratkog impulsa i velikog intenziteta (za lansiranje projektila), a električna energija se transformiše u mehaničku energiju projektila; koeficijent korisnosti je oko 20%;

[16] Toplota sagorevanja topovskih baruta je 3,2 do 4,5 kJ/g, zavisno od toplotne moći i vrste upotrebljenog baruta. U slučaju opaljenja metka 125 mm sa KE projektilom M88 i pripadajućim barutnim punjenjem oslobađa se toplotna energija od oko 31,59 MJ (računajući sa koeficijentom toplote 3,6 MJ/kg). Imajući u vidu kinetičku energiju projektila na ustima cevi (9,049 MJ – videti tabelu 1) dobija se da je koeficijent korisnosti klasičnog tenkovskog topa oko 28,6%. Balističkim rešenjem samohodne top-haubice 155 mm NORA-B52 ostvaren je stepen korisnosti od oko 34%.

[17] Kompulzator je novi tip generatora sa znatno smanjenom impendansom i dodatnim stacionarnim kalemom. Pored stvaranja struje kratkog impulsa, a velikog intenziteta, koristi se i za vremensko induktivno akumuliranje energije.

– ukupni koeficijent korisnosti EM topa je, dakle, 5% do 7% (to je odnos dobijene energije EM projektila na ustima cevi prema ulaznoj energiji primarnog izvora);

– na osnovu prethodnih razmatranja, autori ovoga rada smatraju da princip funkcije EM topa treba i eventualno može da se operativno primeni (ukoliko se ostvare određeni zahtevi) pre svega za lansiranje projektila koji na cilj dejstvuju kinetičkom energijom udara. Primena principa EM topa na samohodna oruđa vatrene podrške (primer: top-haubica 155 mm)[18] i samohodna oruđa namenjena za protivvazduhoplovnu odbranu (primer: dvocevni top 30 mm do 40 mm)[19] eksplicitno zahteva da prethodno budu rešeni brojni tehnički problemi vezani za mogućnost ispaljivanja razornih projektila (detaljnije u poglavlju o brodskom EM topu).

Može se zaključiti da bi projektni zadatak za razvoj EM topa ***namenjenog za osnovno naoružanja tenka*** trebalo da se svede na razmatranje mogućnosti ispunjavanja sledećih zahteva:

a) udarna energija projektila EM topa treba da bude jednaka ili veća od udarne energije najuspešnijeg KE projektila realizovanog za klasičan tenkovski top. Ovaj zahtev se svodi na definisanje potrebne energije projektila na „ustima“ cevi EM topa, imajući u vidu koeficijent korisnosti (odnosno ukupni koeficijent korišćenja primarne energije) EM topa;

b) definisanje i akumuliranje potrebne električne energije za izvršenje projektovane brzine gađanja iz EM topa u slučajevima:

da najveća brzina gađanja bude 6 metaka za jedan minut,

da može da se ostvari produženi režim gađanja od 4 metka/minut u trajanju do 3 minuta;

c) pronalaženje kondenzatora ili neke druge mašine odgovarajućeg tipa i snage potrebnog za akumuliranje energije neophodne za izvršenje funkcije EM topa u traženom vremenu i pri zadatom režimu gađanja (Σenergije $\geq$ (a) + (b));

d) definisanje zapremine i mase EM topa i kompletne prateće opreme potrebne za:

– izvor energije (savremeni tenk koristi dizel motor ili gasnu turbinu),

– transformaciju mehaničke u električnu energiju (homopolarni generator ili kompulzator),

[18] Sa projektilom tipa ERFB-BB (sa generatorom gasa) ostvaren je domet do 55 km, a sa projektilom tipa V-LAP (sa generatorom gasa i raketnim motorom) do 67 km. Dalji razvoj je usmeren na povećanje preciznosti i tačnosti pogađanja ciljeva na tako velikim daljinama (upaljač sa mogućnošću korigovanja putanje), a ne na zamenu baruta kao pogonskog goriva.

[19] Već je u upotrebi klasična municija takvih tehničkih karakteristika, koja (zahvaljujući automatskim punjačima topova i velikoj brzini gađanja) ima vrlo efikasno dejstvo po vazdušnim ciljevima na visinama do 3 km i daljinama do 4 km. Dalji razvoj usmeren je na povećanje efikasnosti uništenja ciljeva na navedenim daljinama (blizinski upaljač, sa mogućnošću programiranja kada je projektil u letu), a za dejstvo na većim daljinama i visinama ekonomski je prihvatljivija primena vođenih PA raketa.

– akumuliranje (stokiranje) potrebne energije za funkciju EM topa (kondenzator, akumulator),

– transformaciju električne energije u mehaničku, odnosno kretanje projektila režimom koji obezbeđuje projektovanu energiju na ustima cevi EM topa, u funkciji raspoloživog prostora i ukupne mase savremenog tenka.

Analiza mogućnosti naoružavanja tenka EM topom

Eksplicitne odgovore na pitanja koja proističu iz razmatranja mogućnosti definisanih projektnih zahteva mogu da daju samo oni istraživači koji raspolažu svim potrebnim znanjima za projektovanje EM topa i raspolažu sopstvenim iskustvom u razvoju svih komponenata opreme koje su neophodne za navedene transformacije energije u procesu funkcije EM topa. Budući da autori ne pretenduju da poseduju takva ekspertska znanja, ponuđeni odgovori su formirani na osnovu analize podataka i saznanja iz raspoložive stručne literature.

Značajan doprinos razmatranju mogućnosti realne primene EM topa predstavlja rad *„Aspects of Modern Tank Design“*[20] [8]. Za predmet ovog rada (slučaj ugradnje EM topa u tenk umesto konvencionalnog topa 120/125 mm) korisne su sledeće konstatacije navedene u tom izvoru:

– potrebna KE projektila na ustima cevi EM topa je oko 20 MJ;

– potrebna akumulirana električna energija za opaljenje jednog projektila (uz pretpostavku da je koeficijent korisnosti 30%[21] i da je za konverziju te energije u KE projektila potrebno samo nekoliko milisekundi) iznosi oko 70 MJ;

– potrebna akumulirana električna energija za opaljenje je: za brzinu gađanja 10 projektila/minut oko 610 MJ; pri brzini gađanja 4 projektila/minut oko 190 MJ;

– vreme za dopunjavanje kondenzatora ili druge mašine za akumuliranje energije (vrši se tokom gađanja): za režim 10 projektila/minut oko 410 sekundi; za režim 4 projektila/minut oko 125 sekundi.

Svi navedeni podaci izračunati su za slučaj korišćenja generatora čija je izlazna snaga 1,5 MW. Bitan je i podatak da je raspoloživi prostor u telu budućeg osnovnog borbenog tenka (prema projektu firme Krauss Maffei) bio 8,8 m^3 za smeštaj sledećih podsistema: pogonske grupe

[20] Rad je nastao korišćenjem saopštenja autora (dipl. inženjera zaposlenog u firmi Krauss Maffei) na Simpozujumu PAPUA 21, organizovanog sa ciljem da se u formi „okruglog stola“ obezbedi rasprava najistaknutijih eksperata u oblasti razvoja oklopnih vozila.

[21] Veći broj autora smatra da je taj koeficijent korisnosti manji i da iznosi samo 20%.

(snage 1,1 MW), sistema mašina za proizvodnju i akumuliranje električne energije za EM top, rezervoara za gorivo (1100 litara), akumulatora, bočnih reduktora, sistema za hlađenje i grejanje.

Uporednom ocenom nedostataka koji se javljaju primenom klasičnog i EM topa autor rada [8] daje značajnu prednost konvencionalnom rešenju. Po njemu, nedostaci klasičnog topa su: buka pri opaljenju metka, zaostali gasovi (CO) u kupoli posle opaljenja metka, eksploziv u razornim projektilima municijskog kompleta. Nedostaci EM topa su: potreban izvor velike energije, uređaji za uključivanje struje visokog intenziteta, akumuliranje električne energije, elektromagnetni fluks, magnetna signatura, IR signatura, velika zapremina i velika masa potrebne opreme EM topa.

Slične i druge informacije korisne pri donošenju ocene o mogućnosti primene EM topa mogu se naći u članku *„Future tank guns – Part II: Electromagnetic and elecrothermal guns“* [9], u kojem se konstatuje da su problemi zapremine i mase vrlo velika prepreka za operativnu primenu EM topa. Tako, na primer, ET top čija je energija na ustima cevi 9 MJ, zahteva da se za jedno opaljenje raspolaže akumuliranom električnom energijom od 30 MJ, imajući u vidu ostvareni koeficijent korisnosti električne energije od oko 30%. Sa kapacitetom akumuliranja 3 kJ/kg, masa kondenzatora je bila čak oko 10 000 kg!

Ocenjujući da je u dogledno vreme moguć napredak u tehnologiji akumuliranja električne energije (procena je data početkom devedesetih godina) Centar za elektromehaniku Univerziteta u Teksasu (CEM-UT) načinio je idejno rešenje tenka sa šinskim topom 100 mm i energijom na ustima cevi 15 MJ, u kojem bi se potrebna električna energija akumulirala sistemom kondenzatora i bipolarnih akumulatora, sa procenom da će se dobiti gustina energije od 15 kJ/kg (kondenzatori) i 135 kJ/kg (akumulatori). Koncept ovog rešenja bio je tenk sa daljinski komandovanom kupolom (sa ugrađenim EM topom) bez posade. Za pogon tenka bilo je planirano korišćenje gasne turbine snage 1100 kW, a procenjena masa tenka sa borbenim kompletom bila je 49,6 tona. Alternativno rešenje predstavlja tenk sa sličnom konfiguracijom, ali se umesto sistema kondenzator/akumulator za akumuliranje energije koriste dva kompulzatora, kako bi se masa tenka smanjila na 47,8 tona.

Razmatranje oba koncepta rešenja sugeriše da se problemi mase i gabarita mogu savladati tek dopunskim i obimnim razvojem komponenata u narednom periodu. Pred toga, autor u [9] upozorava da treba rešiti i druge tehničke probleme, kao što su:

– razvoj prekidača, kliznih kontaktora i fleksibilnih kablova za prenos struje jačine do 4MA,

– zaštita posade tenka (odgovarajućim pregradama) od struje visokog napona,

– zaštita mašina sa velikom brzinom rotacije i mašina za akumuliranje velike količine električne energije od dejstva projektila koji bi probili oklop tenka.

Konačno, za donošenje odluke je relevantno i pitanje cene, pa se navodi podatak da samo kondenzator za akumuliranje energije od 30 MJ košta više od jednog miliona američkih dolara [9].

Konsultovanjem raspoložive literature (mada, verovatno, nije izvršen potpuni pregled štampane literature i/ili potpuno i sveobuhvatno internet pretraživanje) i kritičkim razmatranjem objavljenih podataka autori ovoga rada smatraju da se mogu formulisati sledeće konstatacije i procene o statusu do sada realizovanih EM topova namenjenih za naoružavanje tenkova:

– budući da su već realizovana operativna rešenja tenkovskih klasičnih topova sa energijom projektila na ustima cevi od oko 13 MJ (videti tabelu 1), minimalan zahtev bio bi da se projektuje EM top sa istom energijom projektila na ustima cevi;

– da bi se ostvario isti efekat dejstva na cilju (probijanje oklopa tenka na daljini 2 km, kao i dejstvo iza oklopa) projektil EM topa trebalo bi da ima približno istu udarnu energiju kao KE projektil klasičnog topa.[22]. Ipak, bez dopunskih analiza dinamike lansiranja i efekata na cilju ne može se korektno oceniti ponašanje penetratora (manje mase, a veće brzine) pri sudaru sa oklopom tenka na istoj daljini;

– da bi se ostvario režim gađanja od 6 metaka za jedan minut potrebno je da se u kondenzatoru (ili drugom uređaju) akumulira električna energija od najmanje 367 MJ;[23]

– da bi se formirala i akumulirala navedena energija potrebno je da se u tenk ugradi pogonska grupa (dizel motor i/ili gasna turbina) čija je snaga bar 6,116 MW, odnosno 6116 kW;[24]

– danas se kao izvor mehaničke energije mogu koristiti gasne turbine snage 1100 kW i/ili dizel motori snage 882 kW, prilagođeni za ugradnju u tenk. Očigledno je da je raspoloživi prostor tipičnog osnovnog borbenog tenka 5 do 6 puta manji od prostora u koji bi se smestila pogonska grupa snage veće od 6000 kW;

– procene vodećih istraživačkih centara u svetu (prvenstveno u SAD) da će tokom poslednje dekade ili do kraja dvadesetog veka biti učinjen značajan tehnološki napredak u domenu smanjenja dimenzija i mase električnih mašina za dobijanje i akumuliranje električne energije nisu se ostvarile.[25]

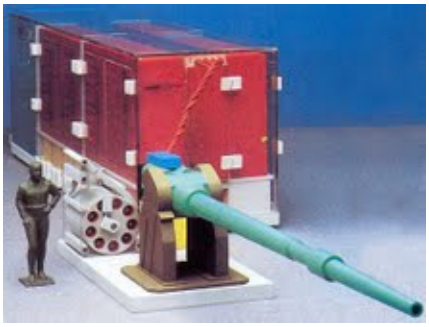
---

[22] U konkretnom slučaju udarna energija KE projektila klasičnog topa na navedenoj daljini je oko 7100 kJ.

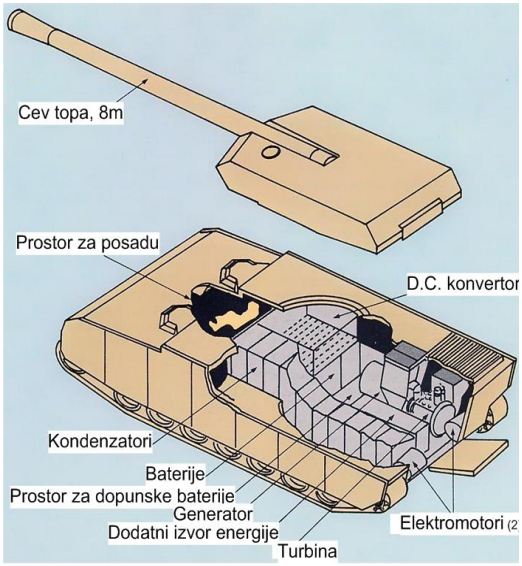
[23] Računajući da se konverzija mehaničke energije pogonske grupe tenka u električnu energiju generatora vrši sa koeficijentom korisnosti 85%, a zatim električne energije u mehaničku energiju projektila sa koeficijentom korisnosti 25%.

[24] Po definiciji, snaga se dobija podelom rada (energije) sa vremenom u kojem se taj rad izvrši (W=J/s), u konkretnom slučaju za 60 sekundi.

[25] Iako je, na primer, firma Maxwell u periodu 1985. do 1990. smanjila zapreminu svojih kondenzatora sa 1,72 m^3 na 0,17 m^3 (za 1MJ).



Slika 6 (gore) – Model ET-H topa 120 mm energije od 9MJ, sa automatskim punjačem (9 opaljenja za 3 minuta) i modulom akumulirane struje u ISO kontejneru



Slika 7 (desno) – Koncept rešenja borbenog tenka mase 49,6 tona naoružanog šinskim EM topom čija je energija na ustima cevi 15 MJ

Jugoslovenske reference u oblasti istraživanja EM topova

U periodu od 1985. do 1990. godine istraživači Instituta za fiziku iz Zemuna i Vojnotehničkog instituta Kopnene vojske JNA iz Beograda u okviru zajedničkog istraživačkog projekta izradili su tri elektrodinamička akceleratora (EM topa) oznake EDA. Provera koncepta funkcionisanja izvršena je 1985. godine na laboratorijskom modelu šinskog EM topa EDA-0 (masa projektila 0,3 g, dužina šina 250 mm, poprečni presek 6x6 mm). Krajem 1987. godine realizovan je novi model EM topa EDA-1, u okviru projekta istraživanja eksperimentalnih metoda za dijagnosticiranje funkcija EM topa pri lansiranju projektila. U periodu do 1990. godine izvršeno je 50 opaljenja. Postignuti su, za to vreme, vrlo dobri rezultati: brzina 3000 m/s sa projektilom mase 0,7 g (odnosno 3,15 kJ energije na ustima cevi) i brzina 2500 m/s sa projektilom mase 1,1 g (odnosno 3,44 kJ). Bilo je planirano da se iz narednog modela EM topa EDA-2 lansira projektil mase 1 g brzinom 7000 m/s. Zbog događaja tokom devedesetih godina nije poznato da li su planirani radovi na projektu završeni.

Na osnovu prethodne analize stanja razvoja sistema EM topova namenjenih za ugradnju u tenk može se zaključiti da su do sada realizovani samo laboratorijski modeli EM topova, da tek treba rešavati borbeni podsistem (konstrukciju šinskog topa i sklopa projektila – armatura, nosač projektila i sam strelasti projektil), a da je određen napredak ostvaren jedino u osvajanju tehnologija izrade komponenata podsistema za formiranje i akumuliranje električne energije. Prema najavama Istraživačke laboratorije američke kopnene vojske, u okviru projekta razvoja budućeg

MBT,[26] čiji se razvoj planira do 2015. godine, nova generacija kompulzatora trebalo bi da bude integralna komponenta EM topa [10]. Nažalost, nema ideja koje bi rešile problem primarnog izvora energije velike snage, a male mase i zapremine.

Brod kao platforma za ugradnju EM topa

Na osnovu iskustava stečenih na razvoju tenkovskog EM topa američki istraživači su u periodu posle 2000. godine započeli istraživanja koja bi dovela do funkcionalnog modela brodskog EM topa. Razlozi su više nego očigledni – brod je adekvatnija platforma od tenkovske za ugradnju gabaritno velikih i još uvek teških funkcionalnih modela EM topova. Snaga brodskih motora je znatno veća od snage tenkovskog motora, pa se jednostavnije rešava zahtev za velikom primarnom snagom potrebnom za formiranje električne energije.

Maja 2003. pomoćnik američkog sekretara za mornaricu zatražio je od Komiteta za brodska istraživanja da se izvrši procena tehnologija u oblasti EM topova. S timu vezi, trebalo je da se izradi [11]:

– pregled i procena tehničkih i operacionih karakteristika potrebnih da bi se ostvario borbeno efektivan sistem EM topa za brodsku upotrebu,

– pregled aktuelnog i očekivanog stanja tehnologija i procena ostvarivanja zahtevanih karakteristika, kao i mogućnosti proizvodnje i održavanja sistema EM topa,

– procena tehničkih i razvojnih rizika (neizvesnosti) u proizvodnji projektila koji bi mogli uspešno da izvrše borbeni zadatak (lansiranje na cilj sa zahtevanom preciznošću).

Izrađena studija je pokazala da postoje značajni projektantski i tehnološki problemi koji tek treba da se savladaju da bi se realizovao sistem operativnog brodskog EM topa. Pored toga, u studiji je bio predložen termin plana na osnovu kojeg bi mornarica mogla da donosi odluke o lansiranju i vođenju pojedinih aktivnosti na programu razvoja u narednih osam godina. Inače, planirane aktivnosti na projektu AGS[27] odnose se na razvoj i izradu funkcionalnih modela EM topova (u više sukcesivnih faza, sa različitom energijom projektila na ustima cevi) i oko 2400 metaka sa KE projektilima dometa više od 370 km.

Sektor za mornarički razvoj u saradnji sa Centrom kopnene vojske za istraživanje, razvoj i inženjering (ARDEC) definisao je, u okviru zajedničkog projekta AGS, sledeće teme istraživanja:

– borbeni sistemi namenjeni za direktno i posredno gađanje, srednjih i velikih kalibara (od jedan do 6 inča, odnosno 25 mm do 155 mm) na bazi primene tehnologija EM topa;

[26] MBT – Main Battle Tank (osnovni borbeni tenk).
[27] AGS (Advanced Gun System – napredni topovski sistem).

– istraživanja i tehnologije od posebnog interesa: pulsni agregati, odnosno mreže uređaja za formiranje i akumuliranje električne energije; integrisani sklop projektila i/ili razvoj komponenata projektila; projektovanje i osvajanje tehnologije izrade sklopa cevi EM topa;

– program istraživanja kojim su zadati nivoi kinetičke energije projektila na ustima cevi koje treba realizovati (od 2 MJ do 64 MJ).

Istraživanje u oblasti sklopa cevi (sa ciljem da se produži život cevi)[28] usmereno je na tri poznata uzroka oštećenja unutrašnjosti cevi pri ubrzanju projektila u njoj: prekomerno zagrevanje šina na mestu dodira sa armaturom; pojava udubljenja na šinama pri kretanju armature sa plazmom velikom brzinom; erozija šina na ustima kada projektil napušta cev.

U oblasti tehnologije pulsne snage planira se nastavak istraživanja primenom dva postupka za proizvodnju visokopulsirajuće struje velikog intenziteta potrebne da se za veoma kratko vreme ubrza projektil u cevi. Prvim postupkom unapređuje se tehnologija pulsnog generatora kao glavnog uređaja za proizvodnju električne energije, a drugim smanjuje zapremina kondenzatora, odnosno povećava gustina akumuliranja. Budući da je kopnena vojska zainteresovana za EM top za neposredno gađanje, koji bi mogao da se ugradi na oklopna vozila, najveći tehnički izazov biće da se obezbedi velika energija na ustima cevi i pogonska grupa male zapremine. Za brodski EM top se zahtev za zapreminu pogonske grupe ne postavlja, a zbog potrebe da se obezbedi vremenski produženi režim gađanja zahteva se brzo dopunjavanje agregata za formiranje pulsne struje, korišćenjem mehaničke energije snažnih brodskih motora.

Što se tiče konstrukcije projektila, osnovni problem je njena otpornost pri visokim ubrzanjima projektila u lansirnoj cevi i obezbeđenje udarne energije KE projektila na cilju. Pri tome je ponašanje elektromagnetne armature, nosača projektila i projektila, kao jedne celine, odlučujuće za pravilnu funkciju. Projektil namenjen za gađanje na velike daljine treba da bude vođen, pa elektronika projektila mora da preživi dejstvo velikih ubrzanja i postojećih visokih elektromagnetnih smetnji okoline. Svojstva projektila po napuštanju usta cevi (stabilnost u letu, zagrevanje zbog otpora vazduha, efektivno i održivo vođenje i upravljanje) odlučujući su za pouzdanost sistema EM oružja namenjenih za dejstvo na ciljeve neposrednim gađanjem na male i posrednim gađanjem na velike daljine.

Tokom 2005. godine započeta je izgradnja novih poligonskih objekata u američkom Mornaričkom opitnom centru u Dahigenu, namenjenih za ispitivanje zemaljske platforme dorađenog šinskog EM topa, čiji je razvoj sredinom osamdesetih godina započela firma BAE Systems. Iz dorađene verzije laboratorijskog EM topa, mase oko 40 tona, 2. oktobra 2006. godine izvršen je uspešan opit gađanjem kome je bila posvećena velika medijska pažnja, pre svega zbog velikog projektovanog dometa od 370 do 400 km [11], [12], [13]. Opit gađanjem izvršen je iz laboratorijskog EM topa sa pogonskom električnom

[28] Zahtevani život cevi je ispaljivanje 10000 projektila.

opremom koja u roku od 5 minuta puni kondenzatore šinskog topa i može da obezbedi efektivnu energiju projektila od 8 MJ.[29] KE projektil mase 2,4 kg bio je lansiran iz cevi kalibra 90 mm (sa šinama od bakra), brzinom od 2520 m/s (ostvarena početna energija je bila 7,6 MJ) na vertikalnu metu (smeštenu u tunel napunjen džakovima peska) udaljenu od usta cevi samo 20 m.

Posle uspešnog opita 2006. godine bilo je planirano da se 2009. godine izvrši prvo ispitivanje EM topa efektivne energije od 32 MJ [11]. Program menadžer firme BAE Systems ipak je bio obazriv kada je izjavio: „Snaga je obezbeđena, jedina je prepreka kako je iskoristiti“ [13]. Naime, pri korišćenju EM topa efektivne energije 8MJ ograničavajući faktor bio je proizvodnja struje 3 miliona ampera za jedno opaljenje. Za opite iz EM topa od 32 KJ u Mornaričkom opitnom centru bi trebalo da se instaliraju dopunski kondenzatori. A šta tek reći za planirani najmoćniji EM top od 64 MJ efektivne energije, za koji bi trebalo da se instalira oprema koja može da akumulira 6 miliona ampera [13]! Možda je kandidat za opremanje budućeg brodskog EM topa već realizovani kompulzator u kojem može da se akumulira 40 MJ energije, što je (prema načinu i vremenu punjenja te vrste mašine) dovoljno za ispaljivanje 15 projektila [10]?[30]

Navedeni problemi vrlo su brzo pokazali da planirana dinamika realizacije budućeg brodskog EM topa mora da se produži. Za izradu dopunske opreme na poligonu u Mornaričkom centru za ispitivanje snažnijih EM topova (od 32 MJ i 64 MJ) firma BAE Systems je zaključila ugovor sa američkom mornaricom vredan 21 milion američkih dolara. Naredni opit iz topa od 32 MJ planira se tek za 2011. godinu [14], [15] .

Slika 8 – Laboratorijska verzija budućeg brodskog šinskog EM topa 90 mm, ispitivanog oktobra 2006. godine: levo – na gornjoj površini zadnjaka je projektil čiji oblik podseća na klasičan APDSFS projektil; desno – plamen (koji mnogi nisu očekivali) pri izlasku projektila iz cevi

[29] Imajući u vidu da kod KE projektila postoji razlika u masi projektila u trenutku napuštanja cevi i u trenutku udara u cilj, kao i razlika brzine na ustima cevi i u trenutku udara u cilj, predlaže se uvođenje sledećih termina: „efektivna energija“ – kinetička energija projektila na ustima cevi i „udarna energija“ – kinetička energija projektila pri udaru u cilj.

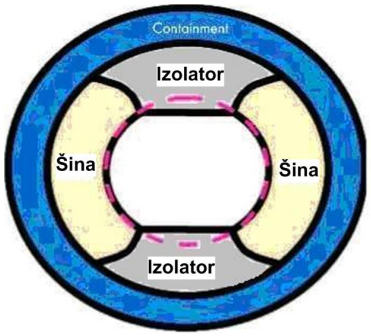
[30] Podatak treba uzeti sa rezervom, jer je vrlo optimističan.

Za ugradnju topa od 64 MJ, po izjavi program menadžera firme BAE Systems, najozbiljniji kandidat je razarač DDG 100 Destroyer, koji ima električni pogon od 72 MW. Proračuni pokazuju da je za lansiranje 6 metaka za jedan minut iz topa 64 MJ potrebna snaga od 16 MW. Takođe, pažnju privlači i procena predstavnika firme BAE Systems da će za konačan razvoj topa od 64 MJ biti potrebno bar 13 godina od dana kada se završi ispitivanje topa od 32 MJ [13]. Dakle, optimistička prognoza bi bila da će, ako se reše svi tehnički i tehnološki problemi, budući brodski EM top moći operativno da se koristi tek posle 2025. godine! Planira se da novi brodski EM top zameni brodske topove 127 mm, čiji je domet oko 21 km, pa bi se uvođenjem u upotrebu EM topa povećao domet brodske artiljerije za oko 20 puta [11], [12].

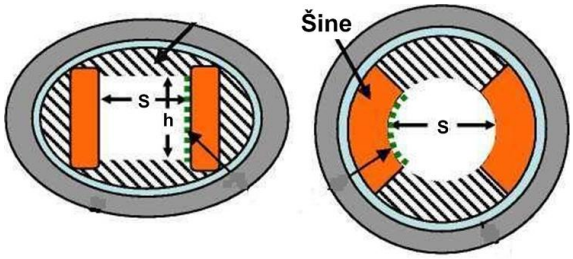
U protekloj dekadi je objavljen veći broj radova u kojima se posebna pažnja posvećuje projektovanju cevi i sklopa projektila. U radu [16] autori detaljno opisuju postupak projektovanja sklopa projektila energije 8 MJ. Sklop projektila je projektovan tako da izdržava ubrzanja od 57 000 g i treba da bude ispitan na probnom stolu u Opitnom centru za EM topove u Škotskoj. Izvršena je unutrašnja balistička analiza, dinamička analiza potkalibarnog projektila (aerodinamički koeficijent, otpornost na dejstvo bočnih sila u toku leta) i strukturalna analiza sklopa projektila i otvaranja nosača projektila pri napuštanju cevi. Izvršeno je uspešno ispitivanje navedenog projektila gađanjem iz britanskog EM topa kalibra 90 mm na opitnom poligonu u Škotskoj. U radu [17] se razmatraju materijali koji se mogu koristiti za izradu cevi i sklopa projektila, a u radu [18] optimizacija oblika cevi i projektila (sa stanovišta naponskog stanja i balistike rešenja) za konkretan slučaj brodskog EM topa efektivne energije 47 MJ (masa projektila 15 kg, početna brzina projektila 2500 m/s).

Ostvareni teorijski i praktični rezultati u prvoj dekadi ovog veka dopuštaju da se implementacija sistema EM topa na brodsku platformu sa više optimizma proceni realnom perspektivom. Još uvek se ne mogu utvrditi konačni taktičko-tehnički zahtevi za budući brodski EM top, ali već ima radova u kojima su definisani polazni projektni zahtevi sistema EM topa, kao što je slučaj sa EM topom energije 8 MJ [16]. Upoređivanjem polaznih zahteva i realizovanih rešenja može se konstatovati zadovoljavajući nivo ispunjenja projektnih zahteva. Vredan pažnje je rad objavljen 2003. godine u kojem se razmatraju rešenja budućeg brodskog EM topa u dve faze, sa više varijantnih rešenja, a zatim daju intencije potrebnih usavršavanja [19]. U prvoj fazi se razmatra rešenje EM topa koji lansira KE projektil sa masom na ustima cevi 21,9 kg, letnom masom 16,4 kg (posle otpadanja nosača projektila) i početnom brzinom 2000 m/s, odnosno top efektivne energije 43,8 MJ. U drugoj fazi se razmatra rešenje sa istom masom projektila, ali je početna brzina 2500 m/s, odnosno top ima efektivnu energiju 68,4 MJ. KE projektil treba da donese na cilj udaljen 430 km udarnu energiju od

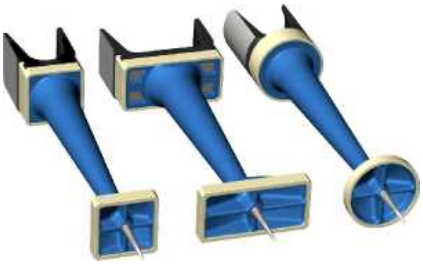
22 MJ.[31] Navedeni podaci odnose se na lansiranje KE projektila iz cevi kalibra 146 mm, a dužine 8760 mm (odnosno cev dužine 60 kalibara, što je uobičajen odnos za cevi brodskih topova – L/d = 60).



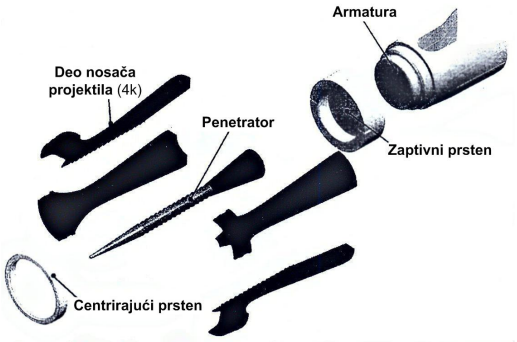
Slika 9 – Izgled preseka cevi šinskog EM topa [17]



Slika 10 – Optimizacija oblika preseka cevi [18]



Slika 11 – Optimizacija oblika EM projektila [18]



Slika 12 – Delovi sklopa KE projektila za EM top

Gađanje ciljeva na tako velikim dometima moglo bi da bude opravdano samo ako iz EM topa može da se lansira i projektil napunjen eksplozivom (razorni projektil), te ohrabruje podatak da se ta mogućnost razmatra u više radova [19], [20]. Pod uslovima lansiranja KE projektila navedene efektivne energije u radu [19] razmišlja se o lansiranju razornog projektila mase 60 kg. Jedan od ozbiljnih problema koje treba rešiti je smanjenje nivoa maksimalnog ubrzanja koje trpi projektil lansiran brzinama oko 2500 m/s. Proračunski nivo maksimalnog ubrzanja razmatranog KE projektila je reda veličine oko 47 500 g, pa se kaže da treba smanjiti nivo ubrzanja na oko 33 000 g [19]. Inače, nivo maksimalnog ubrzanja

[31] Ako su proračuni autora dobri, udarna brzina na cilju bila bi 1417 m/s. Ipak, postavlja se pitanje da li i kakav ubojni efekat može da ostvari KE projektil na tako velikom dometu i na cilj kao što je brod?

pri lansiranju razornih projektila 155 mm iz savremenih klasičnih artiljerijskih oruđa je oko 18 000 g, što nameće potrebu da se pristupi razvoju novih vrsta upaljača i tehnologija laboracije eksploziva u razornim projektilima namenjenim za korišćenje u EM topovima.

U sistem budućeg brodskog EM topa biće integrisani brodski i zemaljski osmatrački radari za otkrivanje ciljeva. Razorni projektil će se navoditi na cilj pomoću satelita GPS tehnologijom sa projektovanom tačnošću od 5 metara. Vreme leta projektila do cilja udaljenog skoro 400 km je oko 6 minuta.

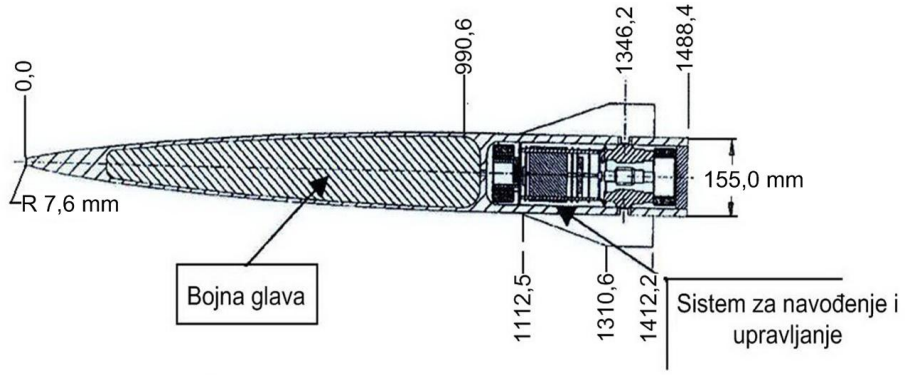
Kada je u pitanju lansiranje razornih projektila, vredan pažnje je rad [20]. Analiza je sprovedena za projektile letne mase 15, 30, 60 i 75 kg, koji se lansiraju početnim brzinama od 2000 m/s do 3000 m/s, iz solenoidnog EM topa dužine cevi 15 m i 20 m. Na primeru projektila letne mase 60 kg daju se vrlo korisni podaci o „parazitskim masama“, a to su masa armature provodnika (17,4 kg) i masa nosača armature (17,3 kg), te je ukupna masa projektila u cevi 94,7 kg. U cevi dužine 15 m predmetni projektil mase 94,7 kg sa ubrzanjem od 13 000 g se do usta cevi ubrzava za 17,6 ms do vrednosti početne brzine od 1900 m/s. Efekti balističkog proračuna navedeni su u tabeli 2.

Tabela 2

Izvod iz balističkog projektovanja za razorne projektile mase 15 kg do 75 kg

	Cev dužine 15 m		Cev dužine 20 m	
Masa projektila, kg	Vo, m/s	Domet, km	Vo, m/s	Domet, km
15	2550	338	3000	520
30	2230	276	2530	390
60	1800	188	2000	245
75	1700	172	1900	220

Koristeći podatke iz radova [19] i [20] moglo bi se posredno pretpostaviti da bi razorni projektil 155 mm, mase 60 kg iz cevi brodskog topa dužine L60 bio ispaljen sa početnom brzinom 1510 m/s. Grubom interpolacijom domet bi bio oko 130 km.



Slika 13 – Referentni projektil 155 mm mase 60 kg. U delu iza bojne glave smešten je sistem za navođenje i upravljanje

Prema procenama koje se javljaju u radovima objavljenim pre nekoliko godina, na primer [19], cena jednog KE projektila mogla bi da bude 5000 USD do 10 000 USD, zavisno od veličine efektivne energije. Imajući to u vidu, procena autora ovoga rada je da bi cena razornog projektila 155 mm, sa odgovarajućim sistemom za vođenje i upravljanje, mogla da bude od 40 000 do 45 000 USD.

Zaključak

Konvencionalni top je „toplotna mašina“ sa pouzdanom konverzijom primarne (toplotne) energije barutnog punjenja u mehaničku energiju klasičnog projektila, uz prihvatljiv koeficijent korisnosti (oko 30%). EM top zahteva da se tri puta vrši konverzija primarne energije u mehaničku energiju projektila, a posledica toga je da takva „mašina“ ima manji koeficijent korisnosti (oko 5% do 7%) i smanjenu pouzdanost osnovne funkcije.

Tokom poslednje dve dekade prošlog veka veoma intenzivno se radilo na razvoju tenkovskog EM topa. Jedno vreme se smatralo da će veću šansu za ugradnju u tenk imati ET ili ET-H topovi, jer je njihova prednost (u odnosu na šinski EM top) manja električna energija potrebna za lansiranje projektila, pa time i lakše akumuliranje energije u ograničenom prostoru tenka. Na osnovu analize izvršene u ovom radu zaključak je da će se odustati od ideje naoružavanja tenka EM topom bilo kojeg tipa, jer je više nego očigledno da se u tenku prihvatljive siluete, gabarita i mase ne može obezbediti zapremina za ugradnju pogonske grupe snage veće od 6 MW (što je znatno više od postojećih 1,1 MW na savremenim tenkovima).

Razvoj i ispitivanje funkcionalnih modela brodskih EM topova su tokom protekle dekade bili vrlo intenzivni i uglavnom uspešni (sa stanovišta provere principa dejstva). Za narednu fazu – projektovanje borbenog sistema EM topa, može se konstatovati:

– brod kao platforma rešava dva vitalna zahteva za mogućnost operativne upotrebe: poseduje pogonsku grupu velike moći, na razaračima čak i preko 70 MW; ne postoje ograničenja, sa stanovišta mase i prostora, za smeštaj snažnog EM topa nominalne energije 64 MJ;

– u postupku daljeg razvoja treba rešavati tehnička i konstrukciona pitanja bitna za projektovanje pojedinih sklopova i komponenata (sklop cevi, sklop projektila, sklop upaljača za razorne projektile, sklop punjača za postavljanja projektila u lansirnu cev koji bi obezbedio zahtevane brzine gađanja, sklopovi pokretanja cevi po elevaciji i pravcu, sklopovi akumuliranja potrebne električne energije, sklopovi električnog interfejsa za funkciju EM topa);

– konačno, za donošenje odluke za uvođenje brodskog EM topa u operativnu upotrebu treba sačiniti ozbiljnu analizu cena – efikasnost, upoređivanjem izvršenja postavljenih zadataka na dometima preko 400 km sa drugim naoružanjem, na primer, vođenim raketnim sistemima.

Ne pretendujući da raspolažu sa dovoljno podataka, znanja i iskustva u oblasti EM lansiranja projektila, inspirisani radovima i iskustvima onih koji su u ovu temu direktno uključeni (radovi [19], [20], [21]), autori ovoga rada zaključuju (iako se oni u mnogim procenama razlikuju od navoda u korišćenoj literaturi):

– u doglednoj budućnosti (bar 30 do 40 narednih godina) konvencionalni top (pogon na barut) i dalje će biti „ultima ratio regum“,[32] odnosno nosilac vatrene podrške kopnene vojske;

– EM top neće biti primenjen kao naoružanje osnovnog borbenog tenka. Ukoliko se, ipak, ponovo pokrene razvoj lovca tenkova naoružanog samo KE projektilima srednjeg kalibra (75 mm do 90 mm) moguća je eventualna primena EM topa energije oko 8 MJ, sa performansama probijanja oklopa sličnim onima koje ima konvencionalni top sa KE projektilom tipa APDSFS sa jezgrom od teškog metala;

– realna je mogućnost da se EM top uvede u operativnu upotrebu ugradnjom na brodske platforme i to za slučaj da se pored KE projektila uvede u upotrebu i razorni projektil, uz pretpostavku da budu rešeni svi tehnički problemi (navedeni u ovom radu) bitni za pouzdanu i bezbednu funkciju te vrste projektila;

– moguća je pretpostavka da će u operativnu upotrebu najverovatnije biti uveden brodski EM top kalibra 155 mm, sa dužinom cevi 60 kalibara, za dejstvo na dometima od oko 120 km. Šansa više za takvo rešenje je povratak na staru ideju odbrane strateških objekata stacionarnom/obalskom artiljerijom, ali sada korišćenjem topova sa EM pogonom (ukoliko se analizom cena – efikasnost potvrdi pretpostavka da su to najefektivnija borbena sredstva);

– optimistička procena je da će se eventualno uvođenja budućeg brodskog EM topa u operativnu upotrebu desiti tek posle 2030. godine.

Literatura

[1] Ristić, Z., Ilić, S. , Kari. A., Karakteristike trzanja elektromagnetskog topa, Vojnotehnički glasnik br. 4/2009, ISSN 0042-8469 Beograd.

[2] Paligorić, A., Ilić, R., Marjanović, B., Savremeni uređaji za ispaljivanje projektila velikim i vrlo velikim brzinama, Naučno-tehnički pregled, volumen XXXVIII, broj 10, Beograd, 1988.

[3] Schmidt, E. M. – Comparison of the recoil of conventional and electromagnetic cannon, Shock and Vibration 8, 2001, IOS Press.

[4] Jandrić, M., Elektromagnetni topovi, Kumulativna naučno-tehnička informacija, VTI, Beograd, 1993.

[5] Ogorkievicz, R. M, Future tanks guns – Part I: Solid and liquid propellant guns, International Defense Review, No 12, 1990.

[6] Fletcher, R., The case for the Raisable Tank Gun, Military Technology, No. 10, 1991.

[32] Parafraza čuvene izreke Luja XV, ispisana na francuskim srednjevekovnim topovima.

[7] Zukas, A. J. i drugi, Dinamika udara, pronikanie i probivanie tverdyh tel, Izdateljstvo MIR, Moskva, 1985.

[8] Drosen, H. Erich, Aspects of Modern Tank Design, Military Technology, No. 10, 1990.

[9] Ogorkievicz, R. M. Future tank guns – Part II: Electromagnetic and elecrothermal guns, International Defense Review, No 1, 1991.

[10] Compulsators, internet pretraživanje, februar 2010.

[11] Navy elecromagnetic rail gun, više izvora dobijenih Internet pretraživanjem, januar– februar 2010.

[12] Fanney, R., Navy fires EM cannon, internet pretraživanje, januar–februar 2010.

[13] Sofge, E., For true sci-fi fans, 14.11.2007., internet pretraživanje, februar 2010.

[14] Bishoni, R., Navy Rail Gun moves forward, 2.02.2007, internet pretraživanje, februar 2010.

[15] Page, L., US Navy orders new electric hyper kill Rail Gun, 11.02.2009, internet pretraživanje, februar 2010.

[16] Satapathy, S. & others - Design of an 8MJ Integrated Launch Package, IEEE No. 1, 2005.

[17] Tzeng, J. & Schmidt, E., Advanced materials bring EM gun technology one step closer to the battlefield, AMPTIAC Quatterly, No 4, 2004.

[18] Ellis, R. L. & others, Influence of bore and rail geometry on an EM naval railgun system, IEEE, 2004.

[19] McFarland, J. & McNab, I., A long rage naval gun, IEEE, No1. 2003.

[20] Shope, S. & others, Results of a study for a long range coilgun naval bombardment system, 10th U. S. Army gun dinamics Symposium, 23–26 april, 2001, in Austin, Texas.

[21] Marshall, R., Railgunery: Where nave we been? Where are we going?, IEEE No. 1, 2001.

ELECTROMAGNETIC GUN
– Still just a research project or the reality of the operational use

Abstract:

For more than a century researchers in many countries have been engaged in research and development of electromagnetic (EM) guns in order to launch projectiles with very high speed. In published sources many papers are related to theoretical considerations of certain phenomena of electrically driven projectiles and hardware solutions for electrical devices and components required for projectile launching. The works related to the philosophy of combat use, the concept of solutions and possibilities of application of such weapon systems are, however, less available to the public. The intention of the authors of this paper is to point out the basic problems of designing such wea-

pon systems, and to give the readers the information on the basis of which they can assess whether it is possible, when and on what kind of platform for the EM gun to be approved for the operational use.

Introduction

The intention of the authors is to present to the VTG readers an overview of the status of development and operational capabilities of electromagnetic guns (EM guns), as well as to present an opinion on the subject which for more than a century intrigues imagination and knowledge of the inventors: would the EM gun leave the laboratories to be used as an armament for land forces or navy combat systems, or as a component in the future space war inventory? This article deals only with the energetic aspect and conditions of creating required projectile kinetic energy. The fields of gun dynamics during projectile launching and target effectiveness are not analyzed.

Tendencies in the development of propulsion and projectiles of conventional weapons

This chapter contains the analysis of current classic fire support artillery weapons and tank guns to prove that the powder propellant is applicable for ballistic solutions allowing muzzle velocities with High-Explosive (HE) and Armor-Piercing Discarding Sabot Fin-Stabilized (APDSFS) projectiles based on kinetic energy (KE projectiles) up to 2000 m/s. Also, it briefly refers to the research of new types of propulsion to achieve higher initial velocity of the projectiles, states that there have been failed attempts (for now) to introduce liquid propellant and light gases, and that the research continues in the field of electromagnetic propulsion. A tabular overview of the most successful conventional solutions of tank guns is given to explain the level of realized muzzle energy of kinetic projectiles (up to 13 MJ).

Basic principles of EM gun functioning

The basic principles of the action of electromagnetic rail guns and coil guns are given, as well as the reasons why the research in the field of electro-thermal (ET) and electro-thermal-chemical guns (in order to obtain necessary propelling energy for projectiles in the process of chemical reactions), which began later, has been listed.

Defining the requirements for the design of tank EM gun

The paper analyzes the status and experiences of development in the world of the mid-80s of the last century suggesting the possibility of the EM gun to be mounted on armoured vehicles, especially tanks, in order to increase the impact energy on the target (KE projectile perforation ratio). The paper gives a proposal for project requirements: the energy required to launch a KE projectile; equipment required for the accumulation of electric power necessary for the execution of the wanted firing regimes; and power ratio of the vehicle power pack as a source of primary energy.

Analysis of the possibilities of mounting EM gun on a battle tank

Judging by the state of the development of EM gun laboratory models, realized in the last two decades of the past century, as well as by the fact that the expected technological progress in developing new generation of compulsators and high density capacitors has not been achieved, it can be concluded that there is no real possibility of mounting an EM gun onto the last generation battle tanks. The requirements defined in the previous chapter conclude that the required power of the power pack for an EM tank gun must be greater than 6000 kW. Unfortunately, available space in the tank hull is 5 to 6 times smaller than the volume needed to accommodate a new 6000 kW power pack.

Ship as a platform for mounting an EM gun

In the period after the year 2000, American engineers started a research in order to design a functional model of an electromagnetic naval rail gun (based on the experience gained during the development of the tank EM gun). The reasons are more than obvious - the ship is (compared to the tank) an adequate platform for mounting a large and complex functional model of the EM gun, and marine engine power is significantly greater than tank engines power (therefore, it is much easier to solve the demand for the necessary primary power).

The status of the development of a future naval EM gun, which is in development by the U.S. Navy and Army jointly, is given in details. Development programs include a number of laboratory EM guns having effective kinetic energy of 2 to 64 MJ and the ultimate goal is the development of guns of 64 MJ for the ranges over 200 miles (>360 km). So far, an EM gun of 8 MJ effective energy has been successfully tested, and the examination of the 32 MJ EM gun is planed during year 2011.

Significant progress has been made in the design of the barrel assembly and the assembly of the KE projectile, and the development of the HE projectile is indicated as being necessary (after solving the technical problems of the development of the fuze exposed to acceleration twice larger than the acceleration of the projectile in conventional guns). However, the development of electric generators and components of EM guns is still not at the level acceptable for operational use.

Conclusion

A conventional gun is a weapon with reliable function and simple conversion of primary energy (chemical energy of powder) into mechanical energy of movement of classical projectiles, with an acceptable coefficient of utility (30%). In contrast, an EM gun requires three conversions of primary energy into the mechanical energy of an EM projectile. Therefore, it has a lower utility ratio of primary energy (about 5% to 7%) and reduced reliability of basic functions. In due time in the future (for at least 30 to 40 next years) a conventional gun (with powder propellant) will thus still be a carrier of fire support for land forces.

Based on the analysis made in this paper, the conclusion is that the idea of the tank armed with an EM gun of any type is going to be abandoned, because it is more than obvious that a tank of acceptable silhouettes, dimensions and weight may not provide the volume for mounting the power pack requiring a power of 6000 kW.

The development of functional models of naval EM guns over the past decade was very intense and largely successful. Ships as platforms address two vital requirements for the possibility of operational use of EM guns: they already have the power pack of high power ratio, even over 70 MW; and there are no restrictions, from the standpoint of weight and space, to accommodate a strong EM gun of effective kinetic energy of 64 MJ.

If HE projectiles, besides KE projectiles, are introduced, the possibility to see the system of naval EM gun in operational use is real, assuming that all technical issues important for a reliable and safe function of this type of projectiles have been previously resolved.

Prior to the decision about the introduction of naval EM guns in operational use, a serious analysis should be carried out on the cost-effectiveness, comparing the performance of combat tasks and missions (for ranges > 360 km) with other weapons, such as existing long range missile systems.

The authors of this paper suggest that the future naval EM gun of 155 mm calibre has the highest probability of entering the operational use for the ranges of about 120 km.

Finally, the optimistic estimate is that the possible introduction of future naval EM guns in operational use will occur after the year 2030.

Keywords: *artillery weapon, conventional gun, electromagnetic gun, EM gun, EM rail gun, EM coil gun, electro-thermal gun, tank EM gun, naval EM gun, generator, capacitor, compulsator, APDSFS projectile, KE projectile, HE projectile.*

Datum prijema članka: 17. 03. 2010.

Datum dostavljanja ispravki rukopisa: 02. 04. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 04. 04. 2010.

POZICIONIRANJE, ORIJENTISANJE I ODREĐIVANJE DALJINE DO CILJA NA SAMOHODNOM VIŠECEVNOM RAKETNOM LANSIRNOM SISTEMU KORIŠĆENJEM GPS I ELEKTRONSKIH KARATA

Sekulović J. *Dragoljub*, Vojna akademija, Dekanat, Beograd,
Đurković P. *Vlado*, Vojna akademija, Katedra prirodnomatematičkih i tehničkih nauka, Beograd,
Milošević B. *Milan*, Vojnotehnički institut, Sektor za naoružanje i vozila, Beograd

UDC: 623.465.5

Sažetak:

U radu je prikazano pozicioniranje i orijentisanje višecevnog raketnog sistema korišćenjem GPS prijemnika i određivanje rastojanja od lansera do cilja upotrebom geografskih koordinata. Koordinate koje se koriste za zadavanje pozicije cilja su geografske ili UTM, a dobijene su sa elektronske karte terena.

Ključne reči: *geografsko-informacioni sistemi, elektronske karte, višecevni lanser raketa, nevođena raketa, elementi gađanja, sistem za upravljanje vatrom.*

Uvod

Kod modernih sistema za upravljanjem vatrom (SUV) obavezna je upotreba geografskih informacionih sistema (GIS). Raketni lansirni sistemi poslednje generacije podrazumevaju da svako oruđe ima svoj oruđni SUV [1]. SUV je namenjen za određivanje elemenata gađanja i korekturu vatre na osnovu osmatranja pogodaka na cilju [2]. Sastoji se od sledećih podsistema:

1. uređaja za zemaljsku orijentaciju i navigaciju;

2. uređaja za proračun elemenata gađanja takozvanog balističkog modula;

sekulovicdr@yahoo.co.uk

3. uređaja za određivanje prizemnih meteoroloških podataka;

4. podsistema za osmatranje;

5. upravljačko-izvršnih organa za zauzimanje elemenata gađanja;

6. uređaja za nišanjenje (nišanske sprave);

7. podsistema za vezu (radio-uređaji).

Određivanje pozicija lansera i cilja, a takođe i drugih objekata, nezamislivo je bez elektronskih karata.

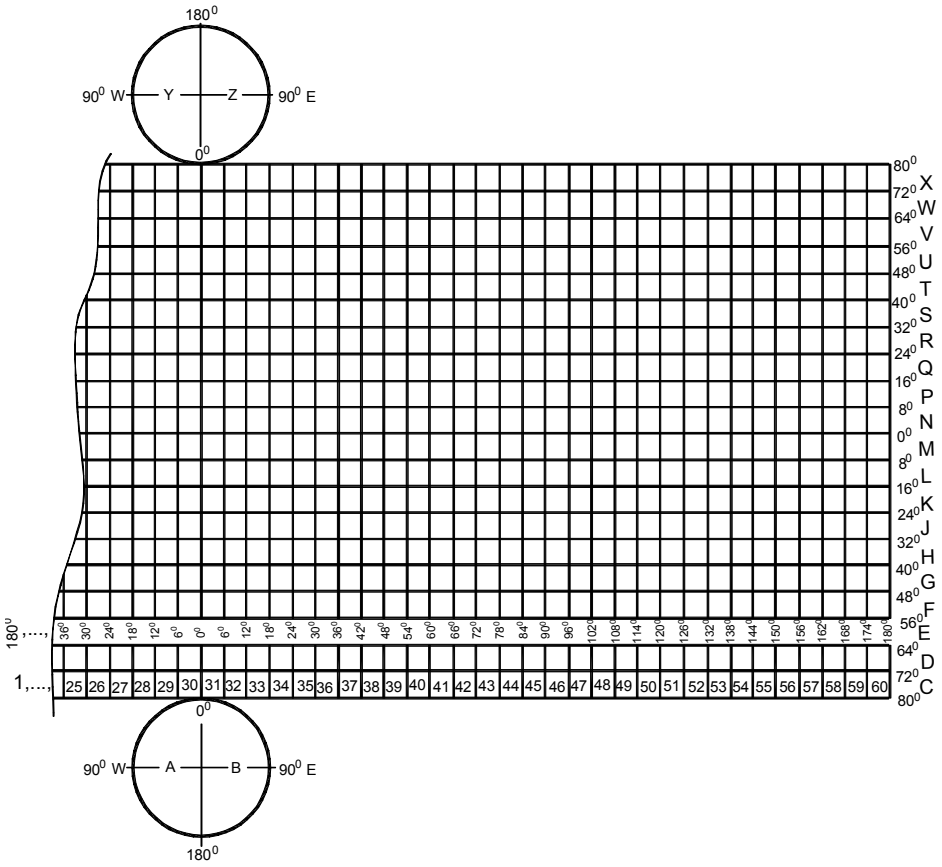
Koordinatni sistemi i kartografske osnove

Dosadašnje topografske karte rađene su u konformnoj Gaus-Krigerovoj kartografskoj projekciji trostepenih zona, na bazi lokalnog Zemljinog elipsoida Besela 1841, gde je koordinatni početak vezan za grinički meridijan [3, 4, 5, 6].

Nove karte zahtevaju kompatibilnost sa STANAG (Standardization Agreement), pa se karte rade prema globalnom elipsoidu WGS84 (World Geodetic System 1984) i prema univerzalnoj poprečnoj Merkatorovoj projekciji UTM (The Universal Transverse Mercator).

Koordinatni sistem je definisan imenom, jedinicama koje koristi, smerom i redosledom *osa*, a čini skup uslovljenih fiksnih linija koje služe za jednoznačno određivanje položaja tačke na nekoj ravni, matematički zadatoj krivoj površi ili u prostoru uopšte.

Projekcija UTM (Svetska poprečna Merkatorova projekcija ili Univerzalna poprečna Merkatorova projekcija) u stvari je izraz anglosaksonskog porekla za modifikiovanu Gaus-Krigerovu projekciju. I pored toga što se u literaturi, naročito kod nas, vrlo često govori o UTM projekciji, u širem smislu, reč je zapravo o referentnom koordinatnom sistemu. To je koordinatni sistem za koji je jasno definisan datum (WGS84 – Svetski Geodetski Sistem) i pravila za obeležavanje površina i tačaka. WGS84 je geocentrični geodetski datum, globalnog karaktera, koji za matematičku aproksimaciju Zemlje koristi parametre Geodetskog referentnog sistema 1980 (GRS80 – Geodetic Reference Sustem). Sistem se zasniva na teoriji nivojskog, geocentričnog, obrtnog elipsoida, izraženog parametrima realne Zemlje.



Slika 1 – Prvi stepen obeležavanja
Figure 1 – The first level of description

Sjedinjene Američke Države prve su usvojile UTM projekciju 1947. godine, a usavršile 1951. godine, stvarajući uslove da cela Zemljina površina, uz jedno ograničenje, bude obuhvaćena jedinstvenim koordinatnim sistemom. Kasnije će se pokazati da je ovaj potez, pored ostalog, olakšao Sjedinjenim Državama vođenje rata u bilo kom delu sveta [7, 8].

Ograničenje se odnosi na polarne oblasti. Naime, zbog izražene konvergencije meridijana u polarnim oblastima, što bi dovelo do neprihvatljivih deformacija kod UTM projekcije, ove oblasti čine posebne celine i za njihovo predstavljanje koristi se univerzalna polarna stereografska projekcija (UPS – Universal Polar Stereographic). Univerzalna polarna stereografska projekcija je komplementarna sa UTM koordinatnim sistemom, ali i nezavisna od njega. Danas UTM koordinatni sistem predstavlja standard za sve države članice NATO saveza.

Osnovne karakteristike UTM koordinatnog sistema su:

• šestostepenske dužinske zone (ukupno 60 zona, početak prve zone je „datumska granica“, tj. srednji meridijan prve zone ima longitudu 177° zapadne geografske dužine);

• susedne zone se preklapaju u pojasu od 400.000 m;

• metar kao merna jedinica;

• uslovna vrednost apscise (ekvatora) za severnu hemisferu je 0 m, a za južnu 10.000.000 m, tako da sve apscise imaju pozitivnu vrednost;

• uslovna vrednost ordinata (srednji meridijan zone) je 500.000 m, tako da sve ordinate imaju pozitivnu vrednost;

• konstantni linearni modul razmere m = 0,9996 (razmer duž srednjeg meridijana, udaljavanjem od srednjeg meridijana zone razmer se povećava);

• pravougle koordinate se jedinstveno određuju za sve zone;

• formule za transformaciju koordinata iz jedne zone u drugu su jedinstvene, i

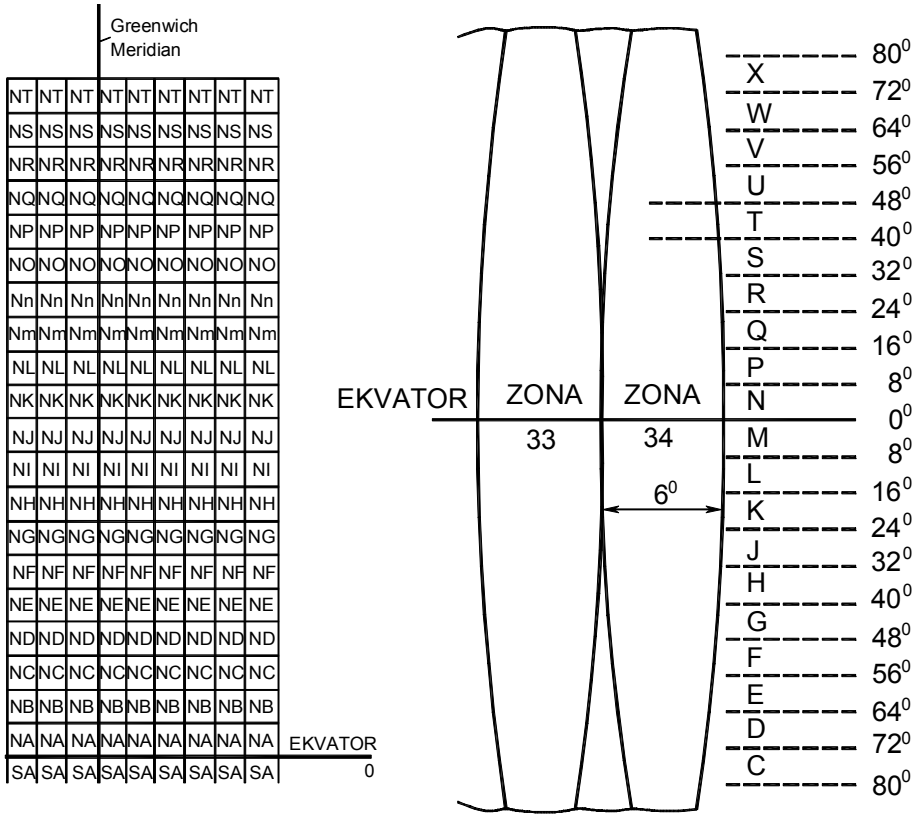
• konvergencija meridijana ne prelazi 5°.

Cilj sistema obeležavanja površina i tačaka jeste da omogući jednoznačno obeležavanje ma koje površine ili tačke na celoj Zemlji, isključujući svako opisno objašnjavanje gde se ta tačka nalazi. Ovaj sistem identifikacije mreže predstavlja standard koji se primenjuje na svim vojnim kartama članica NATO-a.

Sistem sadrži tri stepena obeležavanja. *Prvi* i *drugi* stepen označavaju površine, a *treći* položaj tačaka unutar tih površina.

U prvom stepenu obeležavanja Zemljina površina između 80°N i 80°S je meridijanima i paralelama podeljena na redove i kolone (sl. 1). Uzastopna rastojanja meridijana iznose 6°, a uzastopna rastojanja paralela 8°. Kolone se obeležavaju arapskim brojevima od 1 do 60; a redovi velikim slovima abecede, počev od C do zaključno X, pri čemu su slova I i O ispuštena. Slova A, B, Y i Z rezervisana su za obeležavanje severnog i južnog polarnog prostora. Svaka tako ograničena površina naziva se zonom (Grid Zone Designation). Svaka zona obeležava se oznakom kolone i reda. Tako bi zona koja obuhvata deo naše teritorije nosila oznaku 34 T. Ovaj stepen obeležavanja koristi se samo kada se želi definisati prostor u okviru svetskih relacija, a u lokalnom obeležavanju obično se izostavlja.

U drugom stepenu obeležavanja (sl. 2), svaka zona se deli na kvadratne površine sa stranama od 100 km (meter square Identification). Kvadrati se baziraju na UTM pravougloj mreži. Početak kvadriranja poklapa se sa koordinatnim početkom svake UTM zone. Počev od 180° meridijana, idući istočno duž Ekvatora u intervalima od po 18°, kolone kvadrata obeležavaju se slovima od A do Z (slova I i O su ispuštena).

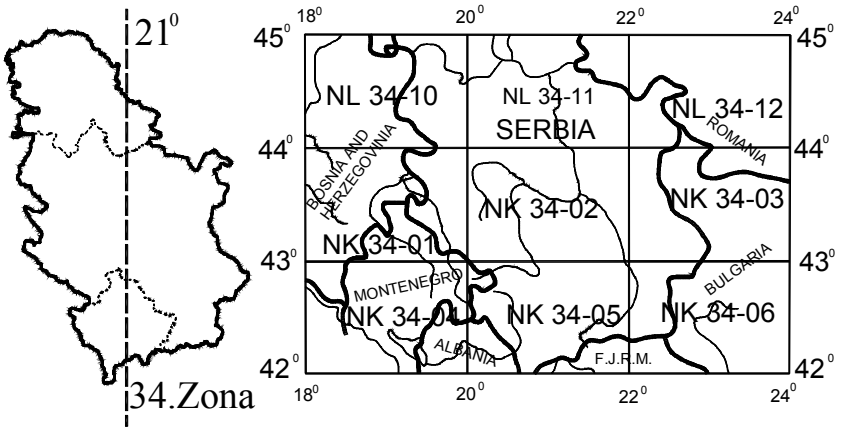


Slika 2 – Drugi stepen obeležavanja
Figure 2 – The second level of description

Obeležavanje redova u neparnim zonama počinje od juga prema severu, slovima A do V (slova I i O su izostavljena). Abeceda se ponavlja svakih 2.000.000 m. U parno obeleženim zonama redovi počinju da se obeležavaju *abecednim* redom, počev od apscisne linije mreže sa vrednošću 500.000 m, i to isto tako od juga prema severu.

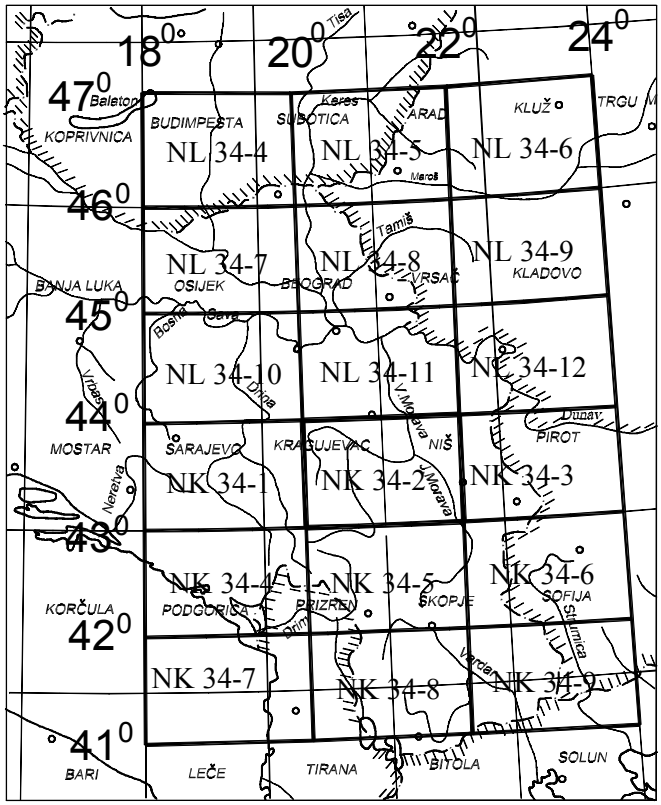
Broj kvadrata sa stranama od 100 km nije isti u svim zonama. Dok je broj redova isti na svim širinama, broj kolona se smanjuje povećavanjem geografske širine. Tako na 80. paraleli ostaju samo dve kolone. S obzirom na to što UTM obuhvata celu Zemljinu površinu, ovakvo obeležavanje ne može se smatrati savršenim.

Prema ovoj podeli teritorija Srbija pripada zoni 34T (sl. 3 i 4).



Slika 3 – Treći stepen obeležavanja
Figure 3 – The third level of description

Slika 4 – Skica položaja lista karte
Figure 4 – Chart of the map position



Slika 5 – Listovi karte i podela
Figure 5 – Map sections and map allocation

Dok je pri obeležavanju zona identifikovanje jednostavno, to nije slučaj i sa obeležavanjem kvadrata. Zato se izdaju posebni registri u vidu skica pojedinih geografskih regiona, u kojima je podela na kvadrate sa stranama od 100 km sa svojim oznakama (sl. 5).

Na preglednim skicama postoji i podatak o tome na kojem sferoidu je određena teritorija izračunata.

Treći stepen obeležavanja određuje položaj tačke pravouglim koordinatama sa željenom tačnošću. Sistem se sastoji od uzastopnogređanja slova i brojki, bez tačaka, zareza, povlaka ili decimala. Način obeležavanja može se sagledati iz datog primera.

Numerička oznaka tačke uvek sadrži paran broj cifara, bez obzira na to sa kojom tačnošću će se tačka obeležiti. Prva polovina cifara predstavlja veličinu ordinate, a druga apscise. Pri tome se, zavisno od razmera karte, neka početna slova i brojke mogu izostavljati radi kraćeg pisanja.

Ciljevi GIS-a:

• Skladištenje, operisanje i povezivanje velikog broja podataka – prostornih (tačka, linija, oblast) i neprostornih (opisne informacije);

• Kako bi se analizirali geografski podaci – gde su oblasti koje pokriva naoružanje napadača, oblikovanje logističkih ruta na vojištu i drugo i

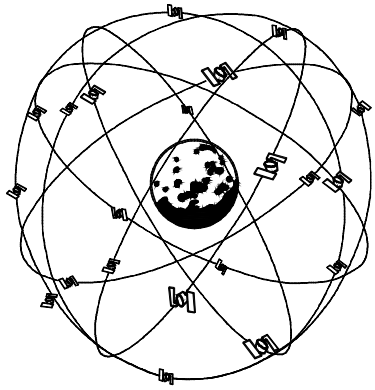
• Kako bi se obradili svi ovi podaci kojima korisnik sa lakoćom može da pristupi.

Moguće primene DMT u Vojsci

• Geomorfološke karakteristike terena, tj. vizualizacija reljefa;
• Optička vidljivost i dogledanje;
• Nagib terena i izrada karte tenkoprohodnosti;
• Izrada profila i analiza zemljišta sa vojnog i bezbedonosnog aspekta.

AMERIČKI – sistem NAVSTAR GPS

U operativnoj upotrebi od 1993. godine GPS sateliti su postavljeni u 6 orbita zakošenih za 55° na visini od 20 km do 200 km i imaju vreme obilaska od 12 sati. Za normalan rad sistema potrebno je 24 satelita (sl. 6).



Slika 6 – Američki sistem NAVSTAR GPS
Figure 6 – US NAVSTAR GPS system

Pozicioniranje lansera raketa na vatrenom položaju

Samohodni višecevni raketni lanseri poslednje generacije pozicioniraju se i orijentišu na vatrenom položaju preko GPS (Global Positioning System) prijemnika. Jedan od načina orijentacije u odnosu na sever jeste orijentisanje pomoću *letve* na kojoj se nalaze dve GPS antene (sl. 7, 8). Dužina letve na kojoj se nalaze antene diktira i tačnost orijentacije prema severu.

Azimut lansirnog oruđa određuje se jednačinom

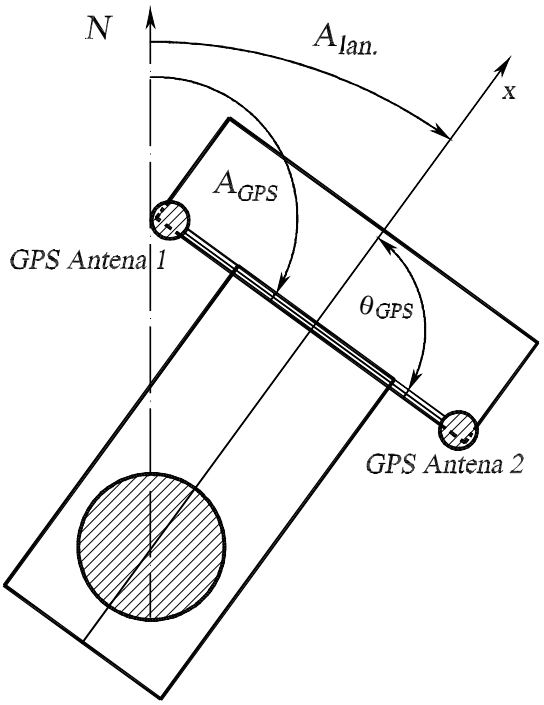
$$A_{lan} = A_{GPS} - \theta_{GPS}\,, \tag{1}$$

gde je:

$A_{lan.}$ – azimut lansirnog oruđa;

A_{GPS} – azimut letve na kojoj se nalaze antene i

θ_{GPS} – ugao ugradnje letve u odnosu na podužu osu vozila.



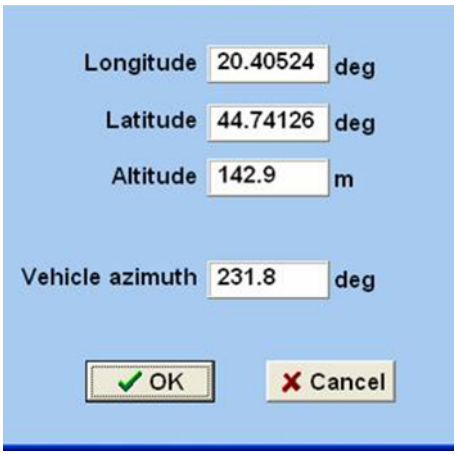
Slika 7 – Orijentacija pomoću GPS prijemnika sa dve antene
Figure 7 – Orientation using a GPS receiver with two antennas

Primer ugradnje antena prikazan je na sl. 8. Jedna antena koristi se za pozicioniranje, a obe za orijentisanje, tj. određivanje azimuta. Preko risivera podaci se prosleđuju računaru gde se vrši njihova obrada. Obrađeni podaci prikazani su u jednom prozoru SUV-a (sl. 11), gde su prikazane geografska dužina, širina, nadmorska visina i azimut oruđa na vatrenom položaju. Izgled GPS antena prikazan je na sl. 9, a risivera za prijem i obradu podataka na sl. 10.

Slika 8 – Letva sa GPS antenama na jednom oglednom vozilu
Figure 8 – Rod with two GPS antennas on an experimental vehicle

Slika 9 – GPS antene
Figure 9 – GPS antennas

Slika 10 – Izgled jednog risivera za prijem i obradu podataka
Figure 10 – A receiver for data acquisition and processing



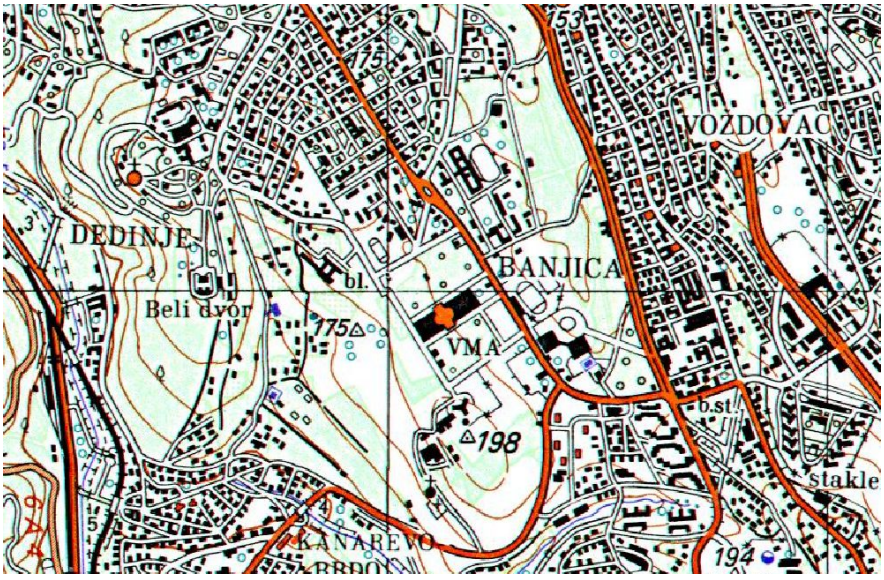
Slika 11 – Izgled prozora u SUV-u za prikaz pozicije i orijentacije lansera
Figure 11 – Window in the FCS for displaying the launcher position and orientation

Elektronske karte

Da bi se dobila elektronska karta u ravni prvo mora da se skenirana karta terena u *jpg* ili *bmp* formatu u što većoj rezoluciji, najbolje 300 tačaka po inču (sl. 12). Na toj karti treba poznavati najmanje šest tačaka čije su koordinate unapred poznate, a određene su pomoću GPS prijemnika ili na neki drugi način. Pomoću nekog softverskog paketa, kao što je GeoMap ili ArcGIS, vrši se kalibracija i digitalizacija karte.

Na elektronskoj karti mogu se prikazivati svi objekti koji su od vitalnog značaja, kao što su:

- lansirna oruđa;
- ciljevi koje treba uništiti;
- komandna mesta;
- osmatrači i drugo.

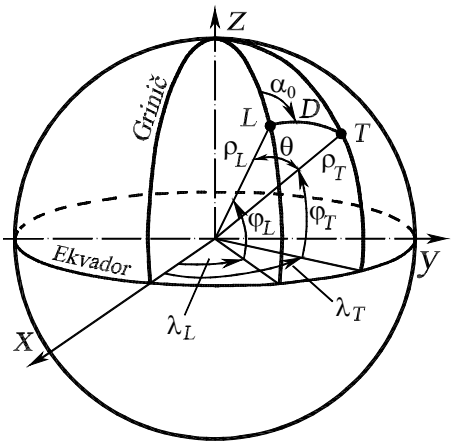


Slika 12 – Elektronska karta TK 100 sa učitanim objektima
Figure 12 – TK 100 Electronic map with objects

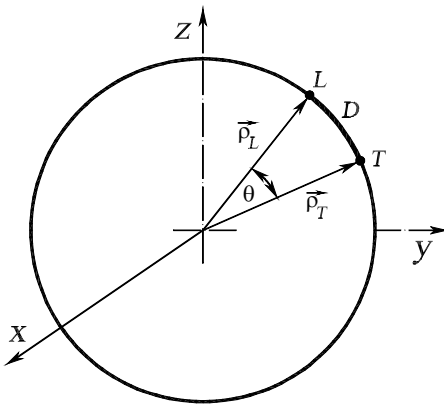
Izračunavanje rastojanja i azimuta od lansera do cilja

Da bi izračunali rastojanje između dve tačke na Zemlji poslužićemo se geografskim koordinatnim sistemom (ρ, φ, λ) (sl. 13). Geografski koordinatni sistem ima za koordinatni početak središte Zemlje. Koordinata ρ je poteg tač-

ke gde se nalazi lanser raketa, φ je geografska širina merena uglom između potega mesta lansera i ravni Zemljinog ekvatora i λ je geografska dužina merena uglom između griničkog meridijana i meridijana mesta na kojem se nalazi lanser sa pozitivnim smerom od griničkog meridijana prema istoku.



Slika 13 – Geografski koordinatni sistem
Figure 13 – Geographical coordinate system



Slika 14 – Vektori položaja lansera, cilja i ugao između njih
Figure 14 – Launcher and target position vectors and the angle between them

Pozicija vatrenog položaja definisana je sa tri koordinate h_L, λ_L, φ_L, gde su: h_L – visina vatrenog položaja; λ_L – geografska dužina vatrenog položaja i φ_L – geografska širina vatrenog položaja.

Pozicija cilja definisana je sa tri koordinate h_T, λ_T, φ_T, gde su: h_L – nadmorska visina cilja; λ_T – geografska dužina cilja i φ_T – geografska širina cilja.

Rastojanje između lansera i cilja biće rešeno tako što će sferne koordinate biti prebačene u pravougaone, za tačku *L*, odnosno:

$$\begin{aligned} x_L &= \rho_L \cos\varphi_L \cos\lambda_L , \\ y_L &= \rho_L \cos\varphi_L \sin\lambda_L , \\ z_L &= \rho_L \sin\varphi_L \end{aligned} \tag{2}$$

i za tačku *T*

$$\begin{aligned} x_T &= \rho_T \cos\varphi_T \cos\lambda_T , \\ y_T &= \rho_T \cos\varphi_T \sin\lambda_T , \\ z_T &= \rho_T \sin\varphi_T . \end{aligned} \tag{3}$$

Pošto su u pitanju dometi 10–70 km može se usvojiti da su poluprečnici Zemlje na mestu lansera i cilja isti sa srednjom vrednošću prema jednačini (4) i sl. 14,

$$\rho_L = \rho_T = 6.378.101\,\mathrm{m}\,. \tag{4}$$

Skalarni proizvod vektora položaja lansera i cilja može se prikazati jednačinom (5).

$$N = \rho_L \cdot \rho_T \cos\sphericalangle\left(\vec{\rho}_L, \vec{\rho}_T\right) = \rho_L \cdot \rho_T \cos\theta = \rho^2 \cos\theta\,, \tag{5}$$

gde je $\rho_L = \rho_T = \rho$.

S druge strane, može se prikazati da je

$$\rho_L \cdot \rho_T \cos\theta = x_L \cdot x_T + y_L \cdot y_T + z_L \cdot z_T\,. \tag{6}$$

Izjednačavanjem jednačine (4) i jednačine (5) i njihovim sređivanjem može se lako doći do jednačine (6) u obliku

$$\cos\theta = \cos\varphi_L \cos\lambda_L \cos\varphi_T \cos\lambda_T + \\ + \cos\varphi_L \sin\lambda_L \cos\varphi_T \sin\lambda_T + \sin\varphi_L \sin\varphi_T\,. \tag{7}$$

Lučno rastojanje između lansera i cilja dato je kao

$$D = \frac{\theta\pi}{180^0}\rho\,. \tag{8}$$

Zamenom jednačine (7) u jednačinu (8) dolazimo do rastojanja između lansera i cilja jednačina

$$D = \frac{\rho\pi}{180^0} arc\cos(\cos\varphi_L \cos\lambda_L \cos\varphi_T \cos\lambda_T + \\ + \cos\varphi_L \sin\lambda_L \cos\varphi_T \sin\lambda_T + \sin\varphi_L \sin\varphi_T)\,. \tag{9}$$

Azimut gađanja (sl. 13) može se prikazati preko jednačine (10):

$$\cos\alpha_0 = \frac{\sin\varphi_T - \sin\varphi_L \cos\theta}{\cos\varphi_L \sin\theta}\,. \tag{10}$$

Zaključak

Ugradnjom GPS prijemnika sa dve antene dobija se pozicija lansirnog oruđa i njegov azimut. Na osnovu geografskih ili UTM koordinata sa GPS prijemnika i azimuta oruđa njegov položaj je potpuno određen u prostoru. Podaci o cilju uzimaju se sa elektronske karte direktnim marki-

ranjem zadatog cilja na displeju računara, posle čega se vrši automatsko određivanje rastojanja do cilja, a zatim se određuju elementi gađanja za zadate uslove.

Uvođenjem orijentacije preko GPS prijemnika i elektronskih karata izvršena je potpuna autonomnost višecevnog lansirnog sistema sa novom i savremenom koncepcijom sistema za upravljanje vatrom.

Literatura

[1] Siouris, M. G., *Missile Guidance and Control System*, Springer-Verlag, New York, Inc. 2004.

[2] ArcGis 9.2, *ESRI*, October 2006.

[3] Nenadović, M., *Osnovi kosmičkog leta*, Institut tehničkih nauka SANU, Beograd, 1979.

[4] Sekulović, D., Gigović, Lj., *Geografski informacioni sistemi u komandnim i kontrolnim informacionim sistemima*, SYM-OP-IS 2008. Soko Banja, 2008

[5] Jovanović, V., *Matematička kartografija*, Vojnogeografski institut, Beograd, 1983.

[6] Borčić, B., *Gauss – Krugerova projekcija (teorija i primena u državnom premeru)*, VGI, Beograd 1955.

[7] Banković, R., Tatomirović S., T*opografska karta 1 : 250 000 – prva karta po NATO standardu izrađena u vojsci Srbije*, OTEH, Beograd–Žarkovo, 2007.

[8] Borisov, M., Tatomirović, S., Banković, R., *Nacionalna infrastruktura geoprostornih podataka u razmeri 1:25000,* SYM-OP-IS 2008, Soko Banja, 2008, pp. 153–156.

POSITIONING, ORIENTATION AND DETERMINATION OF THE DISTANCE TO TARGET ON A SELF – PROPELLED MULTIPLE ROCKET LAUNCHER SYSTEM USING GPS AND ELECTRONIC MAPS

Summary:

The GPS positioning and orientation of a self-propelled multiple rocket launcher is presented. The determination of the distance from the launcher to target using geographic coordinates is given as well The coordinates applied in determining the target position are either geographic or UTM coordinates while terrain electronic maps are obtained as a result.

Introduction

Modern firing control systems (FCSs) require the use of geographic information systems (GIS). All rocket launcher systems of the last generation are equipped with FCSs.

Coordinate systems and cartographic base

Previous topographic maps were made in the Gauss-Kruger cartographic projection with tree-degree zones.

Since new maps require compatibility with STANAG (Standardization Agreement), they are made in accordance with global ellipsoid WGS84 (World Geodetic System 1984) and the universal transverse Mercator projection UTM (The Universal Transverse Mercator).

A coordinate system is defined by its name, the units used, the direction and the order axis, and consists of a set of fixed lines used to uniquely determine the position of points in a plane, mathematical curved surface or in space in general.

The UTM projection (World transverse Mercator projection or Universal transverse Mercator projection) is in fact an expression of Anglo-Saxon origin for a modified Gauss-Kruger projection.

The United States first adopted the UTM projection in 1947, and perfected it in 1951. Today the UTM coordinate system is standard for all NATO member states.

Positioning the rocket launcher in the firing position

A self-propelled multiple rocket launchers of the last generation is positioned and oriented to the fire position by a GPS receiver.

The length of rods with antennas is largely dictated by antennas and the accuracy of the orientation towards the North. The launcher azimuth is determined by the equation

$$A_{lan} = A_{GPS} - \theta_{GPS},$$

Where: $A_{lan.}$ *– launcher azimuth;* A_{GPS} *– azimuth of the rod with GPS antennas; and* θ_{GPS} *– angle of rod mounting to the vehicle longitudinal axis.*

Electronic maps

For obtaining an electronic map in the plane, the terrain map in. jpg or. bmp format must be first scanned in a highest resolution possible. This map should contain at least six points the coordinates of which are already known in advance, obtained by a GPS receiver or by some other method. Software packages such as ArcGIS or GeoMap are used for calibration and digitization of maps.

Calculating the distance and the azimuth from the launcher to the target

The geographic coordinate system (ρ, φ, λ) *is used to calculate the distance between two points on the ground.*

The distance between the launcher and the target is given by the equation

$$D = \frac{\rho\pi}{180^0} arc\cos(\cos\varphi_L \cos\lambda_L \cos\varphi_T \cos\lambda_T +$$
$$+\cos\varphi_L \sin\lambda_L \cos\varphi_T \sin\lambda_T + \sin\varphi_L \sin\varphi_T),$$

and the firing azimuth can be obtained by the equation

$$\cos\alpha_0 = \frac{\sin\varphi_T - \sin\varphi_L \cos\theta}{\cos\varphi_L \sin\theta}.$$

Conclusion

Installing a GPS receiver with two receiving antennas results in obtaining the launcher position as well as its azimuth. Target data are taken from the electronic map by directly marking a previously determined target on the computer display, which is followed by automatic target distance determination and determination of firing elements for the given conditions.

Introduction of GPS receivers and electronic maps in orientation leads to a full autonomy of multiple rocket launcher systems with a new and modern concept of firing control systems.

Key words: *Geographic information systems, electronic maps, multiple rocket launcher, unguided rocket, firing elements, fire control system*.

Datum prijema članka: 15. 01. 2010.
Datum dostavljanja ispravki rukopisa: 22. 01. 2010.
Datum konačnog prihvatanja članka za objavljivanje: 24. 01. 2010.

SOL-GEL SINTEZA I MAGNETNE OSOBINE NANOČESTIČNOG HEMATITA

Tadić M. *Marin*, Institut za nuklearne nauke Vinča, Laboratorija za teorijsku fiziku i fiziku kondenzovane materije, Beograd,
Čitaković M. *Nada*, Vojna akademija, Katedra prirodnomatematičkih i tehničkih nauka, Beograd

UDC: 661.872'021:621.318
549.517.2:621.318

Sažetak:

U radu je prikazano istraživanje magnetnih karakteristika nanočestičnog feri-oksida, α-Fe_2O_3 (hematita), koji ispoljava superparamagnetne karakteristike tj. superparamagnetizam. Prikazano je nanočestično ponašanje uzoraka, upoređene su karakteristike nanočestičnog materijala sa materijalom visokog kristaliniteta i prikazan je uticaj veličine nanočestica na magnetne karakteristike.

Ključne reči: *nanostrukturisani materijali, magnetna merenja, magnetizacija, sol-gel metoda, superparamagnetizam, transmisiona elektronska mikroskopija-TEM, Morinov prelaz*.

Sinteza, difrakcioni eksperimenti i transmisiona elektronska mikroskopija

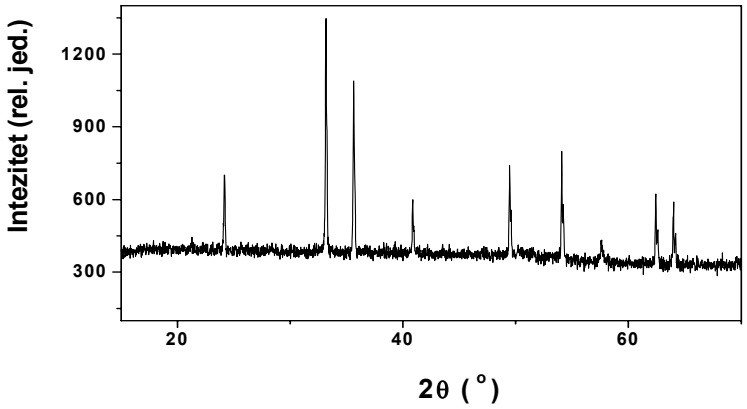
Nanočestični hematit sintetisan je sol-gel postupkom, korišćenjem gvožđe nitrata $Fe(NO_3)_3 \cdot 9H_2O$, etanola CH_3CH_2OH, TEOS-a (tetraetilortosilikat, $Si(OCH_2CH_3)_4$) i azotne kiseline HNO_3 kao polaznih supstanci. Molarni odnosi etanola prema TEOS-u i vode prema TEOS-u uzeti su 4:1 i 11,67:1. Izabrano je da konačni maseni udeo hematita u uzorku bude 30%. Posle mešanja rastvora podešena je pH vrednost na 2. Dobijeni gel je sušen deset dana na temperaturi do 100°C, zatim je uzorak žaren na temperaturi od 400°C u vazduhu 5 sati. Ovako dobijeni uzorci su usitnjeni u prah, a zatim su izvršena merenja.

Dobro iskristalisani hematit (veličina kristalita preko 10 μm), tj. uzorak visokog kristaliniteta dobijen je žarenjem gvožđe nitrata $Fe(NO_3)_3 \cdot 9H_2O$ na temperaturi 900°C u vazduhu 9 sati, a zatim su ispitivane njegove karakteristike.

Snimanja difraktograma izvršena su na sobnoj temperaturi na difraktometru za prah *Philips PW* 1050. Kao izvor x-zraka korišćeno je zračenje bakarne antikatode $K\alpha_{1/2}$, talasnih dužina λ_1 = 1,5405 Å i λ_2 = 1,5443 Å, respektivno. Snimanje je izvršeno sa korakom 0,02° i ekspozicijom 4 s po koraku.

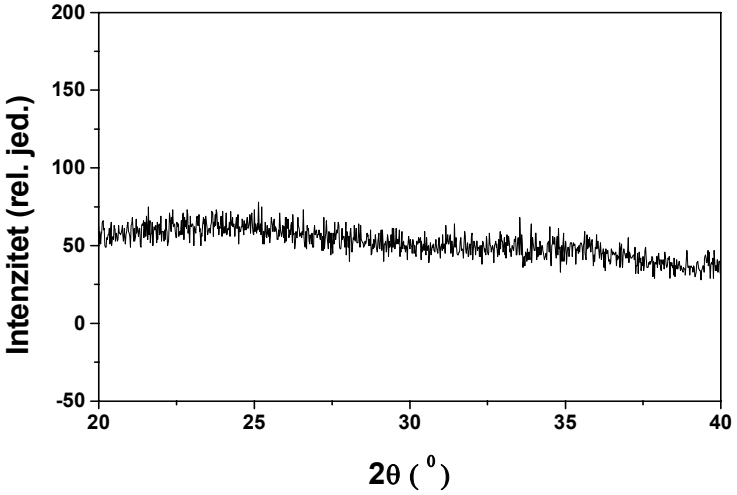
marint@vinca.rs

Analizom difraktograma za uzorak koji je dobijen direktnim žarenjem gvožđenitrata potvrđeno je postojanje dobro iskristalisanog hematita (veličina kristalita veća od 1 μm), bez prisustva neke druge faze (slika 1).



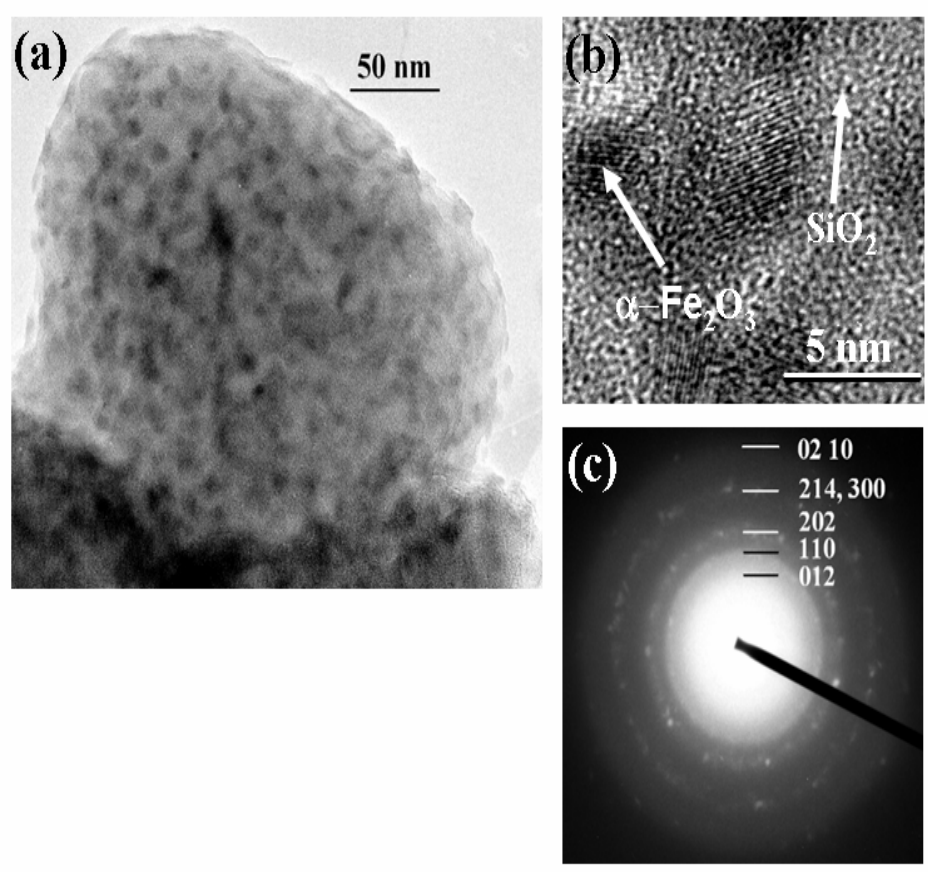
Slika 1 – Difraktogram uzorka α-Fe_2O_3 visokog kristaliniteta, dobijen rasejanjem x-zraka
Figure1 – X-ray diffraction pattern of high cristallinity *α* -Fe_2O_3/SiO_2

Analizom difraktograma za nanočestični hematit (slika 2) uočeni su samo veoma široki maksimumi koji pripadaju amorfnom SiO2, pa je kristalna struktura morala biti utvrđena nekom drugom eksperimentalnom tehnikom.



Slika 2 – Difraktogram nanočestičnog uzorka α-Fe_2O_3, dobijen rasejanjem x-zraka
Figure 2 – X-ray powder diffraction pattern of the nanocomposite α-Fe_2O_3/SiO_2

Veličina nanočestica i kristalna struktura određena je pomoću TEM-a i visoko rezolucionog transmisionog elektronskog mikroskopa (HR-TEM). Slike i odgovarajuća elektronska difrakcija prikazane su na slici 3. Na slici 3.a vidimo jedno zrno amorfnog silicijumdioksida u kojem su ravnomerno raspoređene nanočestice hematita. Čestice su sfernog oblika, veličine nekoliko nanometara sa uskom distribucijom po veličini. Slika 3.b jasno pokazuje da se radi o nanočesticama veličine oko 4 nanometra. Elektronska difrakcija je potvrdila da se radi o fazi hematita (slika 3.c).

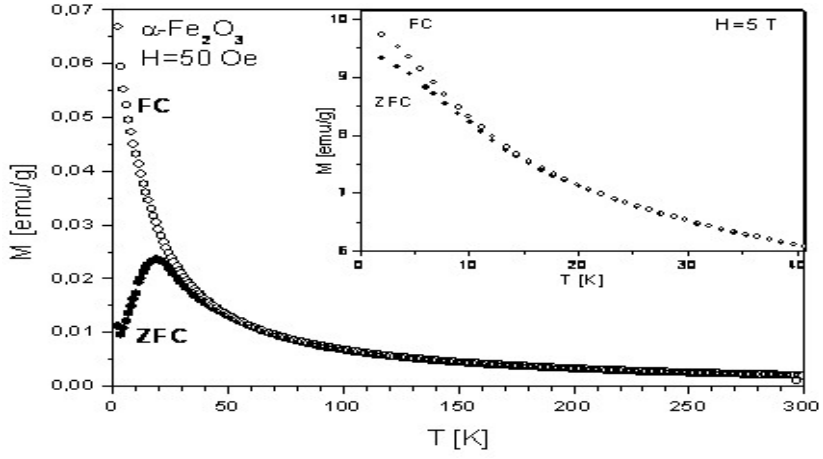


Slika 3 – Fotografije dobijene pomoću TEM-a (a) i HRTEM-a (b) sa elektronskom difrakcijom (c) za nanočestični uzorak α-Fe_2O_3

Figure 3 – Transmission electron micrograph of *α*-Fe_2O_3/SiO_2: (a) silica grain with embedded *α*-Fe_2O_3 nanoparticles; (b) high-resolution image of the selected grain region; (c) the SAED pattern of the same region

Superparamagnetizam kod nanočestičnog hematita

Magnetna merenja urađena su u Laboratoriji za fiziku kondenzovane materije INN „Vinča“. Korišćen je SQUID magnetometar. Magnetne osobine nanočestičnog hematita najpre su ispitivane na osnovu eksperimentalno određenih temperaturnih zavisnosti magnetizacije uzorka. Merena je zavisnost magnetnog dipolnog momenta uzorka α-Fe_2O_3 od temperature T, pri konstantnom magnetnom polju. Merenja su izvršena u magnetnom polju jačine H = 50 Oe, u temperaturnom intervalu 2–300 K. Praćenje temperaturne zavisnosti magnetizacije vršeno je u dva režima rada. U prvom slučaju izvršeno je hlađenje uzorka bez polja, tzv. ZFC (Zero Field Cooled) merenje, tj. uzorak koji se nalazi na temperaturi iznad temperature blokiranja (T_B), $T > T_B$, prvo se ohladi do niske temperature (2 K) $T << T_B$ izvan magnetnog polja, pa se na najnižoj temperaturi T (pošto se temperatura stabilizovala) primeni slabo konstantno DC magnetno polje H=50 Oe i meri se magnetizacija sa povećanjem temperature. U drugom slučaju je tzv. FC (Field Cooling) merenje, tj. uzorak koji se nalazi iznad T_B se hladi do niske temperature u prisustvu istog polja koje je primenjeno pri ZFC merenju. Pošto se temperatura uravnotežila ne menjajući magnetno polje meri se magnetizacija sa povećanjem temperature. Rezultati ovih merenja prikazani su na slici 4.

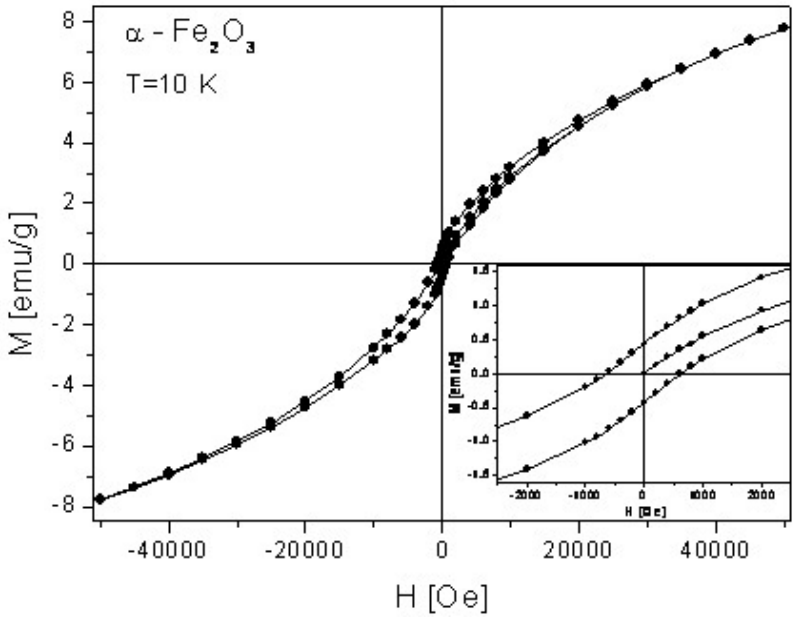


Slika 4 – Zavisnost magnetizacije od temperature za uzorak nanočestičnog hematita (ZFC i FC merenja) u magnetnim poljima jačine 50 Oe i 5 T
Figure 4 – Temperature dependence of the zero-field-cooled (ZFC, solid symbols) and field-cooled (FC, open symbols) magnetization measured in a field of 50 Oe and 5 T (inset)

Za uzorak ohlađen van magnetnog polja (ZFC merenja), magnetizacija prvo raste do temperature jednake temperaturi blokiranja T_B = 19 K, posle koje počinje da opada. Za uzorak ohlađen u magnetnom polju (FC merenja) magnetizacija celim tokom opada sa porastom temperature. To je tipično ponašanje za nanočestične uzorke. Kriva ZFC pokazuje uzak maksimum sa maksimalnom vrednošću koja odgovara temperaturi blokiranja T_B = 19 K. Ispod temperature blokiranja T_B, ZFC magnetizacija oštro opada dok FC magnetizacija raste neprekidno do temperature 2 K, što je karakteristika neinteragujućih ili slabo interagujućih nanočestičnih sistema [1, 5]. Plato (zasićenje) FC magnetizacione krive ispod temperature blokiranja T_B primećen je u nekim nanočestičnim sistemima sa hematitom, ukazujući na postojanje jakih međučestičnih interakcija [2, 3]. Međučestične interakcije, takođe, dovode i do povećanja temperature blokiranja, što je bilo predmet intenzivnog proučavanja [2, 6]. Vrednost koja je dobijena za T_B iz ZFC magnetizacione krive za naš uzorak uporediva je sa vrednostima sličnih sistema u kojima nema interakcija između čestica [1]. Na slici 4.4 (umetak) može se videti da se ZFC i FC krive ne poklapaju čak ni u poljima od 5 T, što pokazuje veliku vrednost energije anizotropije.

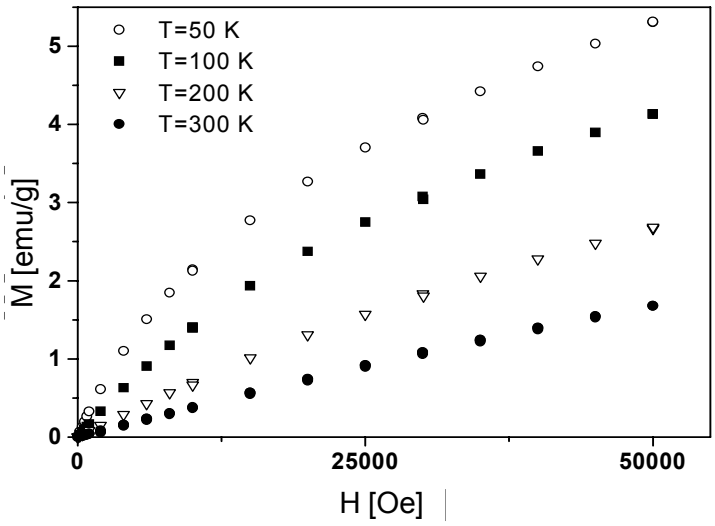
Temperatura na kojoj se počinju odvajati ZFC i FC krive odgovara temperaturi blokiranja najvećih čestica u sistemu. Ona se naziva temperatura ireverzibilnosti T_{irr}, a obično se određuje kao temperatura na kojoj je odnos $(M_{FC}-M_{ZFC})/M_{FC}$ manji od 1% [7]. Pomoću ovog kriterijuma odredili smo vrednost temperature ireverzibilnosti za naš sistem i ona iznosi T_{irr} = 45 K. Razlika između T_{irr} i T_B predstavlja meru širine distribucije nanočestica po veličini [1]. U našem slučaju ova razlika nije velika i pokazuje usku distribuciju po veličini nanočestica (slaže se sa TEM i HRTEM slikama). Iznad temperature ireverzibilnosti ZFC i FC se potpuno poklapaju, i ova činjenica pokazuje da su sve čestice u sistemu u istom stanju (superparamagnetnom).

Zavisnost magnetizacije od polja pri konstantnoj temperaturi ispod temperature blokiranja merena je u poljima u intervalu od –5 T do 5 T i konstantnoj temperaturi 10 K. Rezultati merenja prikazani su na slici 5. Ispod temperature blokiranja pojavljuje se histerezisna kriva, što je karakteristično za superparamagnetne sisteme. Sa slike možemo videti da pri visokim vrednostima magnetnog polja magnetizacija raste linearno ne pokazujući saturaciju. Dobijena histerezisna petlja je simetrična oko inicijalne magnetizacije (slika 5 umetak) sa vrednostima koercitivnog polja i remanentne magnetizacije H_C = 610 Oe i M_r = 0,435 emu/g, respektivno. Ove vrednosti su uporedive sa vrednostima dobijenim u drugim sistemima sa hematitom [1, 3]. Dobijena histerezisna petlja karakteristična je za antiferomagnetne nanočestične materijale.



Slika 5 – Zavisnost magnetizacije od polja pri konstantnoj temperaturi

Figure 5 – Magnetization vs. field dependence recorded at 10 K. The inset shows low field magnetization behavior



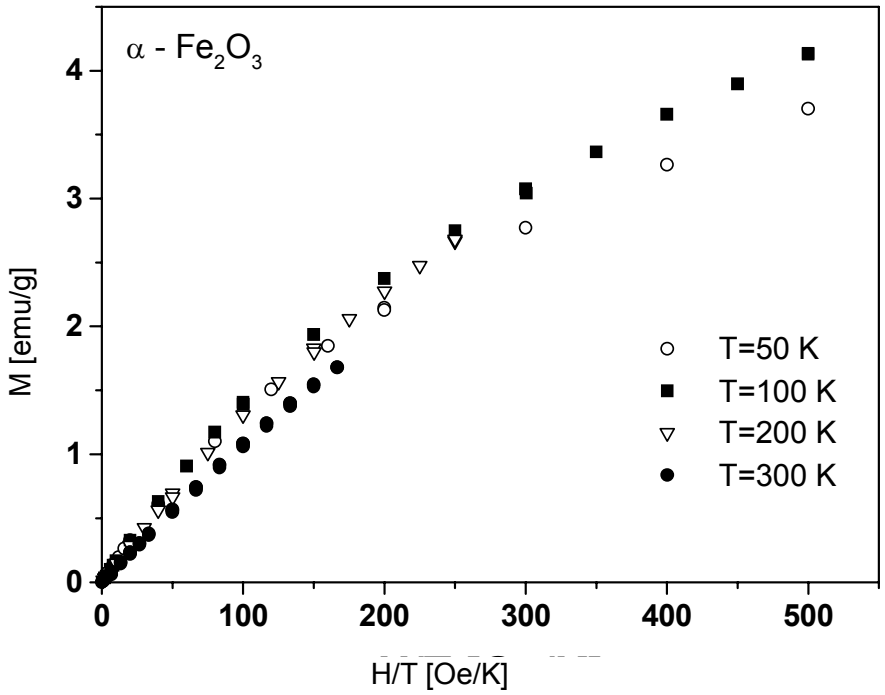
Slika 6 – Zavisnost magnetizacije od magnetnog polja na različitim temperaturama iznad temperature blokiranja

Figure 6 – Magnetization of α-Fe_2O_3 nanoparticles at several temperatures expressed as a function of the applied field *H*

Da bismo proverili da li sistem zaista ima superparamagnetno ponašanje izmerena je zavisnost magnetizacije od polja (0–5 T) na nekoliko temperatura iznad temperature ireverzibilnosti (T_{irr} = 45 K). Sa prikazane slike 6 vidimo da se već na temperaturi od 50 K magnetni histerezis ne pojavljuje. Isti podaci dobijeni za magnetizaciju predstavljeni su na slici 7 u zavisnosti od H/T.

U slučaju superparamagnetnih sistema magnetizacione krive na različitim temperaturama trebalo bi da se poklope ako se magnetizacija predstavi u zavisnosti od H/T [11]. To je zadovoljeno (slika 7), potvrđujući superparamagnetno stanje našeg uzorka na temperaturama iznad 50 K. Superparamagnetizam može se opisati pomoću Langevinove teorije za paramagnetne materijale, gde se zavisnost magnetizacije od temperature i polja može predstaviti jednačinom (1).

$$M = N\mu\frac{x}{3} = \frac{N\mu^2 B}{3k_B T} = \frac{C}{T}B \qquad (1)$$



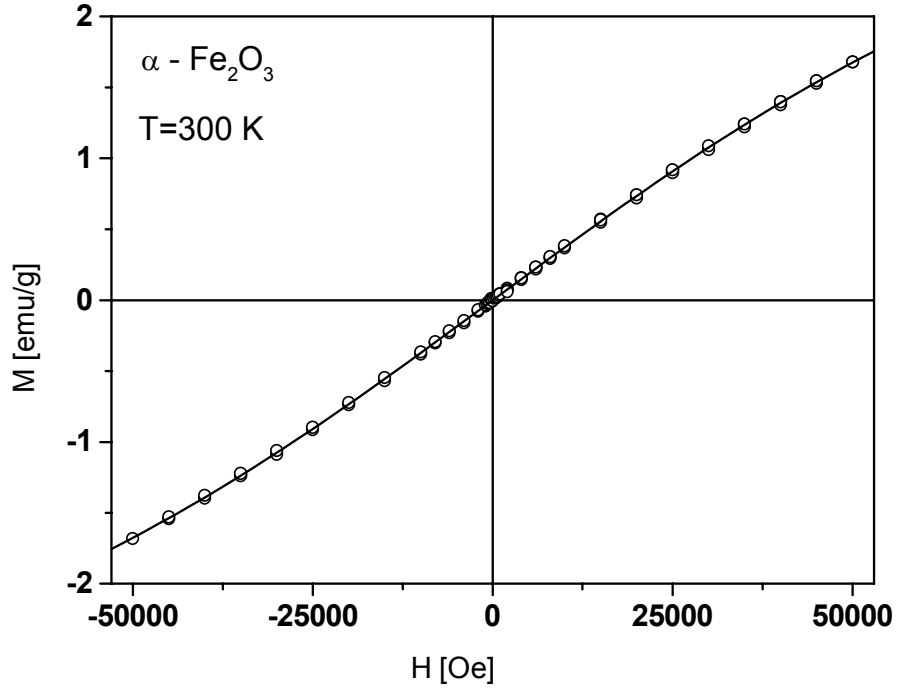
Slika 7 – Zavisnost magnetizacije od H/T

Figure 7 – Magnetization of α-Fe_2O_3 nanoparticles as a function of H/T

Ova jednačina pretpostavlja da je sistem sastavljen od neinteragujućih čestica koje su iste po veličini. Podešavajući podatke na Langevinovu jednačinu, gde je uzeta u obzir saturaciona magnetizacija (M_S) i magnetni moment čestice (m_p) za fitujuće parametre, može se dobiti informacija o veličini i magnetnom momentu superparamagnetnih čestica. Procena srednje veličine čestica može se dobiti pomoću izraza:

$$m_p = \frac{\pi d^3 M_S}{6} \tag{2}$$

gde *d* označava prečnik nanočestice.



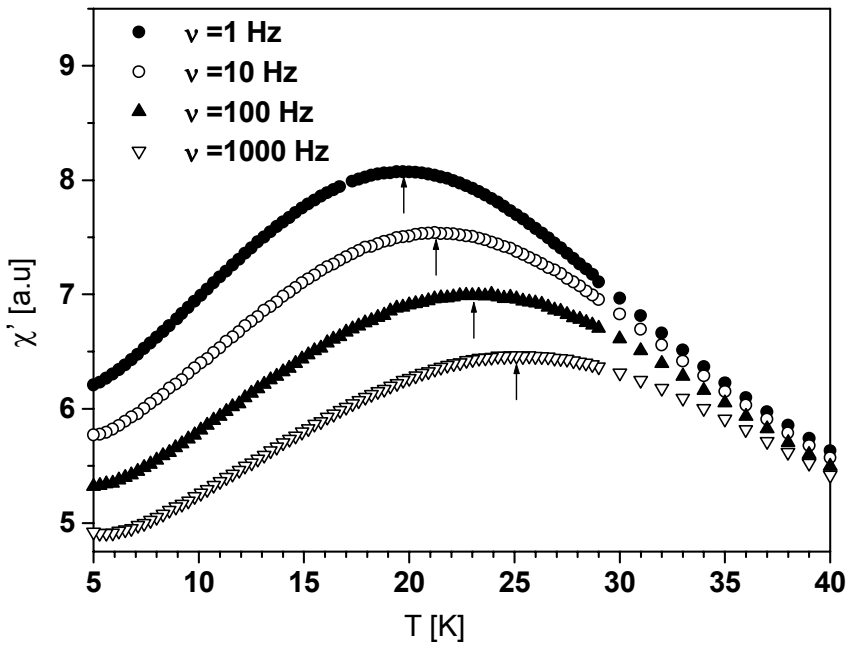
Slika 8 – Zavisnost magnetizacije od magnetnog polja na temperaturi 300 K
Figure 8 – Langevin function fit (full line) to the *M*(*H*) data (dots) measured at 300 K

Podešavanje Langevenove jednačine (1) sa podacima merenim na temperaturi 300 K prikazano je na slici 8. Dobijeni parametri su M_S = 4 emu/g, i m_p = 121 μ_B. Glavni doprinos vrednosti magnetnog momenta čestice potiče od neuređene površinske magnetne strukture gde nema

kompenzovanja spinskih magnetnih momenata. Takođe, za veoma male čestice veličine nekoliko nanometara postojanje nepotpune kompenzacije magnetnih momenata u antiferomagnetnom jezgru nanočestica je očekivano, što takođe daje doprinos vrednosti m_p [2]. Od dobijenih vrednosti za M_S i m_p, pomoću izraza (2), određen je srednji prečnik čestica, i on iznosi d = 4,6 nm. Ova vrednost, dobijena pomoću Langevinove teorije, odlično se slaže sa srednjim prečnikom dobijenim pomoću TEM i HR-TEM merenja, što potvrđuje da se radi o superparamagnetnom sistemu.

Merenja AC susceptibilnosti

Da bismo ispitali prisustvo interakcija između nanočestica urađena su merenja AC susceptibilnosti za četiri različite frekvence magnetnog polja u opsegu od 1 do 1000 Hz. Merenja su vršena u temperaturskom opsegu koji uključuje temperaturu blokiranja (5–40 K).



Slika 9 – Temperaturna zavisnost realnog dela χ' AC susceptibilnosti nanočestičnog hematita za različite frekvencije primenjenog AC magnetnog polja

Figure 9 – Temperature dependence of the real part of the AC susceptibility at different frequencies. The arrows denote the positions of TB

Sa slike 9 može se videti da realni deo susceptibilnosti χ´(T) zavisi od frekvence spoljašnjeg magnetnog polja. Maksimum krive koji odgovara temperaturi blokiranja pomera se ka višim temperaturama sa povećanjem frekvence, dok visina maksimuma opada. Iznad temperature blokiranja χ´ postepeno opada sa povećanjem temperature zato što termalna energija postaje veća od energetske barijere (zadržava magnetni moment u pravcu ose lake magnetizacije). Sa druge strane, ispod temperature blokiranja χ´ opada sa smanjenjem temperature zbog zamrzavanja magnetnih momenata u pravcu osa lake magnetizacije. U skladu sa Néelovom teorijom o superparamagnetizmu [8], magnetni moment neinteragujući monodomenskih čestica sa jednom osom lake magnetizacije fluktuira između dva smera sa relaksacionim vremenom-τ koje se pokorava Arrheniusovom zakonu:

$$\tau = \tau_0 e^{\frac{\Delta E}{k_B T}} \tag{3}$$

gde ΔE predstavlja energetsku barijeru, a τ_0 – vreme za koje magnetni moment pokušava da preskoči barijeru. Pri AC merenjima τ odgovara vremenu merenja i jednako je inverznoj vrednosti frekvence τ = 1/v. U slučaju neinteragujući čestica zavisnost lnv od T_B^{-1} treba da bude linearna. Takođe, u slučaju neinteragujućih čestica τ_0 vrednost se obično nalazi između 10^{-9} i 10^{-12} s [9]. Podešavajući Arreniusov zakon na naše eksperimentalne podatke dobili smo manju vrednost $\tau_0 \approx 10^{-15}$, što ukazuje na postojanje interakcija u našem sistemu (slika 10).

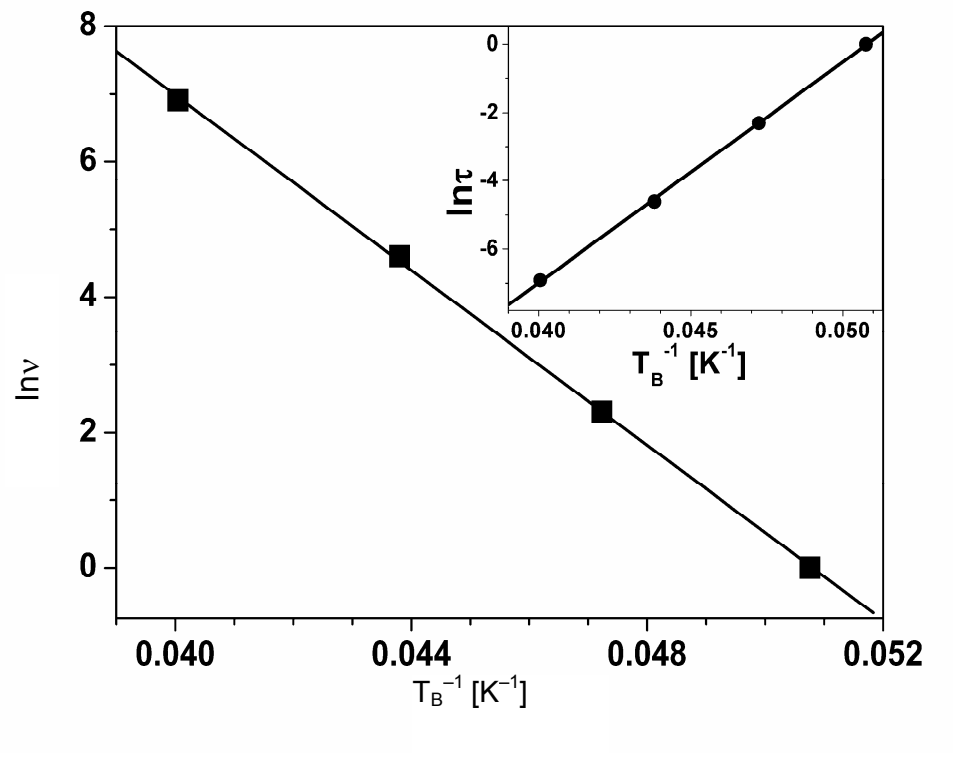
Za dalju potvrdu međučestičnih interakcija može se koristiti empirijski parametar $C_1 = \Delta T_B/(T_B \Delta \log\omega)$, gde T_B predstavlja srednju vrednost temperatura blokiranja za date frekvence, ΔT_B predstavlja razliku između maksimalne i minimalne vrednosti za T_B, dok $\Delta\log\omega$ označava razliku između maksimalnog i minimalnog dekadnog logaritma frekvence.

U slučaju interagujućih čestica zavisnost T_B od frekvence spoljašnjeg magnetnog polja trebalo bi da zadovoljava Vogel-Fulcherov zakon [9]:

$$\tau = \tau_0 \exp\left(\frac{\Delta E}{k_B (T - T_0)}\right) \tag{4}$$

gde T_0 predstavlja vrednost u koju su uključene međučestične interakcije. Podešavajući eksperimentalne podatke na Vogel-Fulcherov zakon (umetak na slici 10) dobili smo sledeće parametre: $\tau_0 = 2{,}5 \cdot 10^{-12}$ s, $\Delta E/k_B = 400$ K

i T_0 = 4 K. Vrednost parametra $\Delta E/k_B$ može se iskoristiti za određivanje vrednosti konstante anizotropije-K, pomoću izraza KV = ΔE, V predstavlja zapreminu čestice. Za sferne čestice prečnika d = 4 nm (dobijeno iz TEM merenja) dobija se vrednost K = $1{,}6 \cdot 10^6$ erg/cm^3. Ova vrednost je za red veličine veća od od vrednosti za hematit visokog kristaliniteta K = $8 \cdot 10^4$ erg/cm^3 [12], što je posledica površinskih efekata. Koristeći vrednost dobijenu za T_0 može se izračunati vrednost parametra $C_2 = (T_B - T_0)/T_B$ i ona iznosi 0,82.



Slika 10 – Punom linijom prikazane su krive dobijene podešavanjem izraza za Arrhenius-ov i Vogel-Fulcherov (umetak) zakon na eksperimentalne vrednosti

Figure 10 – Change of blocking temperatures TB with AC field frequency ν fitted to the Arrhenius function. Inset: fit to the Vogel-Fulcher function

Vrednosti parametra C_1 i C_2 u slučaju neinteragujućih čestica trebalo bi da imaju vrednosti približno 0,1 i 1 [7]. Obe ove vrednosti se smanjuju sa porastom interakcija među česticama [10]. Vrednosti dobijene za naš uzorak su niže, što potvrđuje postojanje međučestičnih interakcija.

U tabeli 1 možemo uporediti vrednosti dobijene za naš uzorak sa vrednostima dobijenim u drugim sistemima sa nanočestičnim hematitom. Sličnost je najveća sa uzorkom nanočestičnog hematita u polimernoj matrici, što potvrđuje da se naš sistem sastoji od slabointeragujućih nanočestica. Uočeno je da na vrednost T_B veliki uticaj imaju veličina čestica i interakcije između čestica (tabela 1). Takođe je primećena zavisnost T_M, m_p, i K od veličine čestica.

Tabela 1

Pregled magnetnih parametara za neke nanočestične sisteme sa nanočesticama hematite

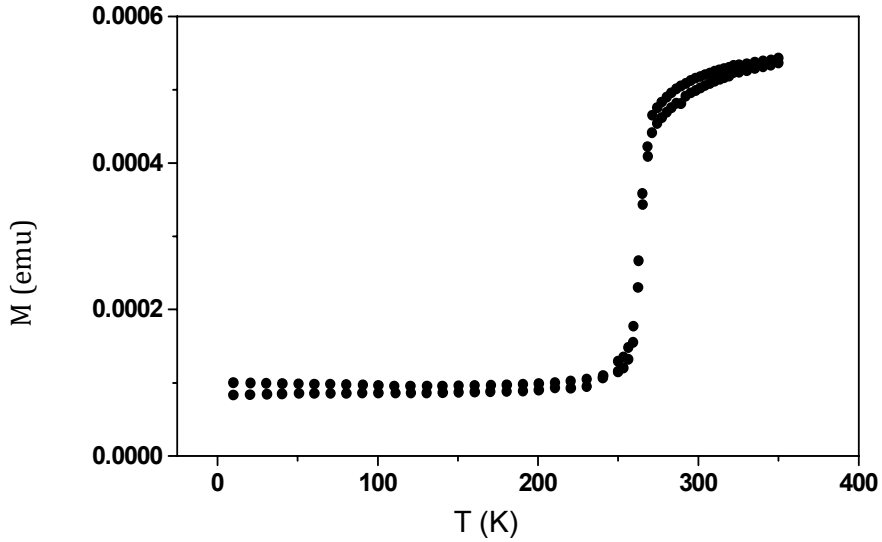
Table 1

Comparative review of magnetic parameters of several distinct nanosized α-Fe_2O_3 systems

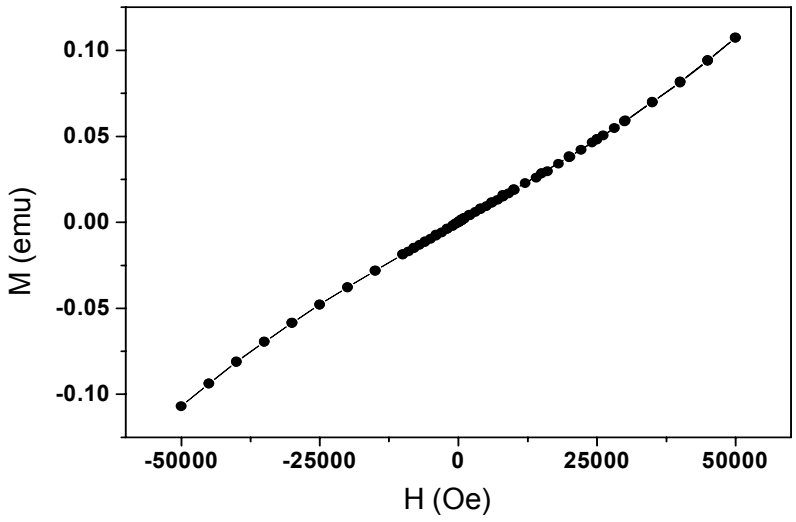
Uzorak	Veličina čestica (nm)	T_B (K)	T_M (K)	$m_p(\mu_B)$	K (erg/cm^3)	Međučestične interakcije	Ref.
α-Fe_2O_3 u polimernoj matrici	d≈5	≈22	Nema	≈80	$8\cdot10^5$	Ne	[1]
α-Fe_2O_3 nanožice	d≈10–20 l≈10–20 μm	≈120	<4	–	–	Da	[3]
α-Fe_2O_3 u alumini	d≈3	≈145	<5	≈40	–	Da	[2]
α-Fe_2O_3 bez odgrevanja – odgrevan	d≈40	≈390 ≈845	177 205	≈13200 ≈11500	$1{,}1\cdot10^5$ $2{,}6\cdot10^5$	Da	[13]
α-Fe_2O_3 u SiO_2 matrici	d≈4	≈19	Nema	≈120	$1{,}6\cdot10^6$	Da	U ovom radu

Magnetne karakteristike hematita visokog kristaliniteta

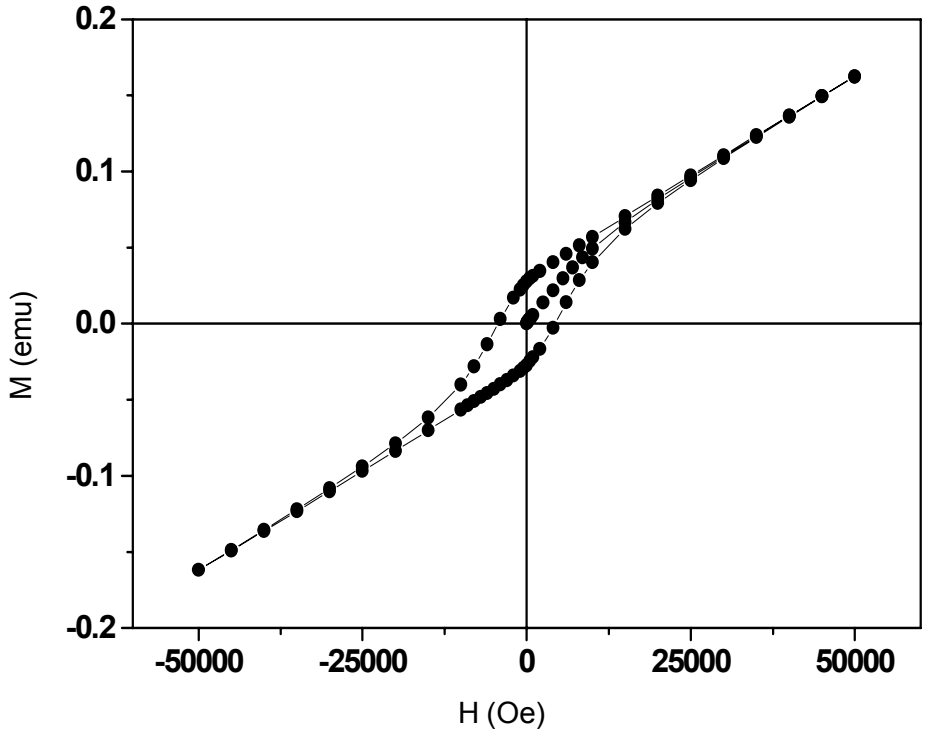
Magnetne karakteristike hematita visokog kristaliniteta (čestice veće od 1 μm) prikazane su pomoću eksperimentalno dobijene temperaturne zavisnosti magnetnog dipolnog momenta u polju od 100 Oe (slika 11) i zavisnosti magnetnog dipolnog momenta od magnetnog polja pri konstantnim temperaturama od 100 K (slika 12) i 300 K (slika 13).



Slika 11 – Zavisnost magnetnog dipolnog momenta od temperature za uzorak hematita visokog kristaliniteta u magnetnom polju jačine 100 Oe (ZFC i FC merenja)
Figure 11 – ZFC and FC magnetization as a function of temperature at 100 Oe magnetic field



Slika 12 – Zavisnost magnetnog dipolnog momenta od magnetnog polja za uzorak hematita visokog kristaliniteta na temperaturi 100 K
Figure 12 – Magnetic dipole moment dependence of the magnetic field at 100K temperature for high cristallinity hematite



Slika 13 – Histerezisna petlja merena na temperaturi od T = 300 K za uzorak hematita visokog kristaliniteta

Figure 13 – Magnetization vs. field dependence recorded at 300K for high cristallinity hematite

Sa slike 11 vidi se tipična zavisnost magnetizacije od temperature za hematit visokog kristaliniteta u magnetnom polju [4]. Na slici se vidi oštar skok na temperaturi 263 K koji odgovara Morinovom prelazu (prelaz iz antiferomagnetnog u slabo feromagnetno stanje). Sa slika 12 i 13 vidi se da iznad Morinove temperature T_M uzorak pokazuje histerezisnu petlju (slab feromagnetizam), dok ispod T_M nema histerezisne petlje (antiferomagnetizam). Na osnovu ovih merenja vidi se da hematit visokog kristaliniteta ima potpuno drugačije magnetno ponašanje od nanočestičnog hematita (poklapaju se ZFC i FC merenja, Morinov prelaz, histerezisna petlja na sobnoj temperaturi i njen izostanak na temperaturama ispod T_M), tako da se smanjenjem veličine kristalita (ispod 100 nm) dobija materijal potpuno drugačijih karakteristika.

Zaključak

Cilj rada bio je istraživanje magnetnih karakteristika nanočestičnog hematita, α-Fe_2O_3, koji ispoljava superparamagnetne karakteristike, tj. superparamagnetizam.

Uzorak nanočestičnog hematita dobijen je sol-gel metodom. Kristalna struktura uzoraka ispitana je pomoću difrakcije elektrona i x-zraka i pokazano je da se radi o monofaznoim uzorku hematita. Na osnovu TEM snimaka utvrđena je veličina čestica, koja za nanočestični hematit iznosi oko 4 nm (uska distribucija čestica po veličini). Ispitivanja magnetnih osobina uzoraka obuhvatila su merenja DC magnetizacije i AC susceptibilnosti u opsegu temperatura od 2 K do 300 K i magnetnih polja od –5 T do 5 T. Merenja su urađena na SQUID magnetometru. Prikazano je nanočestično ponašanje uzoraka, upoređene su karakteristike nanočestičnog materijala sa materijalom visokog kristaliniteta, kao i uticaj veličine nanočestica na magnetne karakteristike.

Kao kod svih superparamagnetnih materijala, nanočestični hematit pokazuje da magnetizacija uzoraka zavisi od magnetne istorije, tj. merenja temperaturne zavisnosti magnetnog dipolnog momenta pri nekom konstantnom magnetnom polju i da daju različite rezultate za uzorak ohlađen bez polja (ZFC merenja) i za uzorak ohlađen u magnetnom polju (FC merenja). Uočeno je pojavljivanje maksimuma u ZFC krivoj, koji odgovara temperaturi blokiranja. Ona iznosi 19 K (uzak maksimum koji odgovara uskoj distribuciji nanočestica po veličini). To se potpuno slaže sa rezultatima dobijenim pomoću TEM merenja (veličine čestica i distribucije po veličinama čestica). Takođe, pokazano je postojanje histerezisne petlje ispod temperature blokiranja-T_B, kao i njeno odsustvo iznad temperature ireverzibilnosti-T_{irr}, što je karakteristika superparamagnetnih materijala. Zavisnost magnetizacije od H/T iznad temperature ireverzibilnosti T_{irr} poklapa se kod svih uzoraka, što je karakteristika superparamagnetnih materijala. Na osnovu ovih rezultata može se zaključiti da uzorak nanočestičnog hematita ima karakteristike nanočestičnog magnetnog materijala (superparamagnetizam). Urađena su i merenja AC susceptibilnosti nanočestičnog hematita, koja su pokazala da položaj maksimuma u $\chi'(T)$, zavisi od frekvencije primenjenog magnetnog polja ω. Primenom Vogel-Fulcherovog zakona dobijene su vrednosti parametara koje odgovaraju slabo interagujućim česticama.

Jasno su uočene razlike između nanočestičnog i hematita visokog kristaliniteta (Morinov prelaz, odsustvo temperature blokiranja, poklapanje ZFC i FC krive, magnetna histerezisna petlja na visokim temperaturama iznad Morinovog prelaza i njen izostanak na nižim temperaturama ispod Morinovog prelaza, itd.), tako da smo pokazali da nanočestični materijal ima potpuno nove magnetne osobina.

Veličinu, oblik, distribuciju i magnetne karakteristike nanočestica ferioksida možemo kontrolisati načinom sinteze. Na osnovu rezultata (TEM, magnetna merenja) jasno se uočava da uzorak nanočestičnog hematita, dobijen sol-gel metodom, ima znatno manje čestice i užu distribuciju po veličini čestica. Aglomeracija kod uzorka dobijenog sol-gel metodom nije primećena.

Literatura

[1] Zysler, R. D., Vasquez Mansilla, M., Fiorani, D., Eur. Phys. J. B 41 (2004) 171.

[2] Zysler, R. D., Fiorani, D., Testa, A. M., J. Magn. Magn. Mater. 224 (2001) 5.

[3] Xu, Y. Y., Rui, X. F., Fu, Y. Y., Zhang, H., Chem. Phys. Lett. 410 (2005) 36.

[4] Morin, F. J., Phys. Rev. 78 (1950) 819.

[5] Fonseka, F. C., Goya, G. F., Yardim, R. F., Muccillo, R., Carreno, N. L. V., Longo, E., Leite, E. R., Phys. Rev. B 66 (2002) 104406.

[6] Dormann, J. L., Bessois, L., Fiorani, D. J., J. Phys. C 21 (1988) 2015.

[7] Mydosh, J. A., *Spin Glasses: An Experimental Introduction*, Taylor and Francis, London (1993).

[8] Neel, L., Ann. Geophys. 5 (1949) 99.

[9] Shtrikman, S., Wolfart, E. P., Phys. Lett. A 85 (1981) 467.

[10] Dormann, J. L., Fiorani, D., Tronc, E., Adv. Chem. Phys. 98 (1997) 283.

[11] Sorensen, C. M., u: Klabunde, K. J. (ed), *Nanoscale Materials in Chemistry*, Wiley-Interscience, New York, (2001).

[12] Morrish, A. H., *Canted Antiferromagnetism: Hematite*, World Scientific, Singapure (1994).

[13] Zysler, R. D., Vasquez, M., Arcriprete, C., Dimitrijewits, M., Rodriguez-Sierra, D., Saragovi, C., J. Magn. Magn. Mater. 224 (2001) 39.

SOL-GEL SYNTHESIS AND MAGNETIC PROPERTIES OF HEMATITE (α-Fe_2O_3) NANOPARTICLES

Summary:

In this work the results of an investigation on hematite (α-Fe_2O_3) nanoparticles magnetic properties, which show superparamagnetic behavior i. e. superparamagnetism, have been presented. Hematite nanoparticles behavior and nanoparticles size influence on magnetic properties have been presented. Hematite nanoparticles properties have been compared with a high cristallinity hematite sample.

Synthesis, diffraction experiments and transmission electron microscopy (TEM)

The α-Fe_2O_3/SiO_2 nanocomposite containing 30 wt.% of α-Fe_2O_3 was prepared using the conventional sol–gel method. An ethanol solution of tetraethoxysilane (TEOS, Aldrich 98%) was mixed with an aqueous so-

lution of iron nitrate ($Fe(NO_3)_3{\cdot}9H_2O$, Aldrich 98%), with HNO_3 as an acid catalyst. The mole ratios of ethanol to TEOS and water to TEOS were 4:1 and 11.67:1, respectively. After 1 h of stirring, the pH of the mixture was about 2. The clear sol was poured into a glass beaker and allowed to gel in the air. The gel was dried for about one week with temperature slowly increasing up to 80°C, and afterwards the sample was heated in air at 400°C for 5 h. A transmission electron micrograph (TEM) and the corresponding selected area electron diffraction (SAED) pattern were shown.

Nanosized hematite superparamagnetism

The zero-field-cooled (ZFC) and the field-cooled (FC) magnetization curves measured in the low DC field of 50 Oe. The ZFC curve exhibits a relatively narrow maximum with the peak value at the temperature T_B =19 K. Below T_B the ZFC magnetization decreases sharply, while the FC magnetization increases continuously below T_B down to 2 K, which is usually considered to be characteristic of noninteracting nanoparticles. The M(H) measurements in the field range 0–5 T at several temperatures above Tirr = 45 K were performed to check the superparamagnetic behavior of the sample.

AC susceptibility measurements

The same instrument was used for AC magnetization measurements carried out in the 1 Hz≤v≤1000 Hz frequency range in a temperature region encompassing the blocking temperatures. The AC susceptibility measurements at four different frequencies in the 1–1000 Hz range, and in the temperature range 5–40 K that encompasses the blocking temperature of the sample were performed in order to investigate the presence of inter-particle interactions.

Magnetic properties of high cristallinity hematite

Magnetic properties of high cristallinity hematite (particles greater than 1 μm) were shown by the experimentally obtained temperature dependence of a magnetic dipole moment in the field of 100 Oe and a magnetic dipole moment of magnetic field at a constant temperature of 100 K and 300 K.

Conclusion

An α-Fe_2O_3/SiO_2 nanocomposite containing 30 wt.% of α-Fe_2O_3 was prepared by the sol–gel method and characterized by using transmission electron micrography and SQUID magnetometry. The obtained hematite nanoparticles, with an average particle size of about 4 nm, were evenly dispersed in an amorphous silica matrix and TEM micrography did not show evidence of significant particle agglomeration. The selected area electron diffraction confirmed the formation of the hematite phase. Both DC magnetization and AC susceptibility experiments

showed behavior characteristic of an assembly of superparamagnetic particles. The particle moments thermally fluctuated freely in the high-temperature superparamagnetic state (above 50 K), and they were blocked below the average blocking temperature of $T_B \approx 19$ K. The temperature and field dependence of magnetization in the superparamagnetic regime satisfactorily fitted Langevin's theory of paramagnetism. The mean particle size determined from this fit was very close to the particle size determined by TEM. The AC susceptibility measurements revealed the existence of weak inter-particle interactions resulting from the high concentration of nanosize magnetic grains in the silica matrix.

Key words: *nanostructured materials, magnetization, magnetic measurements, sol-gel processes, transmission electron microscopy-TEM, superparamagnetism, Morin transition.*

Datum prijema članka: 02. 03. 2010.

Datum dostavljanja ispravki rukopisa: 12. 03. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 13. 03. 2010.

RSA ALGORITAM I NJEGOVA PRAKTIČNA PRIMENA

Kuljanski R. *Sonja,*
EXECOM DOO, Novi Sad

UDC: 004.421

Sažetak:

RSA algoritam jeste algoritam sa javnim ključem koji uključuje tri koraka: generisanje ključa, enkripciju i dekripciju. RSA enkripciona šema je deterministička što znači da se osnovni tekst uvek enkriptuje u isti šifrovani tekst za unapred zadati javni ključ. Da bi se izbegao ovaj problem, praktična implementacija RSA algoritma obično koristi neke strukture, kao što je dodavanje slučajnog teksta u samu poruku pre enkripcije. Ovo dodavanje obezbeđuje da osnovna poruka bude sigurna i da se može enkriptovati u veliki broj različitih šifrovanih poruka. Standardi, kao što je PKCS #1, pažljivo su dizajnirani tako da dodaju tekst u osnovnu poruku pre RSA same enkripcije.

Ključne reči: *kriptografija, enkripcija, dekripcija, RSA, PKCS, OAEP, SAEP*.

Uvod

Kriptografija je poznavanje „tajnog pisanja“, odnosno poznavanje čuvanja informacija tako da one budu čitljive samo onima kojima su namenjene. Reč kriptografija potiče od grčkih reči kriptos (κριπτοσ) – tajna i grafien (γραφιεν) – pisati.

Kriptografija je doživela najznačajniji razvoj 1976. godine kada su Difie (*Whitfield Diffie*) i Helman (*Martin Hellman*) izdali [2]. U ovoj knjizi je uveden revolucionarni koncept kriptografije sa javnim ključem. Takođe, prikazan je i novi, genijalni metod za razmenu ključa, čija je sigurnost bazirana na nerešivosti problema diskretnog logaritma. Mada autori u to vreme nisu imali praktičnu realizaciju šeme enkripcije javnim ključem, ideja je bila jasna i dovela je do velike zainteresovanosti u svetu kriptografije. Rivest (*Ron Rivest*), Šamir (*Adi Shamir*) i Adleman (*Len Adleman*) 1978. godine otkrili su prvu praktičnu šemu za enkripciju sa javnim ključem, sada poznatu kao RSA šema.

Kriptografija se ujedno smatra i granom matematike i granom teorijskog računarstva. Enkriptovanje i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi. Osnovni ele-

sonjakuljanski@gmail.com

ment koji se koristi naziva se enkripcijski sistem ili algoritam enkripcije. Svaki enkripcijski sistem obuhvata par transformacija podataka koje se nazivaju enkripcija i dekripcija. U asimetričnim algoritmima, odnosno algoritmima sa javnim ključem, ključ za enkripciju se razlikuje od ključa za dekripciju. Štaviše, ključ za dekripciju se ne može (u razumnom vremenu) izračunati na osnovu ključa za enkripciju. Ključ za enkripciju naziva se „javni ključ“ i samim tim svako može uputiti šifrovanu poruku primaocu, ali je samo primalac može dešifrovati. Ključ za dekripciju se naziva „tajni ključ“.

Deterministička enkripciona šema je kriptosistem koji uvek produkuje isti šifrovani tekst za dati osnovni tekst i unapred zadati ključ, čak i pored nezavisnog izvršavanja enkripcionog algoritma. Zato deterministička enkripcija može odati informacije napadaču, koji može prepoznati od ranije poznati šifrovani tekst.

Verovatnosna enkripcija koristi slučajnost u algoritmima enkripcije, pa se dobija različita šifrovana poruka kada se više puta enkriptuje ista osnovna poruka. Da bi semantički bio siguran, odnosno da bi sakrio delimične informacije o osnovnoj poruci, enkripcioni algoritam mora biti verovatnosni. Verovatnosna enkripcija ima veoma značajnu ulogu u enkripciji sa javnim ključem. Pretpostavimo da napadač posmatra šifrovani tekst i pretpostavlja da je osnovna poruka DA ili NE. Kada se koristi deterministički enkripcioni algoritam napadač može jednostavno da pokuša da enkriptuje svako od njegovih nagađanja pomoću javnog ključa i da uporedi rezultat sa ranije posmatranim šifrovanim tekstom. Da bi se odbranili od ove vrste napada, enkripcione šeme sa javnim ključem moraju koristiti elemente slučajnosti i tako osigurati da će se jedna osnovna poruka enkriptovati u veliki broj mogućih šifrovanih poruka.

Deterministička enkripciona šema može se konvertovati u verovatnosnu dodavanjem slučajnog stringa u osnovnu poruku pre enkripcije nekim determinističkim algoritmom. U tom slučaju dekripcija zahteva primenu determinističkog algoritma i ignorisanje slučajnog stringa koji je dodat. Ranije šeme koje su primenjivale ovaj pristup bile su razotkrivene na osnovu ograničenja u determinističkim enkripcionim šemama. OAEP integriše slučajan umetak tako da je sigurno korišćenje bilo koje *trapdoor* permutacije.

Osnovni RSA algoritam

Pre dvadeset godina Difie i Helman su izjavili: “We stand today on the bank of revolution in cryptography”. Danas se nalazimo na sredini te revolucije. U poslednje dve decenije došlo je do prave eksplozije istraživanja u oblasti kriptologije. Mnogi kriptosistemi bili su predlagani, a

mnogi od njih bili su razbijeni. Povezanost između kriptologije, teorije kompleksnosti i teorije brojeva postepeno je otkrila i obogatila sve tri grane istraživanja. U radu [3], kao i u radu [6], navedeni su osnovni koncepti kriptografije i kriptografski algoritmi.

Rivest, Šamir i Adleman su 1978. godine objavili kriptosistem sa javnim ključem koji zadovoljava sva tri zahteva koja su postavili Difie i Helman. U toj enkripcijskoj šemi svaki korisnik ima uređeni par celih brojeva (e,n), što predstavlja javni ključ, pri čemu je n proizvod dva velika prosta broja p i i važi $NZD(e,\varphi(n))=1$. Broj $\varphi(n)$ predstavlja red multiplikativne grupe Z^n. Algoritam za enkripciju je:

$$c = m^e \pmod n \tag{1}$$

Odgovarajući tajni ključ je d, pri čemu je $d \cdot e \equiv 1 (\mathrm{mod}\, \varphi(n))$ i algoritam za dekripciju je:

$$m = c^d \pmod n \tag{2}$$

RSA pretpostavka je pretpostavka da je RSA problem težak kada je modul n dovoljno velik i slučajno izabran i kada je osnovna poruka m (a samim tim i šifrovana poruka c) slučajno izabran ceo broj između 0 i $n-1$. Pretpostavka, u stvari, kaže da je RSA funkcija trapdoor jednosmerna funkcija (pri čemu je privatni ključ trapdoor).

Jasno je da RSA problem nije teži od problema faktorisanja celog broja, tako da napadač koji uspe da faktoriše modul n može da izračuna tajni ključ d ako mu je poznat javni ključ (e,n). Još uvek se ne zna da li važi i obrnuto, odnosno da li algoritam za faktorisanje celih brojeva može biti efikasno konstruisan iz algoritma za rešavanje RSA problema. Detaljno objašnjenje problema faktorizacije i RSA problema dato je u [4, poglavlja 3.2 i 3.3].

Algoritam 1 (Generisanje ključeva za RSA enkripciju javnim ključem)

Sažetak: svaki entitet kreira RSA javni ključ i odgovarajući privatni.

1. Generisati dva velika slučajna (i različita) prosta broja p i q, otprilike iste veličine.

2. Izračunati $n = pq$ i $\varphi = (p-1)(q-1)$.

3. Izabrati slučajan ceo broj *e*, $1 < d < \varphi$, takav da $NZD(e,\varphi)=1$.

4. Koristiti prošireni Euklidov algoritam za računanje jedinstvenog celog broja *d*, $1 < d < \varphi$, takvog da $ed \equiv 1 (\mathrm{mod}\, \varphi)$.

5. Javni ključ je (e*, n*), privatni ključ je *d*.

Definicija 1. Celi brojevi *e* i *d* u RSA generatoru ključa nazivaju se enkripcioni eksponent i dekripcioni eksponent, respektivno, dok se *n* naziva modul.

Algoritam 2 (RSA enkripcija javnim ključem)

Sažetak: entitet B enkriptuje poruku m za entitet A, koju će entitet A da dekriptuje.

Enkripcija: entitet B treba da:

1. Dobije od entiteta A autentičan javni ključ (e,n).
2. Predstavi poruku koju želi da enkriptuje kao ceo broj m u intervalu $[0,n-1]$.
3. Izračuna $c = m^e \pmod n$.
4. Pošalje šifrovani tekst c entitetu A.

Dekripcija: za dešifrovanje teksta m iz šifrovanog teksta c entitet A treba da:

1. Koristi tajni ključ d za dešifrovanje $m = c^d \pmod n$.

RSA enkripcija u praksi

Enkripcioni RSA algoritam je deterministički enkripcioni algoritam (nema slučajnih komponenata) i napadač uspešno može izvršiti *chosen plaintext* napad na kriptosistem, enkriptujući mogući osnovni tekst, korišćenjem javnog ključa, i proveravajući da li je jednak šifrovanom tekstu koji želi da dekriptuje. Kriptosistem se naziva „semantički siguran“ ako napadač ne može razlikovati dva enkriptovana teksta, čak i ako mu je poznat odgovarajući osnovni tekst. RSA bez *padding* šeme nije semantički siguran.

Da bi se izbegao ovaj problem praktična RSA implementacija obično ubacuje neki dodatak (*padding*) u osnovnu poruku pre nego što se izvrši enkripcija. Ovaj dodatak omogućava da osnovna poruka ne upadne u opseg nesigurnog osnovnog teksta i da se data poruka enkriptuje u jednu od brojnih, različitih šifrovanih poruka.

Pravilno enkriptovanje RSA algoritmom

Belar (*Mihir Bellare*) i Rodevej (*Phillip Rogaway*) 1993. godine formalizovali su koncept *random orakla*, što predstavlja veoma važan deo teorije kompleksnosti u kriptografiji. Taj novi alat im je omogućio da predstave nekoliko asimetričnih enkripcionih šema koje su efikasne i dokazano sigurne (u random orakl modelu). *The Optimal Asymmetric Encryption Padding* (OAEP) najznačajnija je šema tog modela.

Određeno vreme naučnici su pokušavali da dođu do dokaza o sigurnosti kriptografskih protokola u redukcionom smislu. Da bi to postigli, predstavljali su algoritme koji koriste efektivan napad kao potprogram da bi razotkrili početnu tešku pretpostavku (kao što je RSA pretpostavka ili nemogućnost

faktorizacije celih brojeva). Takvi algoritmi nazivaju se „redukcioni“ i mogu biti uspešni, grubo govoreći, ako ne zahtevaju previše poziva potprograma.

Pre nekoliko godina započeo je novi pravac u istraživanjima koji je kombinovao dokazivanje sigurnosti i efikasnosti. Da bi postigli cilj Belar i Rodževej su formalizovali heuristiku koju su predložili Fiat (*Amos Fiat*) i Šamir. Ona se sastojala u izradi idealne pretpostavke o nekom objektu, kao što je heš funkcija, prema kojoj je moguće simulirati ponašanje zaista slučajne funkcije. Ova pretpostavka, poznata kao „random orakl model“, može izgledati strogo i bez mogućnosti praktične primene.

U random orakl modelu se pretpostavlja da napadač ne može da koristi bilo koji specifičan nedostatak heš funkcije koja se koristi u praksi.

Potrebno je naglasiti da čak i formalna analiza u random orakl modelu nije jak dokaz sigurnosti, jer je zasnovana na idealnoj pretpostavci. Medutim, ovaj model može obezbediti dovoljno sigurnosti i može se koristiti kao osnova za veoma efikasne šeme, videti [5, poglavlje 3.1].

Random orakl, RSA-PKCS[1] i OAEP šema

Random orakl u kriptografiji je orakl (crna kutija) koji na svaki upit odgovara slučajnim odgovorom, izabranim uniformno iz izlaznog domena. Sa druge strane, random orakl je matematička funkcija koja slika svaki mogući upit na slučajan odgovor iz izlaznog domena.

Random orakl predstavlja matematičku apstrakciju koja se koristi u kriptografskim dokazima, a koristi se kada nije poznata matematička funkcija koja dovodi do osobina traženih u dokazu. Sistem za koji je dokazano da je siguran, korišćenjem ovog načina dokazivanja, smatra se sigurnim u random orakl modelu, za razliku od sigurnosti u standardnom modelu 1. U praksi se random orakl obično koristi za modeliranje kriptografske heš funkcije u šemama u kojima je potrebna pretpostavka o strogoj slučajnosti. Ovakvi dokazi obično pokazuju da je sistem siguran, ukazujući na činjenicu da napadač mora da zahteva nemoguće ponašanje orakla ili da reši neki matematički problem za koji se veruje da je težak u cilju razotkrivanja sistema.

Ne postoji realna funkcija koja predstavlja random orakl. U suštini, određene enkripcione šeme su dokazano sigurne u random orakl modelu, ali su trivijalno nesigurne kada bilo koja realna funkcija zameni random orakl. Bez obzira na to, dokaz o sigurnosti u random orakl modelu obično daje veoma jak dokaz da napad koji ne razbije druge pretpostavke dokaza (kao što je faktorizacija celih brojeva) mora otkriti neke nepoznate osobine heš funkcije koja se koristi. Među šemama koje su dokazano sigurne u random orakl modelu jedna od najznačajnijih je OAEP šema.

[1] Public-Key Cryptography Standards.

Posle Blaihenbaherovog (*Daniel Bleichenbacher)* razarajućeg napada na RSA-PKCS #1 v1.5 1998. godine, RSA-OAEP (RSA-PKCS #1 v2.0) postao je naslednik standarda 2, a samim tim i internacionalni standard. Interesantno je da je ˇ Soup (*Victor Shoup*) nedavno pokazao da originalni dokaz sigurnosti OAEP-a nije korektan. Srećom, ubrzo posle toga otkrio je formalan i kompletan dokaz koji garantuje visok nivo sigurnosti RSA-OAEP šeme. Međutim, ovaj novi dokaz sigurnosti još uvek ne garantuje sigurnost za veličinu ključa koji se koristi u praksi. Alternative OAEP šeme, kao što su OAEP$^+$ i SAEP$^+$ omogućavaju efikasnije dokazivanje i zbog toga obezbeđuju adekvatan nivo sigurnosti za veličinu ključa koja se koristi u praksi. Sve tri šeme su navedene u [5, poglavlje 3].

RSA-PKCS #1 v1.5 enkripcija

Široko rasprostranjen *padding* za RSA enkripciju definisan je u PKCS #1 v1.5 standardu: za bilo koji modul $2^{8(k-1)} \le n \le 2^{8k}$, kako bi se enkriptovala l bitova dugačka poruka m $(l \le k-11)$ potrebno je slučajno izabrati string r dužine $k-3-l$ bitova. Tada se definiše k bitova duga poruka $M = 02 \,||\, * \,||\, 0 \,||\, *$. Ako je šifrovana poruka ovog formata, dekriptor dešifruje osnovni tekst, a ako nije onda se šifrovani tekst odbacuje.

Tabela 1
Table 1

0	2	ne nula bitovi (više od 8 bitova)	0	m

Intuitivno, ovaj *padding* izgleda dovoljan da otkloni nedostatke obične RSA enkripcije, ali ne postoji formalan dokaz koji to i garantuje. Blaihenbaher je neočekivano pokazao da jednostavan aktivan napad može kompletno slomiti PKCS #1. Taj napad je primenjen na realan sistem kao što je Web server koji koristi SSL v3.03. Ovi serveri često produkuju specifičnu poruku o grešci ako šifrovani tekst nije korektan. Ta osobina servera omogućava napadaču da testira da li su dva najznačajnija bajta šifrovanog teksta c baš 02. Ako jesu, napadač saznaje sledeće ograničenje za dekriptovanje šifrovanog teksta c:

$$2 \cdot 2^{8(k-2)} \le c^d \bmod n < 3 \cdot 2^{8(k-2)} \tag{3}$$

Zahvaljujući samoreducibilnosti RSA permutacije, naročito homomorfizmu $cs^e = m^e s^e = (ms)^e \bmod n$, kompletna dekripcija šifrovanog teksta c može biti razotkrivena posle relativno malog broja upita. Samo nekoliko miliona upita potrebno je za 1024-bitni modul.

Blaihenbaherov napad imao je uticaj na mnoge praktične sisteme i odjednom je postalo jasno koliko je veliki značaj formalnog dokaza sigurnosti, videti [5, poglavlje 2.2].

OAEP šema

U vreme kada je Blaihenbaher objavio svoj napad na RSA-PKCS #1 v1.5 jedina efikasna i „dokazano sigurna“ enkripciona šema, zasnovana na RSA problemu, bila je OAEP šema, koju su predložili Belar i Rodževej. OAEP se može koristiti sa bilo kojom *trapdoor* permutacijom f.

Belar i Rodževej su dokazali da OAEP *padding* korišćen bilo kojom *trapdoor* – jednosmernom permutacijom f semantički obezbeđuje sigurnost enkripcionoj šemi. Dopunjavanjem osnovne poruke oni su, pored sigurnosti, dokazali i da je OAEP *padding* slabo svestan osnovne poruke. Kriptosistem je slabo svestan osnovne poruke ako bilo koji algoritam teško može da dode do šifrovanog teksta kad mu nije poznat odgovarajući osnovni tekst. Nažalost, *adaptive chosen-ciphertext* napad dozvoljava napadaču da proizvoljno dugo pristupa dekripcionom oraklu, čak i posle primanja spornog šifrovanog teksta o kojem napadač želi da dobije neke informacije. Zbog toga, semantička sigurnost, zajedno sa slabom svešću o osnovnom tekstu, samo implicira semantičku sigurnost na *non-adaptive chosen-ciphertext* napad (*lunchtime* napad ili indiferentan*chosen-ciphertext* napad), gde je pristup dekripcionom oraklu ograničen, dok napadač ne primi testirani šifrovani tekst.

Činjenica je da je jedini formalan dokaz sigurnosti OAEP šeme dokaz da je ona semantički sigurna na *lunchtime attacks,* pod pretpostavkom da je osnovna permutacija jednosmerna. Međutim, veruje se da je OAEP takođe semantički sigurna šema na *chosen-ciphertext* napad.

OAEP šema je vrsta Feistelove mreže koja koristi par random orakla G i H da bi obradila osnovni tekst asimetričnom enkripcijom. Kada se kombinuje sa bilo kojom jednosmernom *trapdoor* permutacijom f ova obrada će dokazano, u smislu random orakl modela, rezultirati kombinovanom šemom koja je semantički sigurna na *chosen plaintext* napad (IND-CPA). Kada je implementirana sa pouzdanom *trapdooor* permutacijom (na primer RSA), OAEP će biti dokazano siguran i na *chosen ciphertext* napad (IND-CCA).

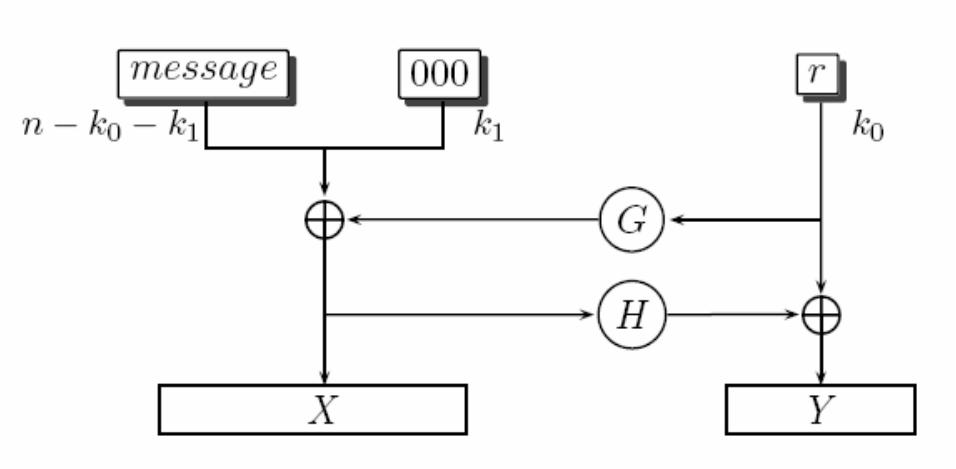
OAEP šema zadovoljava sledeća dva uslova:

– dodaje elemente slučajnosti koji mogu biti korišćeni za konvertovanje determinističke enkripcione šeme (kakva je RSA šema) u verovatnosnu šemu,

– štiti delimičnu dekripciju šifrovanog teksta, onemogućavajući napadača da otkrije bilo koji deo osnovnog teksta ako nije u mogućnosti da invertuje *trapdoor* jednosmernu permutaciju f.

Dijagram OAEP šeme

Na prikazanom dijagramu:
- n predstavlja broj bitova RSA modula;
- k_0 i k_1 su celi brojevi određeni protokolom;
- $message$ je osnovna poruka, čija je dužina $n - k_0 - k_1$ bitova;
- G i H su heš funkcije utvrđene protokolom.



Slika 1 – OAEP šema[2]
Figure 1 – OAEP diagram

Enkripcija se vrši na sledeći način:

1. osnovna poruka se proširi sa k_1 nula i na taj način se dobija poruka dužine $n - k_0$ bitova;
2. r je proizvoljan string dužine k_0 bitova;
3. G je heš funkcija koja konvertuje k_0 bitova stringa r u $n - k_0$ bitova;
4. $X = message0^{k_1} \oplus G(r)$;
5. H je heš funkcija koja konvertuje $n - k_0$ bitova od X u k_0 bitova;
6. $Y = r \oplus H(X)$;
7. Izlaz je $X \,||\, Y$.

Dekripcija se vrši na sledeći način:

1. izračunava se proizvoljan string $r = Y \oplus H(X)$;
2. izračunava se osnovna poruka $message0^{k_1} = X \oplus G(r)$.

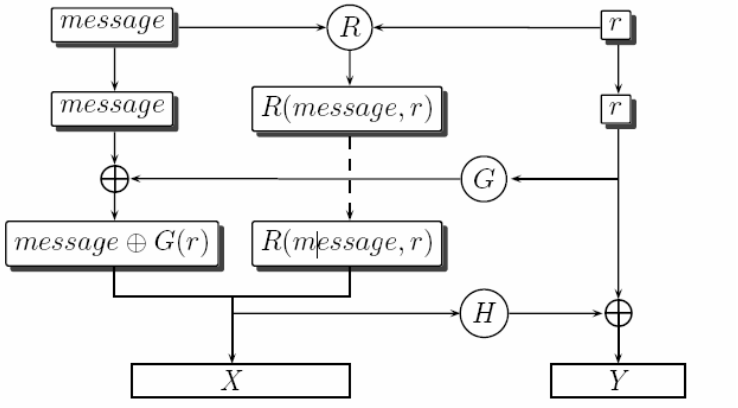
[2] Slika preuzeta iz [5].

Sigurnosna redukcija RSA inversa u napad je neefikasna u praktičnoj primeni. Samim tim, redukcija je besmislena ako se neće koristiti dovoljno veliki modul, pri čemu bi RSA invers (ili faktorizacija) zahtevao mnogo više od 2^{150} poziva. Koristeći postojeće tehnike faktorizacije potrebno je koristiti modul veći od 4096 bitova kako bi redukcija imala smisla. Sa druge strane, redukcija pokazuje da 1024-bitni modul obezbeđuje dokazani nivo sigurnosti od 2^{40}, što je neadekvatna zaštita, imajući u vidu trenutnu kompjutersku moć.

Alternative OAEP šeme

OAEP⁺ Padding

Šoup je predložio formalan dokaz sigurnosti RSA-OAEP šeme sa mnogo uspešnijom sigurnosnom redukcijom, ali u praktičnoj primeni to znači da bi enkripcioni eksponent trebao da bude 3. Međutim, mnogi naučnici veruju da je RSA *trapdoor* permutacija sa eksponentom $e = 3$ slabija od permutacije sa većim eksponentom. Zato je predložio modifikovanu verziju OAEP šeme, koja se naziva OAEP⁺. Ova šema koristi redundantnost promenljivih $R(message, r)$ umesto konstantnog broja 0 (k^{k_1}), pa je samim tim OAEP⁺ šema malo kompleksnija od OAEP šeme, [5, poglavlje 4.1]. Fujisaki je u [4] pokazao da isto važi za RSA permutaciju sa bilo kojim javnim eksponentom e.

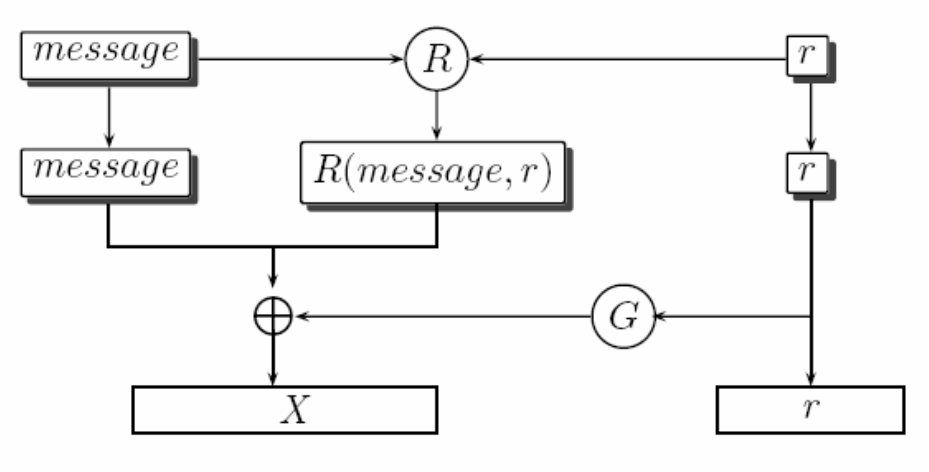


Slika 2 – OAEP⁺ šema[3]
Figure 2 – OAEP⁺ diagram

[3] Slika preuzeta iz [5].

SAEP⁺ Padding

Bonei je nedavno objavio novu *padding* šemu, SAEP⁺. Ona je jednostavnija od OAEP šeme, pa je nazvana *Simplified Asymmetric Encryption Padding*. Dok je OAEP šema dvostruka Feistelova mreža, SAEP⁺ je jednostruka. Međutim, za velike eksponente $(e > 2)$, SAEP⁺ ne garantuje sigurnost u praktičnoj primeni [5, poglavlje 4.2].



Slika 3 – SAEP⁺ šema[4]
Figure 3 – SAEP⁺ diagram

Zaključak

Među algoritmima sa javnim ključem postoji ogroman jaz između praktičnih šema i šema za koje je dokazano da su sigurne: praktični metodi su efikasni, ali nemaju dovoljan nivo dokazane sigurnosti, dok su dokazano sigurne šeme sigurne, ali ni blizu toliko efikasne. U ovom radu prikazane su šeme koje su dokazano sigurne, ali i zadovoljavajuće efikasne.

Pri dokazivanju sigurnosti OAEP šeme zahteva se da G i H budu random funkcije, međutim, prilikom konkretne implementacije koriste se kriptografske heš funkcije. Paradigma [1] tvrdi da rezultati koji se zasnivaju na idealnoj heš funkciju i koji dokazuju sigurnost imaju veći značaj od protokola koji su dizajnirani *ad. hoc*.

Pri dokazivanju da je OAEP sistem siguran garantuje se da napadač, koji poseduje šifrovani tekst, mora otkriti $message0^{k_1} \oplus G(r)$ ako želi da otkrije bilo šta smisleno o osnovnoj poruci $message$. Pokazano je da postoji

[4] Slika preuzeta iz [5].

jednostavnija *padding* šema za konvertovanje RSA enkripcione šeme u verovatnosnu, koja je, takođe, sigurna u random orakl modelu. To je takozvana SAEP$^+$. Primećeno je da jednostavnija *padding* šema čini sistem lakšim za opisivanje i lakšim za implementaciju, a samim tim mnogo elegantnijim. Pojednostavljenje *padding* šeme ima malo uticaja na performanse, jer je vreme za njeno izvršavanje zanemarljivo u odnosu na samu enkripciju.

Mada je SAEP$^+$ *padding* šema jednostavnija od OAEP šeme, ona je i restriktivnija. Korišćenjem OAEP i OAEP$^+$ šeme može se enkriptovati poruka koja je dugačka skoro kao I modul. Na primer, za 1024-ro bitni modul bezbedno je enkriptovati poruku koja je dugačka 768 bitova. Nasuprot tome, korišćenjem modula iste veličine, SAEP$^+$ šema može enkriptovati poruku od najviše 384 bita. Ova razlika je nije toliko bitna u svakodnevnoj upotrebi (za transport ključa), ali je ipak vredna pomena.

Literatura

[1] Bellare, M. and Rogaway, P., *Random oracles are practical: a paradigm for designing efficient protocols*," Proceedings of the First Annual Conference on Computer and Communications Security, ACM, 1993.

[2] Diffie, W. and Hellman, M., *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22, no. 6, November 1976, pages 644–654.

[3] Menezes, A., Oorschot, P. and Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, October 1996.

[4] Menezes, A., *Evaluation of Security Level of Cryptography: RSA-OAEP, RSAPSS, RSA Signature*, CRYPTREC, December 2001.

[5] Pointcheval, P., *How to Encrypt Properly with RSA*, RSA Laboratories' CryptoBytes. Volume 5, No. 1 – Winter/Spring 2002, pages 9–19.

[6] Rivest, R., *Cryptology*, MIT Laboratory for Computer Science, 1990.

RSA ALGORITHM

Summary:

Introduction

RSA is an algorithm for public-key encryption. It is the first algorithm known to be suitable for encryption as well as digital signing.

The RSA encryption scheme is deterministic in the sense that under a fixed public key, a particular plaintext is always encrypted to the same ciphertext. A deterministic encryption scheme (as opposed to a probabilistic encryption scheme) is a cryptosystem which always produces the same ciphertext for a given plaintext and key, even over separate executions of the encryption algorithm. Probabilistic encryption uses randomness in an encryption algorithm, so that when encrypting the same message several times it will, in general, yield different ciphertexts.

Basic RSA algorithm

The RSA algorithm involves three steps: key generation, encryption and decryption.

The key generation algorithm:
1. Generate two large random primes, p and q.
2. Compute n = pq and φ = (p-1)(q-1).
3. Choose an integer e, 1 < e < φ, such that gcd(e, phi) = 1.
4. Compute the secret exponent d, 1 < d < φ, such that ed ≡ 1 (mod φ).
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and φ secret.

• n is known as the modulus.
• e is known as the public exponent or encryption exponent or just the exponent.
• d is known as the secret exponent or decryption exponent.

Encryption:

Sender A does the following:
1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m
3. Computes the ciphertext $c = m^e \bmod n$.
4. Sends the ciphertext c to B.

Decryption:

Recipient B does the following:
1. Uses his private key (n, d) to compute $m = c^d \bmod n$.

RSA encryption in practice

To solve a deterministic problem, practical RSA implementations typically embed some form of structured, randomized padding into the plaintext before encrypting it. This padding ensures that the plaintext does not fall into the range of insecure plaintexts, and that a given message, once padded, will encrypt to one of a large number of different possible ciphertexts. Standards, such as PKCS #1, have been carefully designed to securely pad messages prior to RSA encryption.

How regularly encrypt RSA algorithm

A few years ago, a new line of research started with the goal of combining provable security with efficiency. To achieve this goal, Bellare and Rogaway formalized a heuristic suggested by Fiat and Shamir. This heuristic consisted in making an idealized assumption about some objects, such as hash functions, according to which they were assumed to behave like truly random functions. This assumption, known as the „random oracle model", may seem strong, and lacking in practical embodiments.

Random oracle, RSA-PKCS and OAEP scheme

No real function can implement a true random oracle. In fact, certain encryption schemes are proven secure in the random oracle model, but are trivially insecure when any real function is substituted for the random oracle. Nonetheless, a proof of security in the random oracle model gives very strong evidence that an attack which does not break the other assumptions of the proof, if any (such as the hardness of integer factorization) must discover some unknown and undesirable property of the hash function used in the protocol to work. Many schemes have been proven secure in the random oracle model, for example the OAEP scheme.

Shoup also proposed a formal security proof of RSA-OAEP with a much more efficient security reduction, but in the particular case where the encryption exponent e is equal to 3. However, many people believe that the RSA trapdoor permutation with exponent 3 may be weaker than with greater exponents. Therefore, he also proposed a slightly modified version of OAEP, called OAEP+.

Boneh recently proposed a new padding scheme, SAEP+, to be used with RSA. It is simpler than OAEP, hence the name Simplified Asymmetric Encryption Padding: whereas OAEP is a two-round Feistel network, SAEP+ is a single round.

Key words: *cryptography, encryption, decryption, RSA, PKCS, OAEP, SAEP*

Datum prijema članka: 16. 01. 2010.

Datum dostavljanja ispravki rukopisa: 01. 02. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 02. 02. 2010.

STRUČNI ČLANCI

JEDAN PRISTUP U OCENI EFEKTIVNOSTI SISTEMA ZA ZVUKOMETRIJSKO IZVIĐANJE „BOOMERANG“

Terzić R. *Miroslav*, Vojna akademija, Katedra vojnih elektronskih sistema, Beograd

UDC: 355.535.2:534.88
355.535.2:681.88

Sažetak:

U radu je prikazan jedan pristup u oceni efektivnosti sistema za zvukometrijsko izviđanje. Sistem za zvukometrijsko izviđanje modelovan je kao sistem masovnog opsluživanja, opisana su stanja sistema, parametri i izveden izraz za određivanje verovatnoće opsluživanja sistema za zvukometrijskao izviđanje, kao kriterijuma za ocenu efektivnosti.

Ključne reči: *zvukometrijsko izviđanje, teorija masovnog opsluživanja, efektivnost, verovatnoća opsluživanja.*

Uvod

Pravovremen, pouzdan i siguran prijem, obrada i dostavljanje podataka, primenom novih informacionih tehnologija i sistema uslov su uspešnog rukovođenja i komandovanja i efikasne upotrebe resursa u borbenim dejstvima. Podaci o lokaciji protivničkih snaga mogu se dobiti izviđanjem komunikacionih i izviđanjem nekomunikacionih signala. Izviđanje komunikacionih signala realizuje se upotrebom stanica i centara za radio-izviđanje. Izviđanje nekomunikacionih signala realizuje se upotrebom stanica za radio-tehničko izviđanje, stanica za radarsko izviđanje, stanica za televizijsko izviđanje, stanica za zvukometrijsko izviđanje... Sistem za zvukometrijsko izviđanje čini „**n**“ jednokanalnih identičnih stanica koje se postavljaju za potrebe odgovarajuće komande – jedinice. U radu se sistem za zvukometri-

terzicmiroslav@yahoo.com

jsko izviđanje razmatra kao tehnički sistem čija je osnovna funkcija identifikacija, prijem, obrada akustičkog signala i dostavljanje informacija o smeru i lokaciji izvora akustičkog signala. Efektivnost tehničkih sistema je kompleksni pokazatelj funkcionisanja sistema, te, zavisno od njegove osnovne namene i funkcije cilja, obuhvata različite karakteristike sistema. Odgovarajući modeli ocene funkcije efektivnosti tehničkih sistema obuhvataju relevantne parametre funkcionisanja sistema i ispunjavanja funkcije cilja.

Jedan od često korišćenih modela, koji je definisan u okviru koncepta efektivnosti vojske (Army System Effectiveness Concept) [1], a prema kojem se kvantitativna ocena funkcije efektivnosti tehničkog sistema **E(t)** vrši na osnovu svojstava pouzdanosti **P(t)**, raspoloživosti **A(t)** i funkcionalne podobnosti **Fp(t)**, može se predstaviti izrazom [2]:

$$E(t) = P(t) \cdot A(t) \cdot F_p(t) \qquad (1)$$

gde je:
E(t) – efektivnost sistema, predstavlja verovatnoću da će sistem stupiti u dejstvo, izvršiti postavljene zadatke na osnovu projektovanih mogućnosti u zadatom periodu i datim uslovima rada,
P(t) – pouzdanost sistema je verovatnoća da sistem bude u operativnom, radnom stanju, u toku vremena **t**, odnosno verovatnoća da u određenom periodu sistem ispravno funkcioniše i obavlja svoje zadatke,
A(t) – raspoloživost sistema je pokazatelj koji predstavlja vreme u kojem se može očekivati da sistem bude u operativnom stanju, tj. procenat vremena kada je sistem upotrebljiv u odnosu na ukupno vreme rada sistema. Raspoloživost se iskazuje koeficijentom spremnosti Ks,
Fp(t) – funkcionalna podobnost, koja predstavlja prikladnost sistema za vršenje funkcije. To je svojstvo sistema koje ukazuje na to kojom će verovatnoćom sistem izvršiti postavljeni zadatak.

Treba napomenuti da se kod različitih tehničkih sistema, zavisno od osnovne funkcije cilja i glavnih posledica otkaza, ocena funkcije efektivnosti može definisati i preko pojedinačnih pokazatelja. Pored toga, važan je probabilistički aspekt prisutan u prikazanom konceptu i stohastička priroda relevantnih parametara, koji efektivnost određuju kao veličinu kategorije verovatnoće. Matematički izrazi za funkcije efektivnosti sistema, dati u obliku proizvoda različitih verovatnoća, mogu se formalno prihvatiti ukoliko parametri koji figurišu u navedenim izrazima predstavljaju međusobno nezavisne slučajne veličine. Uz pretpostavku da je sistem potpuno pouzdan i funkcionalno podoban, efektivnost će se razmatrati u funkciji raspoloživosti sistema.

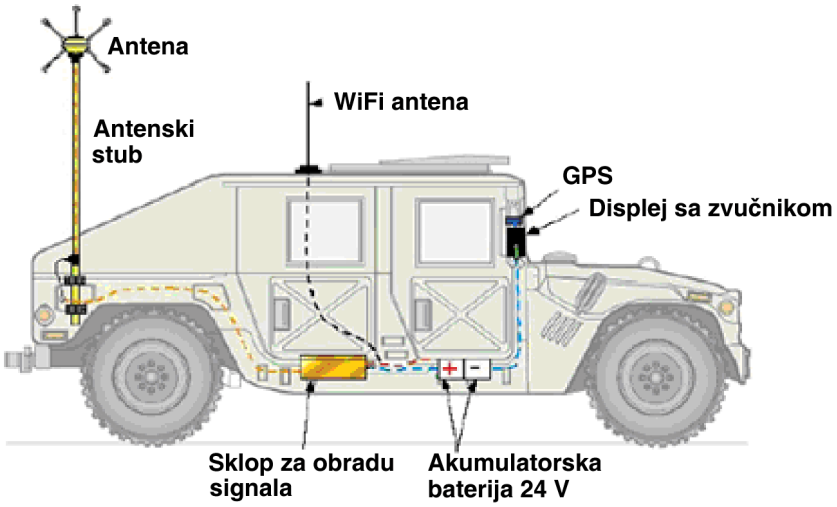
Ocenom efektivnosti sistema za zvukometrijsko izviđanje kvantitativno se može oceniti njegovo funkcionisanje i izvršenje namenskog zadatka (određivanje i prenos informacija o lokaciji akustičkog signala). Radi određivanja efektivnosti potrebno je sistem za zvukometrijsko izviđanje predstaviti odgovarajućim modelom i kvantitativno odrediti njegova svojstva u odnosu

na mogućnosti zadovoljenja njegovih funkcija u složenim uslovima. Sistem za zvukometrijsko izviđanje je modelovan kao sistem za masovno opsluživanje sa otkazom, imajući u vidu da je funkcionisanje sistema limitirano propusnom sposobnošću sistema i potrebom da svaki detektovani akustički signal bude pravovremeno obrađen i prenet.[1] Kako akustički signali u stanice pristižu pojedinačno, nezavisno jedan od drugog i u slučajnim vremenskim intervalima, nadalje će se razmatrati samo Poasonov sistem masovnog opsluživanja sa otkazom, sa prostim tokom događaja. Verovatnoća opsluživanja sistema predstavlja kriterijum za ocenu njegove efektivnosti.

Osnovne karakteristike sistema za zvukometrijsko izviđanje „Boomerang“

Sistem „Boomerang“ jeste integrisani hardverski i softverski sistem namenjen za detekciju projektila ispaljenih iz ručnog naoružanja i za utvrđivanje azimuta i lokacije sa koje je ispaljen projektil. Detektuje zvuk projektila, vrši akustičku analizu i pokazuje pravac (vizuelno i zvučno) iz kojeg je projektil ispaljen.

Sistem je instaliran na vozilo HMMWV (hamvi) sa mogućnošću rada iz mesta i iz pokreta (slika 1).



Slika 1 – Elementi sistema „Boomerang“ instalirani na vozilo *hamvi*

[1] Sistemi masovnog opsluživanja su bilo koji sistemi predodređeni za opsluživanje nekog toka zahteva i mogu biti sistemi sa otkazom i sistemi sa čekanjem. U sistemima sa otkazom potraživanje koje je došlo u momentu kad su svi kanali opsluživanja zauzeti dobija otkaz i napušta sistem. U sistemima sa čekanjem takvo potraživanje ne prekida rad sistema, već se svrstava u red i čeka dok se ne oslobodi neki kanal [3].

Osnovne karakteristike:

– radi u pokretu kada se vozilo kreće brzinama do 96 km/h, na otvorenom prostoru i u urbanim sredinama,

– osnovno oružje koje detektuje je automatska puška AK-47,

– otkriva neprijateljskog strelca nakon ispaljivanja prvog hica u svim vremenskim uslovima (danju, noću, pri kišovitom, maglovitom i snežnom vremenu i pri peščanoj oluji),

– sistem dostavlja informacije o azimutu i lokaciji, vizuelno i zvučno,

– prikazivanje desetocifrenih koordinata u vojnom geografsko-inforamcionom sistemu,

– jednostavno rukovanje, bez potrebe za kalibracijom, korišćenjem prekidača za uključivanje i isključivanje,

– ugrađen softver za samotestiranje i Ethernet interfejs.

Tehničke karakteristike:

– uspešnost detekcije nadzvučnih projektila je veća od 95%,

– greška u otkrivanju azimuta neprijateljskog strelca je manja od 2,5°,

– greška pri određivanju daljine do neprijateljskog strelca je +/–10%,

– detektuje relativan pravac strelaca za 1 s nakon dolaska akustičnog signala,

– detektuje pucnje koji su prošli pored vozila u prečniku od 1 do 30 metara.

Analitički model za ocenu efektivnosti sistema za zvukometrijsko izviđanje „boomerang“

Sistem za zvukometrijsko izviđanje sačinjen od „**n**“ jednorodnih zvukovnih sistema (stanica za zvukometrijsko izviđanje), koje mogu vršiti razmenu informacija mrežnim linkom. U sistem pristižu informacije sa intenzitetom „λ“, što predstavlja karakteristiku ulaznog toka izraženu kroz broj akustičnih signala u jedinici vremena, odnosno može se tretirati kao recipročna vrednost srednjeg vremena između dva dolaska akustičkih signala koji se obrađuju (λ = 1/tp, tp – srednje vreme između dva dolaska akustičkih signala). Intenzitet opsluživanja „μ“ predstavlja karakteristiku izlaznog toka izraženu kroz broj prenesenih informacija o smeru izvora zvuka u jedinici vremena, odnosno može se tretirati kao recipročna vrednost srednjeg vremena zauzetosti sistema za zvukometrijsko izviđanje (μ = 1/tops, tops – srednje vreme zauzetosti sistema za zvukometrijsko izviđanje). Karakteristika izlaznog toka „μ“ može se smatrati složenom, jer se sastoji od intenziteta obrade i intenziteta razmene informacija. Intenzitet opsluživanja jednak je zbiru ovih intenziteta pod pretpostavkom da i tok obrade podataka i tok razmene informacija imaju odlike Poasonovog toka.

Sistem se može naći u nekom od sledećih mogućih stanja:

S_0 – sve stanice za zvukometrijsko izviđanje su slobodne,

S_1 – jedna stanica za zvukometrijsko izviđanje je zauzeta, ostale stanice su slobodne,

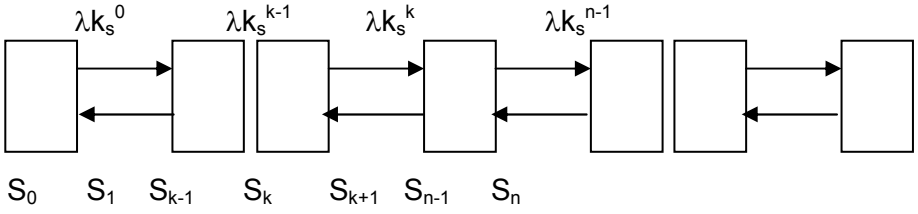
S_k – **k** stanica za zvukometrijsko izviđanje je zauzeto, ostale stanice su slobodne,

S_n – sve stanice za zvukometrijsko izviđanje su zauzete.

Da bi se odredila verovatnoća otkaza sistema (sistema za zvukometrijsko izviđanje) potrebno je najpre naći verovatnoću da se sistem nađe u **k-**tom stanju. Na taj način će se dobiti i verovatnoća otkaza sistema kao specijalni slučaj izvedene formule u kojoj je **k = n**.

Radi predstavljanja dinamike funkcionisanja sistema (kao sistema masovnog opsluživanja) i opisa sistema i njegovih stanja, neophodno je nacrtati graf stanja sistema.

Primenom mnemoničkih pravila [3] prikazan je graf stanja sistema **(S_0, S_1, . . . S_n)** sa intenzitetima prelaska iz jednog u drugo stanje (slika 2). Verovatnoće **$p_0(t)$, $p_1(t)$, . . . $p_n(t)$** predstavljaju verovatnoće da će se sistem naći u određenom stanju.



$p_0(t), p_1(t), \ldots, p_{k-1}(t), p_k(t), p_{k+1}(t), \ldots, p_{n-1}(t), p_n(t)$

Slika 2 – Prikaz grafa stanja sistema

Verovatnoća da će sistem preći iz jednog u drugo stanje jednaka je proizvodu verovatnoće da u sistem pristigne informacija (intenzitet dolaska informacija u sistem), odnosno verovatnoće da bilo koja stanica za zvukometrijsko izviđanje izvrši svoju misiju, tj. oslobodi se (intenzitet opsluživanja) i verovatnoće da svih **k** stanica za zvukometrijsko izviđanje budu u ispravnom stanju (bez otkaza) i da obavljaju svoju funkciju (raspoloživost izraženu koeficijentom spremnosti).[2] Za pojedina stanja sistema važe sledeće diferencijalne jednačine:

[2] Raspoloživost se iskazuje koeficijentom spremnosti koji se može predstaviti izrazom [2]:

$$K_s = \frac{T_o}{T_o + T_{no}} = \frac{T_o}{T} = \frac{T - T_{no}}{T} = 1 - \frac{T_{no}}{T}$$

gde je:

T_o – srednje vreme rada bez otkaza,

T_{no} – srednje vreme zastoja sistema, odnosno opravke,

T – ukupno planirano vreme rada.

$$p_0'(t) = -\lambda\, k_s^{0}\, p_0(t) + \mu\, k_s^{1}\, p_1(t) \quad (2)$$

$$p_k'(t) = \lambda\, k_s^{k-1}\, p_{k-1}(t) + (k+1)\mu\, k_s^{k+1}\, p_{k+1}(t) - (\lambda+k\mu)\, k_s^{k}\, p_k(t) \quad (3)$$

$$p_n'(t) = \lambda\, k_s^{n-1}\, p_{n-1}(t) - n\mu\, k_s^{n}\, p_n(t) \quad (4)$$

U slučaju graničnog, stacionarnog režima rada sistema, ovaj sistem diferencijalnih jednačina može se prevesti u sistem algebarskih jednačina. Kada se posmatranje vrši u dugom vremenskom periodu, tj. kada $\mathbf{t} \to \infty$, svi prvi izvodi verovatnoća jednaki su nuli i rešavanjem sistema jednačina izvodi se opšti izraz za verovatnoću stanja sistema:

$$p_k = \frac{\lambda^k}{k!\,\mu^k} \cdot \frac{1}{k_s^k}\, p_0 \quad (5)$$

Pošto je uslov:

$$\sum_{k=0}^{n} p_k = 1 \quad \Rightarrow \quad p_0 = \frac{1}{\sum_{k=0}^{n} \frac{\lambda^k}{k!\,\mu^k} \cdot \frac{1}{k_s^k}} \quad (6)$$

zamenom u opšti izraz (2) i ako uvedemo zamenu:

$$x = \frac{\lambda}{\mu} \cdot \frac{1}{k_s} = \frac{\alpha}{k_s} \quad (7)$$

dobija se formula Erlanga, koja određuje verovatnoću stanja sistema:

$$p_k = \frac{\frac{x^k}{k!}}{\sum_{k=0}^{n} \frac{x^k}{k!}}, \text{ odnosno } p_k = \frac{\frac{\lambda^k}{k!\,\mu^k} \cdot \frac{1}{k_s^k}}{\sum_{k=0}^{n} \frac{\lambda^k}{k!\,\mu^k} \cdot \frac{1}{k_s^k}} \quad (8)$$

Izraz (8) predstavlja verovatnoću da se posmatrani sistem nađe u stanju **k**, tj. verovatnoću da je **k** stanica za zvukometrijsko izviđanje zauzeto. Ako je **k = n**, tada su sve stanice za zvukometrijsko izviđanje zau-

zete, što znači da sistem za zvukometrijsko izviđanje nije više u stanju ni da preda ni da primi informacije, tj. nalazi se u stanju otkaza. Iz toga proizilazi da je verovatnoća opsluživanja sistema:

$$p_{op} = 1 - p_n = 1 - \frac{\frac{\lambda^n}{n!\mu^n} \cdot \frac{1}{k_s^n}}{\sum_{k=0}^{n} \frac{\lambda^k}{k!\mu^k} \cdot \frac{1}{k_s^k}} \qquad (9)$$

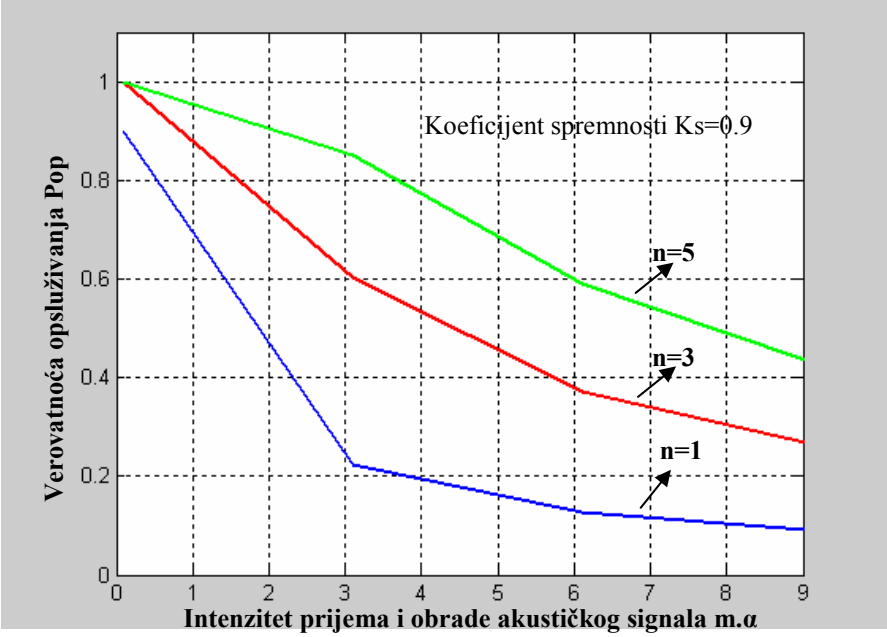
Verovatnoća opsluživanja sistema predstavlja kriterijum ocene efektivnosti rada sistema (sistema za zvukometrijsko izviđanje), odnosno njegovog funkcionisanja u zavisnosti od intenziteta dolaska informacija, intenziteta opsluživanja, raspoloživosti sistema za zvukometrijsko izviđanje i kapaciteta sistema.

Ocena efektivnosti sistema za zvukometrijsko izviđanje „boomerang“

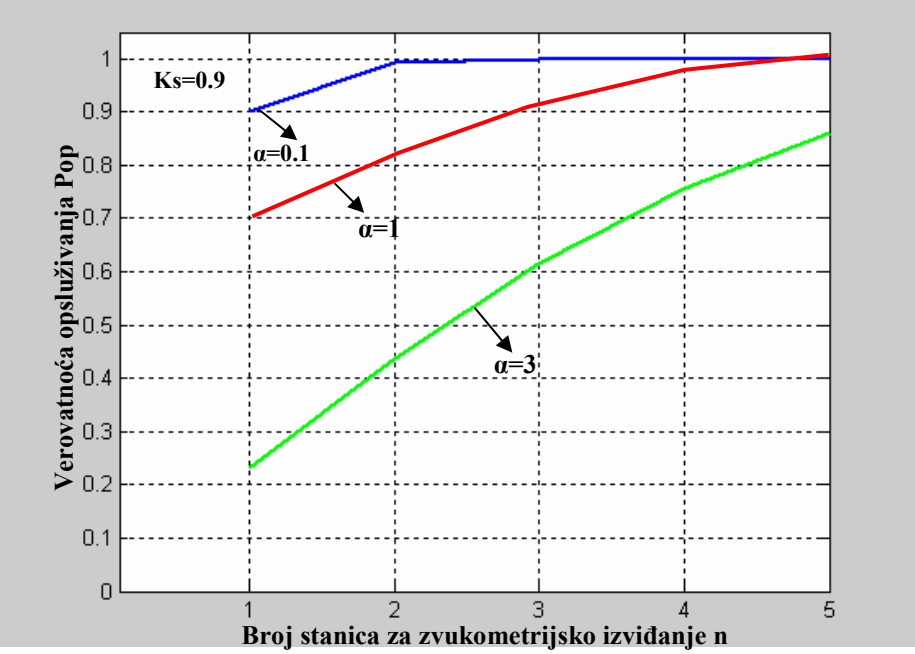
Izvedeni izraz (9) predstavlja osnovu za ocenu efektivnosti u zavisnosti od zadatih parametara. U relaciji (7) odnos intenziteta pristizanja akustičkih signala i intenziteta opsluživanja (obrade signala i dostavljanja informacija o smeru i lokaciji izvora zvuka) zamenjen je sa α **($\alpha = \lambda/\mu$)** i predstavlja „srednji broj akustičkih signala koje registruje stanica za srednje vreme opsluživanja“. Na osnovu izraza (9), za poznatu raspoloživost sistema za zvukometrijsko izviđanje **(k_s)** i različit broj stanica za zvukometrijsko izviđanje **(n),** može se analizirati zavisnost verovatnoće opsluživanja sistema za zvukometrijsko izviđanje **(p_{op})** od intenziteta prijema akustičkog signala, obrade i dostavljanja informacije. Izračunavanje verovatnoće opsluživanja (Pop) u funkciji intenziteta prijema akustičkog signala, obrade i dostavljanja informacije **(α)**, gde je kao parametar uzet broj stanica za zvukometrijsko izviđanje **(n)** i koeficijent spremnosti **(k_s)** će se provesti koristeći programski paket Matlab 6.5R13 [6].

Na slici 3 uočava se da verovatnoća opsluživanja opada sa povećanjem odnosa intenziteta prijema i obrade akustičkog signala, te da je jako zavisna od broja stanica za zvukometrijsko izviđanje.

Grafik na slici 3 predstavlja slučaj kada je vreme pauze između pucnjeva (akustičkih signala) od 1 do 10 sekundi i vreme opsluživanja od 1 do 3 sekunde, odnosno λ = 0,1–1, μ = 0,33–1. Parametar „**m“** predstavlja broj ponavljanja celokupnog događaja.



Slika 3 – Zavisnost verovatnoće opsluživanja od intenziteta prijema i obrade akustičkog signala za m = 1, 2, 3



Slika 4 – Zavisnost verovatnoće opsluživanja od broja stanica za zvukometrijsko izviđanje

Na sličan način može se analizirati zavisnost efektivnosti sistema za zvukometrijsko izviđanje od broja stanica, za zadate veličine drugih parametara (slika 4). Za izračunavanje verovatnoće opsluživanja u funkciji broja stanica za zvukometrijsko izviđanje **(n),** gde je kao parametar uzet odnos intenziteta, prijema i obrade signala i dostavljanja informacija **(α)** i koeficijent spremnosti **(k_s)**, korišćen je programski paket Matlab 6.5R13 [6].

Grafik zavisnosti omogućuje optimizaciju sistema za zvukometrijsko izviđanje, odnosno izbor potrebnog broja stanica za zvukometrijsko izviđanje radi obrade i prenosa određene količine informacija za zadatu (potrebnu) njegovu efektivnost i poznatu raspoloživost sistema za zvukometrijsko izviđanje.

Zaključak

Sistem za zvukometrijsko izviđanje „Boomerang“ je tehnički sistem čija se efektivnost ocenjuje verovatnoćom da će pomenuti sistem, u realnom vremenu, izvršiti detekciju, obradu i prenos informacija koje u njega pristižu, odnosno predstavlja verovatnoću opsluživanja sistema. Modelovan je kao sistem za masovno opsluživanje sa otkazom, a njegova svojstva opisana su parametrima: brojem stanica za zvukometrijsko izviđanje, njihovom raspoloživošću, intenzitetom dolaska zvučnih signala na sistem za zvukometrijsko izviđanje i intenzitetom opsluživanja sistema. Primenom programskog paketa Matlab 6.5R13 može se kvalitetnije i brže analizirati efektivnost sistema za zvukometrijsko izviđanje i predstaviti krive zavisnosti efektivnosti od parametara koji opisuju svojstva sistema. Za zadatu efektivnost može se odrediti broj potrebnih stanica za zvukometrijsko izviđanje u zavisnosti od broja akustičnih signala koje želimo pratiti. Analiza se može primeniti u proceni situacije i odlučivanju o upotrebi resursa u borbenim dejstvima.

Literatura

[1] Blanchard, B. S., Lowery E. E., Maintainability Principles and Practices, McGraw Hill Book Company, New York, 1969.

[2] Šepec, V., Procena efikasnost sistema veze u borbi, Makarije, Beograd, 2004.

[3] Vučićević, R., Teorija verovatnoće sa osnovama TMO, VIZ, Beograd, 2003.

[4] Vukadinović, S., Elementi teorije masovnog opsluživanja, Naučna knjiga, Beograd, 1975.

[6] Devetak, S., Đorđević, D., Analiza efikasnosti funkcionalnih radio-komunikacionih sistema, Vojnotehnički glasnik, br. 4/2008, str. 38–47, ISSN 0042-8469, Beograd, 2008.

[6] Programski paket Matlab 6.5R13.

[7] Boomerang, Operator´s Manual, www.bbn.com/boomerang.htm, 27. 02. 2009.

ONE APPROACH TO THE EVALUATION OF THE EFFECTIVENESS OF THE *BOOMERANG* SYSTEM FOR ACOUSTIC SOURCE LOCALIZATION AND IDENTIFICATION

Summary:

One approach to the evaluation of the effectiveness of a system for acoustic source localization and identification has been shown in this article. The system for acoustic source localization and identification has been presented as a model of mass servicing system. The states of the system as well as its features have been described while the formula for service probability determination has been derived as a criterion for effectiveness evaluation.

The introductory part of the article describes the system for acoustic source localization and identification and shows a model for quantity estimation of the function of technical system effectiveness E (t). The system effectiveness represents a probability of system initiation as well as a probability of its successful mission accomplishment on the basis of designed capabilites within the given time period and operational conditions.

The basic characteristics of the Boomerang system for acoustic source localization and identification show the system elements and its designed capability to detect, analyse and distribute acoustic source location data.

The analytical model for the evaluation of the effectiveness of the Boomerang system for acoustic source localization and identification shows that 'n' stations for acoustic source localization can exchange information with each other using the network link. The system conditions are described and the expression for the determination of service probability as a criterion for system effectiveness evaluation is derived.

The evaluation of the effectiveness of the Boomerang system for acoustic source localization and identification is presented with a formula for determining mass servicing system probability from the Matlab 6.5R13 program. The following graphs have been obtained:

– correlation between mass servicing probability and processing acoustic signal intensity for m=1,2,3,i;

– correlation between mass servicing probability and the number of stations for acoustic source localization and identification.

The obtained graphs help in the optimization of the system for acoustic source localization and identification.

The conclusion gives some guidelines in applying this analysis and achieving optimal resources employment in combat environment.

Key words: *acoustic source localization and identification, the theory of mass servicing, effectiveness, probability.*

Datum prijema članka: 05. 06. 2009.

Datum dostavljanja ispravki rukopisa: 23. 09. 2009.

Datum konačnog prihvatanja članka za objavljivanje: 25. 09. 2009.

KOMUNIKACIONI KANAL SA ŠIFROVANJEM INFORMACIJA

Markagić S. *Milorad,* Vojna akademija, Katedra vojnih elektronskih sistema, Beograd

UDC: 621.391

Sažetak:

U radu se opisuje jedan model telekomunikacionog kanala, na kojem su primenjene mere kriptozaštite informacija, sa sastavnim elementima kanala.

Da bi šifrovanje informacija bilo uspešno na celom spojnom putu neophodno je razmotriti neke osnovne odredbe telekomunikacione i kriptološke sinhronizacije i delimično naglasiti način šifrovanja informacije, kao i proces generisanja i distribucije kriptoloških ključeva.

Ključne reči: *telekomunikacioni kanal, šifrovanje, kriptološki ključevi.*

Uvod

Komunikacioni kanal, koji se koristi u komercijalne svrhe, nezavisno od modela i primenjenih uređaja i spojnih puteva, podložan je uticajima koji mogu biti prirodni ili veštački.

Osnovne vrste napada na komunikacioni kanal su: presretanje, obmanjivanje, ometanje i prisluškivanje.

Imajući u vidu da informacije koje koristi veliki broj javnih i državnih službi predstavljaju neki vid tajne, potrebno je da se na tim informacijama primene mere kriptozaštite – šifrovanje informacija.

Sam proces zaštite informacija vezan je za nekoliko parametara koji odlučujuće utiču na kvalitet, vrstu i zaštitu prenosa. To su, pre svega, parametri telekomunikacione i kriptološke sinhronizacije, kao i vrsta primenjenog kriptološkog ključa (ključa za šifrovanje i dešifrovanje).

U radu je prikazan jedan telekomunikacioni kanal sa sastavnim elementima, kako u smislu klasičnog prenosa informacija, tako i u načinu prenosa zaštićenih (kriptovanih) informacija. Analiziran je pojam kriptološke sinhronizacije i osnovni pojmovi telekomunikacione sinhronizacije koja prethodi kriptološkoj sinhronizaciji. Takođe, opisuju se i tri tipa kriptološke sinhronizacije: sinhronizacija na početku, tekuća sinhronizacija i sinhronizacija sa restartom. Analizirane su prednosti i nedostaci svih tipova kriptološke sinhronizacije sa kriptološkog i telekomunikacionog aspekta.

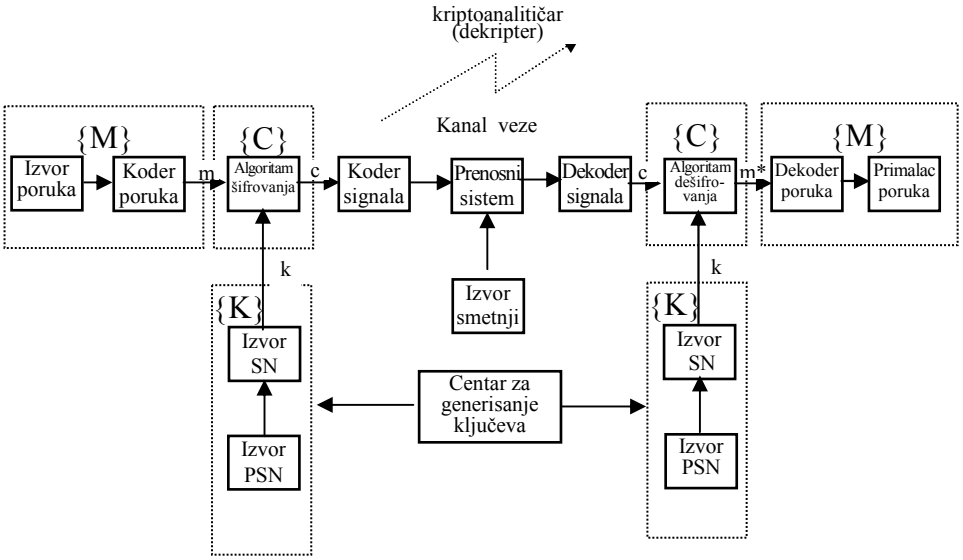
milmarkag@yahoo.com

Izvršena je i analiza parametara kriptološke sinhronizacije (dužina spoljašnjeg ključa, verovatnoća uspešne sinhronizacije i vreme sinhronizacije), na osnovu modernih saznanja iz oblasti kriptologije sa težištem na opštim i uzajamnim ograničenjima pri izboru ovih parametara.

Model komunikaconog kanala sa šifrovanjem informacija

U odnosu na opšti model komunikacionog kanala, komunikacioni kanal sa šifrovanjem informacija u svom sastavu ima još i elemenat – algoritam šifrovanja-dešifrovanja, a koji je realizovan u sklopu kriptouređaja. To može biti samostalni uređaj ili sklop u okviru telekomunikacionog uređaja.

Izgled ovog modela prikazan je na slici 1.



Slika 1 – Šema komunikacionog kanala sa šifrovanjem informacije

Uočava se da je za realizaciju algoritma potrebno obezbediti određene uslove, pa će biti prikazani kao izvori SN (slučajnog niza) i PSN (pseudoslučajnog niza). Ovi izvori najčešće se generišu na jednom mestu – centru za generisanje ključeva.

Shvatanje ovih elemenata, uz prihvatanje činjenica iznetih u poglavlju o elementima komunikacionog kanala bez šifrovanja informacija, pomaže da se sagleda problem kriptološke sinhronizacije i generisanja i distribucije ključeva.

Pojam sinhronizacije

Dva niza su sinhrona ukoliko se odgovarajući događaji u oba niza javljaju jednovremeno.

Sinhronizacija je proces kojim se ostvaruje i održava sinhrona situacija.

U telekomunikacionom sistemu pod sinhronizacijom se podrazumeva niz radnji i postupaka koji omogućuju uređaju na prijemnoj strani da izvrši inverzne transformacije onih transformacija koje vrši uređaj na predajnoj strani nad porukom kako bi je prilagodio kanalu.

U opštem slučaju kriptološka sinhronizacija je postupak koji obezbeđuje da GPSN (generator pseudoslučajnog niza) u prijemnom uređaju vrši inverziju transformacije poruke koju vrši GPSN u predajnom uređaju.

Kao što se zna, transformacija šifrovanja određenim algoritmom zavisi od elemenata: unutrašnjeg ključa (UK) i spoljašnjeg ključa (SK). Uz normalnu pretpostavku da predajni i prijemni GPSN imaju identičan UK, potrebno je obezbediti da imaju i identičan SK. Pošto se za svaku poruku generiše novi SK u predajnom uređaju, neophodno ga je preneti prijemnom uređaju. Prema tome, pod kriptološkom sinhronizacijom podrazumevamo proces prenošenja SK, sa kojim radi predajni GPSN, prijemnom GPSN.

Telekomunikaciona sinhronizacija

Neophodno je naglasiti da je GPSN po svojoj prirodi digitalni sklop koji funkcioniše na osnovu digitalnih ulaznih podataka (UK i SK) i signala takta. Prema tome, čak i u sistemima za zaštitu informacija na analognom nivou (npr. kod zaštite govornog signala na analognom principu) proces kriptološke sinhronizacije je u telekomunikacionom smislu proces digitalnog prenosa SK od predajnog GPSN prijemnom GPSN.

Da bi proces kriptološke sinhronizacije mogao otpočeti neophodno je da se prethodno završi proces tzv. telekomunikacione sinhronizacije. Kao što je rečeno, svi blokovi u modelu prijemnika telekomunikacionog sistema koji se nalaze između izlaza iz kanala i prijemnog GPSN, moraju obaviti inverzije transformacija koje se vrše u predajniku. Zavisno od složenosti telekomunikacionog sistema, postoji čitava hijerarhija sinhronizacionih problema koji se rešavaju u okviru telekomunikacione sinhronizacije. Ako se za prilagođenje kanalu koristi modulacija, onda je prvi nivo sinhronizacije sinhronizacija nosioca (po frekvenciji i fazi), što je potrebno za proces demodulacije. Nakon toga se iz analognog demodulisanog signala vrši ekstrakcija digitskog takta (bitska sinhronizacija) koja omogućuje konverziju analognog demodulisanog signala u digitalni (binarni niz). Nakon toga dolazi sinhronizacija kodnih reči (ukoliko se vrši zaštitno kodovanje poruke), zatim sinhronizacija rama koja omogućuje demultipleksiranje i, konačno, paketska sinhronizacija.

Kada se sve ove faze telekomunikacione sinhronizacije završe, uspostavljen je digitalni kanal i može otpočeti proces kriptološke sinhronizacije.

Tipovi kriptološke sinhronizacije

Kriptološka sinhronizacija predstavlja nalaženje optimuma između, uglavnom oprečnih, kriptoloških i telekomunikacionih zahteva. Iako su kriptološki zahtevi od prvenstvenog značaja, pogodno je izvršiti podelu kriptološke sinhronizacije i sa telekomunikacionog aspekta.

Pošto kriptološka sinhronizacija predstavlja proces digitalnog prenosa SK prijemnom uređaju, za njega, pre svega, treba obezbediti kanal.

Kako je tehnički neprihvatljivo, a materijalno nerentabilno da se sinhronizacija (telekomunikaciona i kriptološka) obavlja odvojenim kanalom, neophodno je izvršiti multipleksiranje sinhronizacionog sadržaja sa informacijom koju treba preneti, te se za prenos može koristiti isti telekomunikacioni kanal. Najčešće se koristi vremenski multipleks. Drugim rečima, kriptološka sinhronizacija prethodi šifratu.

Razlikuju se tri osnovna tipa kriptološke sinhronizacije:

– kriptološka sinhronizacija na početku poruke (sinhronizacija na početku),

– periodična kriptološka sinhronizacija (tekuća sinhronizacija), i

– sinhronizacija sa restartom.

Sinhronizacija na početku

Prednosti sinhronizacije na početku su:

– izuzev početnog kašnjenja ne narušava ukupan kapacitet kanala raspoloživ za prenos šifrata;

– obezbeđuje šifrovanje/dešifrovanje „bit-za-bit“ (jedna greška u šifratu proizvodi jednu grešku u otvorenom tekstu), i

– otežano je otkrivanje i ometanje.

Nedostaci sinhronizacije na početku su:

– ukoliko se iz nekih razloga ne ostvari uspešna sinhronizacija, propada čitava poruka;

– ukoliko dođe do „proklizavanja“ digitskog takta (što je retka, ali realna pojava), što se manifestuje ubacivanjem novog bita ili gubljenjem emitovanog, ostatak poruke je neupotrebljiv, i

– u radio-mreži ne omogućuje naknadno uključivanje učesnika.

Tekuća sinhronizacija

Prednosti tekuće sinhronizacije su:

– ukoliko se ne ostvari kriptološka sinhronizacija na samom početku poruke, postoji mogućnost da se ostvari pri sledećem emitovanju u okviru poruke. Drugim rečima, neostvarivanje kriptološke sinhronizacije na početku ne čini čitavu poruku beskorisnom;

– obezbeđuje šifrovanje/dešifrovanje bit-za-bit;

– uz složene tehničke zahvate i narušavanje kapaciteta kanala raspoloživog za prenos šifrata, može se rešiti problem „proklizavanja“ digitskog takta, i

– omogućuje naknadno uključivanje učesnika u radio-mreži.

Nedostaci tekuće sinhronizacije su:

– narušavanje kapaciteta kanala raspoloživog za prenos šifrata (da bi se sinhronizacija mogla periodično ubaciti u šifrat, kapacitet kanala mora biti jednak zbiru kapaciteta sinhronizacionog i informacionog kanala), i

– uočljivost kriptološke sinhronizacije na kanalu.

Izbor jednog od navedena dva tipa kriptološke sinhronizacije zavisi prevashodno od konkretnog telekomunikacionog sistema u kojem se vrši kriptozaštita.

Sinhronizacija sa restartom

Problem narušavanja kapaciteta kanala zbog prenosa kriptološke sinhronizacije, problemi neuspešne sinhronizacije, proklizavanja digitskog takta i naknadnog uključivanja učesnika u radio-mreži rešavaju se na sledeći način: ako se GPSN na predajnoj strani modifikuje tako da stalno prati sadržaj šifrata i da kada se pojavi tačno određena n-torka (određena sadržajem UK) GPSN uvek startuje od istog mesta (takođe određenog sadržajem UK), onda nije potrebno slati kriptološku sinhronizaciju prijemnom GPSN. Dovoljno je da prijemni GPSN prati sadržaj šifrata i čeka navedenu n-torku, zatim startuje od zadatog mesta i sinhronizacija je ostvarena.

Zbog ponavljanja startovanja GPSN od iste pozicije, ovaj način sinhronizacije dobio je ime sinhronizacija sa restartom.

Prednosti ovog metoda kriptološke sinhronizacije su što rešava većinu telekomunikacionih problema:

– nema narušavanja kapaciteta kanala, i

– neostvarivanje ili gubitak sinhronizacije iz bilo kog razloga traju samo do sledećeg restarta.

Glavni nedostatak je kriptološke prirode, pa je ova sinhronizacija teško prihvatljiva.

Prenos SK u skladu sa definicijom kriptološke sinhronizacije se ne vrši zato što je SK već poznat prijemnom GPSN. To je baš n-torka na osnovu koje se vrši restart. Pošto se radi o jednom ili o malom broju različitih SK, delovi jedne poruke se šifruju istim ili malim brojem različitih ključeva, što bitno smanjuje kriptološku vrednost algoritma, uprkos činjenici da se restart dešava na slučajan način. Da bi se iskoristile prednosti ovog metoda kriptološke sinhronizacije, neophodno da se restart relativno često dešava. To direktno utiče na dužinu n-torke i na korišćenje vrlo kratkog dela periode GPSN, koja može biti ekstremno velika, ali bez uticaja na kriptološki kvalitet rešenja.

Pri korišćenju restarta nije moguće šifrovanje/dešifrovanje bit-za-bit. Posledica je da jedna greška u šifratu izaziva više grešaka u otvorenom tekstu. Posebno je nepogodno kada se greška javi u restartnoj n-torki ili ukoliko prevede neku „sličnu“ n-torku u restartnu. U tom slučaju javlja se paket grešaka koji traje do sledećeg uspešnog restarta. To je neprihvatljivo u telekomunikacionim sistemima koji moraju tolerisati relativno veliku verovatnoću greške po bitu, reda 10^{-2} (KT i UVF/VVF radio).

Kod uređaja za zaštitu govora na analognom principu zaštita se može ostvariti, recimo, permutovanjem delova analognog govornog signala u f-t ravni (f-frekvencija, t-vreme). Permutovan signal se u svom analognom obliku šalje prijemniku. Digitalni kanal potreban za kriptološku sinhronizaciju može se ostvariti emitovanjem SK pre analognog šifrata, kada se sinhronizacija granica delova analognog govornog signala nad kojima treba izvršiti inverznu permutaciju ostvaruje zahvaljujući preciznosti oscilatora predajnika i prijemnika koji se sinhronizuju u fazi kriptološke sinhronizacije.

Drugi način, koji se, zahvaljujući jednostavnom tehničkom rešenju koje je inherentno jednom ovakvom uređaju, često koristi, obezbeđuje jedan deo spektra standardnog telefonskog kanala za prenos spoljašnjeg ključa. (Obično se bira deo spektra oko sredine kanala koji je najpogodniji za digitalni prenos). Bitska sinhronizacija ovde ima dvostruku ulogu. S jedne strane, omogućuje uspešnu detekciju spoljašnjeg ključa, a sa druge olakšava precizno određivanje granica delova analognog govornog signala, čime omogućuje preciznije vršenje inverzne permutacije u f-t ravni.

Parametri kriptološke sinhronizacije

Osnovni parametri kriptološke sinhronizacije su:
– dužina spoljašnjeg ključa,
– verovatnoća uspešne sinhronizacije,
– vreme sinhronizacije.

Ova tri parametra su međusobno povezana i na njihovo dimenzionisanje utiču kriptološki i telekomunikacioni zahtevi, kao i ograničenja vezana za konstrukciju uređaja (dimenzije, potrošnja el. energije, masa, itd.).

Telekomunikacioni zahtevi nose i deo taktičkih zahteva. Naime, postojeći telekomunikacioni sistem je već na određeni način korišćen i bez kriptozaštite, pa se obično zahteva da ne narušava njegove performanse.

Telekomunikacioni zahtevi su posebno kritični u dva slučaja:

1. Kada se vrši kriptozaštita signala u realnom vremenu (npr. u slučaju kriptozaštite govornog signala). U tom slučaju se postavljaju vrlo oštri uslovi za početno kašnjenje i nisu dozvoljeni diskontinuiteti u prenosu signala.

2. Kada se digitalni prenos vrši postojećim analognim kanalima (telefonski i radio-kanali). U tom slučaju se u kanalu pri prenosu računa sa verovatnoćom greške čak do $5 \cdot 10^{-2}$

Ova dva slučaja najčešće se javljaju zajedno. Ako se ima u vidu da je kapacitet navedenih kanala relativno mali, potrebno je izvršiti dodatnu kompresiju informacije koja se prenosi, što je čini osetljivijom na greške u prenosu.

S druge strane, ako se kriptozaštita vrši u mrežama za prenos podataka, one su već tako projektovane da korišćenjem niza tehnika obezbeđuju verovatnoću greške u kanalu za nekoliko redova veličine manju nego u navedenim slučajevima. Pored toga, ne postoji problem početnog kašnjenja pri prenosu podataka, tako da se u tom slučaju razmatra samo kriptološki aspekt problema.

Dužina spoljašnjeg ključa

Posmatrano samo sa kriptološkog aspekta, dužina SK trebalo bi da bude što veća, kako bi se dobio što veći broj različitih startnih pozicija GPSN i smanjila opasnost od šifrovanja različitih poruka istim ključem.

Ako se sa n označi dužina SK izražena brojem bita, onda GPSN može imati ukupno 2n različitih startnih pozicija. Ukoliko su one međusobno nezavisne i jednako verovatne (što se obezbeđuje načinom generisanja SK), onda je verovatnoća uzastopnog ponavljanja dva identična SK 2-n. Naravno, sa povećanjem broja poruka raste i verovatnoća da će se ponoviti već generisani SK.

Ako sa N označimo prosečan broj poruka između dve promene UK, onda očigledno mora biti zadovoljen uslov $2^n >> N$ [4].

Da bi se stekao osećaj o ovim vrednostima treba pretpostaviti da se u jednoj radio-telefonskoj mreži koja se intenzivno koristi UK menja svakih mesec dana. Uz pretpostavku da se koristi sinhronizacija samo na početku poruke, da prosečna poruka u ovoj mreži traje 10 s i da je mreža aktivna 24^h dnevno, dobija se da je N = 259200.

Ako se želi ostvariti $2n > 1000\ N$ dobija se $n \approx 28$.

Ukoliko n nije dovoljno veliko, ovaj odnos može se dobiti smanjenjem ukupnog broja poruka između dve promene UK. Češća promena (generisanje i distribucija) UK povezana je sa organizaciono-tehničkim poteškoćama.

U savremenim uređajima za kriptozaštitu GPSN se realizuju pomoću mikro-računara na bazi mikroprocesora. Da bi se olakšala obrada SK, po pravilu se bira da dužina SK bude celobrojni umnožak od 8 bita, odnosno ceo broj bajtova (niz od 8 bita = 1 byte (bajt)).

Verovatnoća uspešne sinhronizacije

Kao što se vidi, argumenti za povećanje dužine SK su vrlo čvrsti. S druge strane, međutim, zahteva se da verovatnoća uspešne sinhronizacije iznosi 0,95 do 0,99, zavisno od namene uređaja. Ova verovatnoća određena je verovatnoćom greške na kanalu kojim se prenosi SK i dužinom SK.

Najjednostavniji način za analizu (koji ne uzima u obzir statistiku grešaka u datom telekomunikacionom sistemu) jeste modeliranje kanala kojim se vrši kriptološka sinhronizacija, preko binarnog simetričnog kanala.

U ovom modelu, nezavisno od toga da li se emituje 0 ili 1, verovatnoća greške iznosi p, a verovatnoća tačnog prijema jednog bita 1-p. Greške su međusobno nezavisne.

U dosadašnjem tekstu nije izričito naglašeno da se SK mora potpuno tačno preneti. U kanalu sa greškama o tome se može suditi samo u okviru teorije verovatnoće.

Zaštitno kodovanje kao činilac verovatnoće uspešne sinhronizacije

Ako se rezultat ne može postići skraćenjem dužine SK na granicu kriptološke prihvatljivosti, jedino rešenje problema jeste korišćenje zaštitnog kodovanja SK.

Zaštitno kodovanje je postupak namernog unošenja redundanse u prenošenu poruku i to na način koji omogućuje detekciju i korekciju grešaka koje se javljaju u primljenoj poruci.

Teorija zaštitnog kodovanja predstavlja naučnu disciplinu u okviru statističke teorije telekomunikacija i nudi veliki broj tipova kodova, optimiziranih sa raznih aspekata (tip kanala, sinhronizacija, itd.).

U uslovima telekomunikacionog kanala ograničenog kapaciteta, koji ne dozvoljava zaštitno kodovanje cele poruke, korišćenje složenijeg zaštitnog kodovanja samo pri prenosu SK nije tehnički opravdano, a ponekad je i neostvarljivo (kada se radi o tekućoj kriptološkoj sinhronizaciji).

Najjednostavnije je zaštitno kodovanje ponavljanjem poruke neparan broj puta i majoritetnim (većinskim) odlučivanjem na prijemu. (Recimo, ako se poruka ponovi 3 puta, onda prijemnik za slučaj da se na istom mestu u sve 3 poruke jave 2 ili 3 jedinice odlučuje da je poslata jedinica. U suprotnom se odlučuje za nulu).

Ako se sa m označi (neparan) broj ponavljanja, onda je verovatnoća greške po bitu [2].

$$p_{1,m} = \sum_{i=\frac{m+1}{2}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \qquad (1)$$

U slučaju trostrukog ponavljanja dobija se

$$p_{1,3} = 3p^2 - 2p^3 \quad (2)$$

a u slučaju petostrukog ponavljanja

$$p_{1,5} = 10p^3 - 15p^4 + 6p^5 \quad (3)$$

Verovatnoća uspešne sinhronizacije data je sa

$$P^{sk} = (1-P_{1,m})^n \quad (4)$$

U tabeli 1 date su vrednosti Psk za parametre iz prethodnog primera, ali za slučaj trostrukog ponavljanja.

Tabela 1

Verovatnoća P_{sk} u slučaju trostrukog ponavljanja

p n	32	64
10^{-2}	0,9905	0,9811
10^{-3}	0,99999	0,99998

U slučaju verovatnoće greške veće od 10^{-2} može se koristiti petostruko ponavljanje. Međutim, pri verovatnoćama greške oko 10^{-1} smetnje su tako velike da naglo raste verovatnoća proklizavanja bitske sinhronizacije, odnosno razlikovanja broja emitovanih i primljenih bita, kada nijedan zaštitni kod ne pomaže.

Pri izradi ovakvih analiza treba neprestano imati na umu da se radi o vrlo visokom stepenu idealizacije prenosnog kanala, tako da se dobijeni rezultati mogu koristiti samo kao gruba procena stvarne situacije. Pravi uvid pružaju samo intenzivna laboratorijska merenja (ukoliko omogućuju simulaciju ključnih fenomena vezanih za prenos u konkretnom telekomunikacionom sistemu), odnosno merenja u realnim uslovima.

Zaštitni kodovi, izuzev specijalno projektovanih, „izlaze na kraj“, uglavnom, sa greškama koje su „raspršene“ u okviru poruke. Međutim, ako se duži niz uzastopnih bita primi sa velikom greškom, zaštitni dekoder postaje nemoćan. Takve greške nazivaju se paketiranim ili usnopljenim greškama.

Paket grešaka definiše se kao niz uzastopnih bita određene dužine, koji se prima sa verovatnoćom greške po bitu koja je znatno veća od prosečne vrednosti verovatnoće greške po bitu u datom telekomunikacionom sistemu. Definicija veličine greške u okviru paketa zavisi od performansi zaštitnog kodera (ukoliko postoji u sistemu) i osetljivosti prenošenih informacija na greške u prenosu. Pri prenosu digitalizovanog govornog signala sa malim vrednostima bitskog protoka to je između 0,1 i 0,5.

Efikasan metod borbe protiv paketa grešaka je tehnika preklapanja (eng. interleaving). Može se koristiti i u kriptološkoj sinhronizaciji, a posebno je popularna pri prenosu pisanog teksta preko radija.

Za primenu ove tehnike potrebno je poznavati statistiku paketiranih grešaka u posmatranom telekomunikacionom sistemu. Potrebno je poznavati raspodelu verovatnoća pojavljivanja paketa određene dužine, kao i raspodelu rastojanja između susednih paketa grešaka.

Ako se to zna, onda se na predajnoj strani vrši „raspršivanje“ susednih bita poruke u vremenu, tako da njihovo međusobno rastojanje bude veće od maksimalne dužine paketirane greške λ. Ako je 1p slučajna promenljiva koja predstavlja dužinu paketa grešaka, onda λ definišemo kao

$$P\{1p \geq \ell\} < \varepsilon$$

gde je ε proizvoljan broj iz intervala (0,1)

Ilustrovaćemo ovu tehniku sledećim primerom:neka je u nekom telekomunikacionom sistemu 1 = 10, a minimalno rastojanje paketa grešaka veće od 100. Ako obeležimo redne brojeve bita neke poruke sa 1, 2, 3,..., onda se u predajniku vrši memorisanje podataka koje treba preneti, a na liniju idu u sledećem redosledu:

1, 11, 21, ... 91,
2, 12, 22, ... 92,
.
.
.
10, 20, 30, ..., 100

U prijemniku se ova poruka ponovo memoriše, a zatim iščita u normalnom redosledu.

Ako se pri prenosu javio paket grešaka dužine 10 (što je izuzetno redak slučaj), onda će tek svaki deseti bit biti pogrešno primljen. Preciznije, biće primljen sa znatno većom verovatnoćom greške od prosečne. U nekim sistemima je i ovaj princip dovoljan da se poruka primi u granicama prihvatljivosti, a metod je posebno efikasan kada se udruži sa zaštitnim kodovanjem. On ne zahteva prenošenje dodatnih informacija, pa ne smanjuje kapacitet kanala raspoloživ za prenos informacija, a pogodan je i zbog jednostavnosti tehničke realizacije. Njegov nedostatak predstavlja dodatno kašnjenje, koje je jednako trajanju dela poruke na kojem se vrši premeštanje.

Do sada smo u razmatranju implicitno smatrali da prijemnik tačno prepoznaje kada počinje prijem spoljašnjeg ključa. To, međutim, nije ispunjeno u većini slučajeva.

U teoriji zaštitnog kodovanja postoji pojam sinhronizibilnosti, što je osobina koda da bude sinhronizovan na prijemu, odnosno da kao kodna reč ne može biti shvaćen neki pomeraj bilo koje kodne reči za određeni broj bita.

Metod višestrukog ponavljanja zbog potpune slučajnosti SK nema ove osobine. Teorijski, pod nekim uslovima se uz poznatu dužinu SK mogu odrediti granice n-torke SK, tekućim kroskoreliranjem date n-torke sa dve sledeće.

Sličan problem se javlja i pri određivanju granica dela poruke na kojoj se vrši preklapanje. Ovaj problem se rešava tako da se pre emitovanja SK šalje najava ili preambula kojom se obezbeđuje precizan prijem SK (bilo da se koristi zaštitno kodovanje ili ne).

Postoje i kodovi koji omogućuju detekciju i korelaciju greške u sinhronizaciji i to veoma brzo (sa stanovišta broja bita potrebnih za ustanovljenje sinhronizacije).

Jedan od pristupa rešavanju ovog problema jeste da se pošalje niz čija je autokorelaciona funkcija minimalna izvan osnovnog vrha. Postoji čitava klasa nizova sa ovom osobinom, a nazivaju se Barkerovi nizovi.

Pomerački registri sa povratnom spregom

Slične, ali nešto nepovoljnije osobine imaju pseudoslučajni nizovi generisani pomeračkim registrom sa odgovarajućim povratnim spregama. Zbog jednostavnosti generisanja i visoke pouzdanosti jednom ostvarene sinhronizacije oni se često koriste u vidu najave.

Ako je L dužina pomeračkog registra, onda on, kao što je poznato, uz odgovarajuće povratne sprege može generisati pseudoslučajni niz dužine $2^L - 1$, u kojem se nalaze sve L-torke, izuzev one sastavljene od samih nula.

Prema tome, moguće je na predaji postaviti pomerački registar u stanje koje će nakon 2^L-1 koraka dati, recimo, L-torku sastavljenu od svih jedinica. Kada se završi emitovanje ovog pseudoslučajnog niza započinje emitovanje SK.

U prijemniku se nalazi identičan pomerački registar sa povratnom spregom. Njemu je u početku raskinuta povratna sprega i u njega se upisuje sadržaj sa linije. Kada se napuni L bita, povratne sprege se zatvore i registar nastavlja sa autonomnim radom. Istovremeno započinje poređenje lokalno generisanog niza sa onim koji se prima. Ukoliko je pri početnom punjenju prijemnog pomeračkog registra primljeno svih L bita bez greške, poređenje nizova će dati grešku koja odgovara grešci u prenosu. Ukoliko je neki od početnih L bita u pomeračkom registru prijemnika pogrešno primljen, greška će biti jako velika. Odluka o tačnom/pogrešnom prijemu prvih L bita donosi se nakon sekvencijalnog testa, zbog brzine ove vrste testova. Pragovi odlučivanja se određuju prema uslovima greške u kanalu, pri kojima treba izvršiti sinhronizaciju za zadatu vrednost grešaka I i II vrste. Kao što je poznato, greška prve vrste se javlja ako je

primljeno početno stanje registra tačno, a test usled grešaka odbaci ovu hipotezu. Greška druge vrste bi bila kada se pogrešan sadržaj prihvati kao pravi.

Kada se ustanovi da ne postoji sinhronizacija lokalno generisanog i primljenog niza, povratna sprega prijemnog pomeračkog registra se ponovo raskida, novi sadržaj ulazi u registar i procedura se ponavlja.

Kada se ustanovi da je lokalni niz sinhronizovan sa dolazećim, sačeka se da se izgeneriše zadata L-torka (recimo sve jedinice, kao što je rečeno). Kada se ona detektuje to je signal da posle toga nailazi SK.

Verovatnoća korektne sinhronizacije prijemnika, P_N, zavisi od uslova prijema (greške na kanalu), dužine najave (dozvoljenog vremena odlučivanja) i pragova odlučivanja [1].

Prema tome, rezultujuća verovatnoća uspešne sinhronizacije biće data proizvodom

$$P_{us} = P_N \cdot P_S \tag{5}$$

Vreme sinhronizacije

Vreme sinhronizacije predstavlja vreme potrebno da se izvrši kriptološka sinhronizacija.

Ukoliko se radi o sinhronizaciji na početku, to je zbir vremena potrebnog za najavu (T_N) i vremena potrebnog za prijem spoljašnjeg ključa (T_{SK})

$$T_S = T_N + T_S \tag{6}$$

Ukoliko se radi o tekućoj sinhronizaciji može se govoriti o prosečnom vremenu potrebnom za uspešnu sinhronizaciju.

Ako se sa $T_Š$ obeleži vreme za koje se emituje šifrat između dve kriptosinhronizacije, prosečno vreme sinhronizacije će, u slučaju naknadno uključenog učesnika u radio-mreži biti

$$\overline{T_S} = 0,5T_Š + \sum_{i=1}^{\infty}\left[iT_S + (i-1)T_Š\right]\pi(i) \tag{7}$$

gde je $T_S = T_N + T_{SK}$

$\pi(i)$ predstavlja verovatnoću da je sinhronizacija ostvarena u i-tom pokušaju,

$\pi(1) = P_{US}$

$\pi(2) = P_{US}(1-P_{US})$,

.

.

.$\pi(i) = P_{US}\,(1-P_{US})^{i-1}$.

Na osnovu ovih relacija dobija se:

$$\overline{T}_S = \frac{T_S + T_{\check{S}}}{P_{US}} - 0,5 \cdot T_{\check{S}} \tag{8}$$

Kao što je objašnjeno, u sistemima za kriptozaštitu signala u realnom vremenu kašnjenje informacije na putu do prijemnika može biti oštro ograničeno.

Ukupno kašnjenje predstavlja zbir vremena potrebnog za telekomunikacionu sinhronizaciju, kriptološku sinhronizaciju, dešifrovanje i eventualno početno kašnjenje D/A konvertora.

Pri prenosu govornih informacija već je kašnjenje od 0,5 s značajno, a kašnjenje od 1 s već je praktično neprihvatljivo.

Ovde treba ukazati na još jedan problem. Kada se uređaj prebaci na predaju, korisnik mahinalno počinje da govori. Pošto po proceduri u tom trenutku kreće najava, a zatim SK, deo informacije propada, jer je tehnički neopravdano njeno memorisanje i naknadno emitovanje čitave poruke sa kašnjenjem [4]. To se obično prevazilazi tako što se u vreme slanja kriptološke sinhronizacije u slušalici emituje ton, kao znak zauzeća kanala. Ima, međutim, situacija kada je to neprihvatljivo i kod kojih je i vreme sinhronizacije kritično. Jedan primer je radio-veza, gde je veliki deo poruka veoma kratak, čak oko 1 s. Posebno je neprihvatljivo da pilot u fazi borbenih dejstava čeka da se završi upozoravajući ton, pa da počne da govori. Čitava situacija je otežana činjenicom da se za prebacivanje radio-uređaja koristi VOX (elektronski prekidač koji reaguje na pojavu govora).

Značaj vremena sinhronizacije (izraženog brojem bita potrebnog za njegovo postizanje) bitno zavisi od veličine bitskog protoka u posmatranom sistemu veze. Tako 1000 bita za sinhronizaciju nema isti značaj pri prenosu govora komprimovanog nekim od metoda analize i sinteze, gde su brzine prenosa do 2400 bit/s i prenosa govora digitalizovanog pomoću delta-modulacije, gde je brzina prenosa 32 kbit/s.

S druge strane, kao što je rečeno, pri prenosu podataka (u računarskim mrežama ili pri prenosu pisanog teksta) ovaj parametar, praktično, nije bitan.

Zaključak

Izloženi materijal daje osnovne informacije o komunikacionom kanalu sa zaštitom informacija i kriptološkoj sinhronizaciji. Istovremeno, data je više kvalitativna nego kvantitativna analiza problema koji se javljaju pri dimenzionisanju parametara kriptološke sinhronizacije.

Može se zaključiti da je problem rešavanja kriptološke sinhronizacije problem nalaženja optimuma između kriptoloških, telekomunikacionih i taktičkih zahteva i da je za njegovo rešavanje potrebno dobro poznavanje svih ovih elemenata, što znači da se u principu različito rešava zavisno od sistema veze u kome se vrši kriptozaštita.

Ova razmatranja, kao i razmatranja o telekomunikacionoj sinhronizaciji, omogućavaju sagledavanje problema generisanja i distribucije kriptoloških ključeva, odnosno izbor sistema kojim će se vršiti šifrovanje informacije.

Literatura

[1] Grupa autora, Elementi moderne kriptologije, GŠ VJ, Beograd, 1997.

[2] Dukić, M., Principi telekomunikacija, Akademska misao, Beograd, 2008.

[3] Šumonja, P., Zaštitno kodovanje kratkih binarnih sekvenci – magistarski rad, ETF, Beograd, 1992.

[4] Markagić, M., Interni radovi, Vojna Akademija, Beograd.

COMMUNICATION CHANNEL WITH THE ENCRYPTION OF INFORMATION

Introduction

According to predefined concepts as a basic provision of telecommunications, encryption synchronization and communication threats, it is possible to determine terms for a safe commercial communication channel.

The basis of this work is a model of a telecommunication channel with its elements, with encryption and without it. Pursuant to this model, this paper examines the problems of encrypting commercial communication channels.

The concept of encryption synchronization, realized by different types of synchronization, is discussed.

Model of a communication channel with information encryption

Compared with a general model, this one is composed of an algorithm for encryption and decryption. It could be realized as an element of a telecommunication device or as a separate device.

Understanding this element as well as a model without encryption helps comprehending a problem of encryption synchronization, generation and distribution of encryption keys.

Notion of synchronization

Generally, synchronization is a process which implies implementation and maintenance of a synchronous situation.

Encryption synchronization is, consequently, a procedure which means that the PRNG – (Pseudo Random Number Generator) in the

receiver performs the inversion of a transformation message made by the PRNG in the transmitter.

Encryption transformation using a particular algorithm depends on internal and external encryption keys.

Assuming that both the receiver and the transmitter have the same internal encryption key, and according to the fact that the device uses a new external encryption key for every new message, it is necessary to transmit that key to the receiver.

Encryption synchronization is, therefore, a process of transmitting the external encryption key from the PRNG of the transmitter to the PRNG of the receiver.

Communication synchronisation

In order to start the process of encryption synchronization, it is necessary to finish the communication synchronization.

During the communication synchronization, depending on how complex the communication system is, there is a hierarchy of synchronization problem solving.

Types of encryption synchronization

The types of encryption synchronization are:
– Encryption synchronization at the beginning of the message,
– Periodical encryption synchronization (current synchronization),
– Encryption synchronization with a restart.

Encryption synchronization at the beginning

The advantages of this synchronization are:

– except for initial delay, it does not impair the total channel capacity available for transmission of the ciphertext;

– it provides encryption / decryption „bit for a bit“ (an error in the ciphertext produces an error in the plaintext); and

– detection and jamming are difficult.

The disadvantages of synchronization at the beginning:

– if synchronization is not successful for some reason, the whole message is lost,

– if slipping of the digit clock happens, the rest of the message is useless,

– in radio-network, the later inclusion of participants is not allowed.

Periodical encryption synchronization

The advantages are:

– if there is no encryption synchronization at the beginning of the message, it can be realized in the next mailing;

– it provides encryption / decryption „bit for a bit“ (an error in the ciphertext produces an error in the plaintext);

– slipping of the digit clock can be solved;
– inclusion of participants is allowed later, in radio-network.
The disadvantages are:
– it impairs the total channel capacity available for transmission of the ciphertext;
– visibility of encryption synchronization on the channel.

Encryption synchronization with a restart

Due to the repetition of the same starting position, this synchronization is called synchronization with a restart.
The advantages are:
– total channel capacity is available for transmission,
– if there is no synchronization at the beginning of the message, it can be realized after the next restart.
The main disadvantage results from the encryption nature itself, and, as such, this type of synchronization is hardly acceptable.

Parameters of the external encryption key

The basic parameters of the external encryption keys are:
– length of the external encryption key;
– probability of successful synchronization;
– time of synchronization.
These three parameters are interrelated and their determination depends on encryption and communication requirements as well as on device limitations (dimensions, power consumption, mass, etc.)

Length of the external encryption key

From the encryption aspect, the length of the external encryption key should be as great as possible, in order to get as big number of starting positions of PRNGs s possible and to reduce the risk of various posts with the same encryption key.
In modern encryption devices, PRNGs are realized by means of microprocessor-based microcomputers.

Probability of successful synchronization

The arguments that the length of external encryption keys should be as great as possible are very strong. However, probability of successful synchronization is from 0.95 to 0.99, depending on a device.
The previous text does not explicitly emphasize that the external encryption key must be transferred completely correctly. Within an error channel, this can be judged only by the theory of probability.

Protective encoding as a factor of successful synchronization probability

Protective coding is a process of deliberate introduction of redundancy in the transmitted message and in a manner that allows detection and correction of errors that appear in the message.

The protective coding theory is a scientific discipline within the statistical theory of telecommunications and offers many types of codes optimized with various aspects (type of channel, synchronization, etc.). In terms of telecommunication channels of limited capacity which does not allow protective coding of an entire message, the use of protective complex encoding only during the transfer of external encryption key is not technically justified, and is sometimes impossible (when it comes to current encryption synchronization).

This section deals with protective coding by repeating messages an odd number of times and by majority decision-making at the reception.

Feedback shift registers

Similar, but slightly less favorable characteristics are those of pseudo-random sequences generated by feedback shift registers. Due to their generating simplicity and high reliability of once-realized synchronization, they are often used at the beginning.

Time of syncronization

Synchronization time is the time needed to perform encryption synchronization.

The importance of synchronization time (measured by a number of bits needed for its achievement) significantly depends on the size of channel rate in the monitored system. 1000 bits for synchronization does not have the same significance in the transfer of speech compressed by some of the methods of analysis and synthesis, where the transfer speed is up to 2400 bit / s, and in transmitting voice using delta-modulation, where the rate is 32 kbit / s.

On the other hand, as mentioned before, in data transmission (in computer networks and transmission of written text) this parameter is practically of no sifnificance.

Conclusion

The basic information about the communication channel with encryption of information and encryption synchronization is given here together with a more qualitative than quantitative analysis of the problems that occur when dimensioning parameters of encryption synchronization.

It can be concluded that the problem of solving encryption synchronization is a problem of finding the optimum between encryption, telecommunications and tactical requirements and that, in order to solve it, a good knowledge of all these elements is necessary, i. e. each particular problem is addressed separately, depending on a communication system in which cryptography is applied.

This consideration and the consideration of the telecommunications synchronization allow the assessment of the problem of generating and distributing encryption keys as well as selecting a system for information encryption.

Key words: *telecommunication chanel, encoding, encryption key.*

Datum prijema članka: 06. 08. 2009.

Datum dostavljanja ispravki rukopisa: 29. 01. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 01. 02. 2010.

DEFINISANJE EKVIVALENTNOG TORZIONOOSCILATORNOG SISTEMA

Trifković R. *Dragan,* Vojna akademija, Katedra vojnih mašinskih sistema, Beograd,
Obradović M. *Aleksandar*, Mašinski fakultet, Katedra za mehaniku, Beograd

UDC: 621.3.029:629.03

Sažetak:

U radu je prikazan postupak zamene elemenata kompleksnog torzionooscilatornog sistema brodske dizelmotorne propulzije uprošćenim ekvivalentnim elementima istih dinamičkih karakteristika. Izloženi postupak sadrži metode za određivanje ekvivalentnih dužina, krutosti i momenata inercije na osnovu jednakosti kinetičkih i potencijalnih energija realnih i ekvivalentnih elemenata sistema. Osim toga, analizirani su pobudni momenti koji izazivaju prinudne torzione oscilacije razmatranog sistema.

Ključne reči: *torzione vibracije, brodska dizelmotorna propulzija.*

Uvod

Da bi se izbegla nedozvoljena naprezanja elemenata mehaničkog sistema koji torziono osciluje neophodno je, u fazi projektovanja takvog sistema, proračunom odrediti, pre svega, sopstvene frekvencije i frekvencije prinude, odnosno kritične brzine obrtanja. U inžinjerskoj praksi obično se primenjuju dva principa za formiranje i rešavanje jednačina oscilovanja. Prvi, koji je i predmet ovog rada, podrazumeva uprošćavanje i idealizaciju posmatranog mehaničkog sistema za prenos snage sa brodskog motora na propeler. Uprošćenje se svodi na to da se realan sistem zameni jednostavnijim sistemom, istih dinamičkih karakteristika, koji se naziva ekvivalentni torzionooscilatorni sistem. Ekvivalentan sistem sastoji se od odsečaka vratila konstantnog prečnika i zanemarljive mase, ali iste krutosti kao kod realnih delova vratila i koncentrisanih masa koje zamenjuju realne mase. Rezultat takve idealizacije je model sa konačnim brojem stepena slobode čije je kretanje opisano sistemom običnih diferencijalnih jednačina. Drugi princip zasniva se na razmatranju realnog sistema kao složenog elastičnog tela sa beskonačno mnogo stepena slobode, čije je torziono oscilovanje opisano sistemom parcijalnih diferencijalnih jednačina. Specijalizovani računarski programi pružaju mogućnosti za uspešno rešavanje i najsloženijih sistema dife-

dragantrif@ptt.rs

rencijalnih jednačina matričnim metodama, kao i analizu oblika oscilovanja sistema. Za pravilno definisanje ekvivalentnog sistema važno je pravilno definisati sve njegove karakteristične veličine kao što su: dužine, momenti inercije, krutosti, prigušenja i poremećajni impulsi.

Ekvivalentna dužina i krutost

Ekvivalentan torzionooscilatorni sistem predstavlja vratilo sa koncentrisanim masama pričvršćenim na određenom rastojanju od njega ili sa diskovima jednakih momenata inercije kao i odgovarajuće realne mase.

Ekvivalentne dužine određuju se iz uslova jednakosti potencijalnih energija realnog i ekvivalentnog dela vratila prema izrazu [1]:

$$\frac{1}{2}[M_t \cdot \theta]_E = \frac{1}{2}[M_t \cdot \theta]_R \tag{1}$$

gde je: M_t – moment torzije [Nm],
δ – ugao uvijanja [rad].

Indeksi E i R odnose se na ekvivalentan, odnosno realan deo vratila.

Ugao uvijanja se proračunava prema formuli:

$$\theta = \frac{M_t l}{GI_0} = \frac{M_t}{c} = M_t e \tag{2}$$

gde je: G – modul klizanja [N/m^2],
I_0 – polarni moment inercije poprečnog preseka vratila [m^4],
c – torziona krutost vratila $c=GI_0/l$ [Nm/rad],
e – torziona elastičnost vratila [rad/Nm],
l – dužina vratila [m].

Iz jednačina (1) i (2) sledi da se jednakost potencijalnih energija svodi na jednakost torzionih krutosti ekvivalentnog i stvarnog dela vratila:

$$\left(\frac{GI_0}{l}\right)_E = \left(\frac{GI_0}{l}\right)_R \tag{3}$$

Ako se za ekvivalentno vratilo usvoji isti materijal, kao i kod realnog ($G_E=G_R$), iz izraza (3) dobija se dužina ekvivalentnog vratila:

$$l_E = l_R \frac{I_{0E}}{I_{0R}} \tag{4}$$

gde je: l_E – dužina ekvivalentnog vratila [m],
l_R – dužina realnog vratila [m],
I_{0R} – polarni momenti inercije realnog vratila [m^4],
I_{0E} – polarni momenti inercije ekvivalentnog vratila [m^4].

Pri aproksimaciji kolenastog vratila motora, za spoljni i unutrašnji prečnik ekvivalentnog vratila usvajaju se odgovarajuće vrednosti prečnika oslonačkog rukavca. Ukoliko na realnom vratilu postoje žlebovi ili stepenasti prelazi sa većeg na manji prečnik, njegova se krutost smanjuje zbog koncentracije napona. U tom slučaju, moraju se uvoditi popravni koeficijenti koji zavise od odnosa većeg i manjeg prečnika, kao i od veličine prelaznog prečnika. Složeni oblici vratila razlažu se na elementarne delove za koje se mogu sračunati ekvivalentne dužine. U tom slučaju je ugao uvijanja složenog dela jednak zbiru uglova uvijanja *n* elementarnih delova. Torziona elastičnost tako složenog dela jednaka je zbiru torzionih elastičnosti n elementarnih delova i predstavlja se izrazom:

$$\theta = \sum_{i=1}^{n} \theta_i \Rightarrow \quad \frac{1}{\mathrm{c}} = \sum_{1=1}^{n} \frac{1}{c_i} \tag{5}$$

Ekvivalentna dužina vratila, ugrađenog iza reduktora (uporno, međuvratilo i propelersko vratilo), proračunava se, na osnovu jednakosti potencijalnih energija, po formuli:

$$l_E = l_R \frac{I_{OE}}{I_{0R}} \cdot \frac{1}{\xi \cdot i^2} \tag{6}$$

gde je: i – prenosni odnos reduktora,

ξ' – popravni koeficijent obzirom na elastičnost zuba, oboda i diskova zupčanika (ξ' = 0,9 – 1,0).

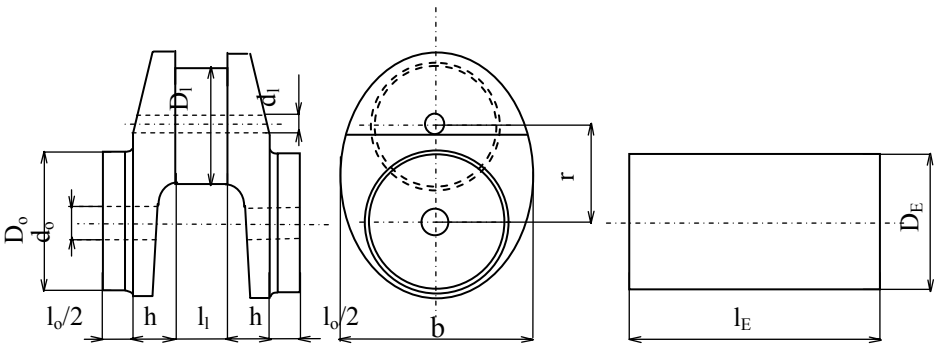
Ekvivalentne dužine i krutosti složenih oblika vratila i drugih delova realnog sistema mogu se određivati na tri načina: eksperimentom, numeričkom metodom (metodom konačnih elemenata) i empirijskim formulama [3], [4].

Eksperimentalni metod sastoji se u tome da se jedan kraj vratila fiksira, a na drugom kraju se deluje poznatim momentima uvijanja M. Za različite vrednosti momenta uvijanja dobijaju se odgovarajući uglovi uvijanja θ. Zatim se pomoću formule (2) računa krutost vratila c. Zbog male vrednosti ugla uvijanja često se prave greške u očitavanju, pa je potrebno napraviti više merenja i kao konačnu vrednost uzeti srednju vrednost torzione krutosti. Zatim se za prečnik ekvivalentnog vratila uzima prečnik oslonačkog rukavca i računa ekvivalentna dužina po formuli [6]:

$$l_E = \frac{GI_{0E}}{c} \tag{7}$$

gde su sve veličine ranije definisane.

Empirijske jednačine za određivanje ekvivalentne dužine i krutosti kolenastog vratila dobijene su kombinacijom eksperimentalnih i računskih metoda, a treba ih koristiti prema preporukama autora [3]. Za upotrebu ovih formula potrebno je poznavati dimenzije kolenastog vratila i osobine materijala (modul klizanja G). Na sl. 1 prikazana je skica jednog realnog i ekvivalentnog kolena kolenastog vratila.



Slika 1 – Skica realnog i ekvivalentnog kolena kolenastog vratila

Najčešće se u literaturi sreću sledeće aproksimirane jednačine za izračunavanje ekvivalentne dužine jednog kolena kolenastog vratila (prema oznakama na sl. 1) [3], [6]:

Wilsonova jednačina:

$$l_E = D_o^{\,4}\left(\frac{l_o + 0.4D_o}{D_o^4 - d_o^4} + \frac{l_l + 0.4D_l}{D_l^4 - d_l^4} + \frac{r - 0.2\left(D_l + D_o\right)}{hb^3}\right) \tag{8}$$

Tuplinova jednačina:

$$l_E = D_o^4\left\{\frac{l_o + 0.15D_o}{D_o^4\left[1-\left(\frac{d_o}{D_o}\right)^4\right]^2} + \frac{l_l + 0.15D_l}{D_l^4\left[1-\left(\frac{d_l}{D_l}\right)^4\right]^2}\right\} + \frac{2h - 0.15\left(D_o + d_l\right)}{b^4 - d_o^4} + \frac{r}{hb^3}\left(0.58 + \frac{0.065D_o}{h}\right) + \frac{0.016}{bh^2} \tag{9}$$

Zimanjenkova jednačina:

$$l_E = D_o^4 \left(\frac{l_o + 0.6\dfrac{D_o h}{l_o}}{D_o^4 - d_o^4} + \frac{0.8 l_l + 0.2\dfrac{bD_o}{r}}{D_l^4 - d_l^4} + \frac{r}{hb^3}\sqrt{\frac{r}{D_l}} \right) \tag{10}$$

Timošenkova jednačina:

$$l_E = D_o^4 \left(\frac{l_o + 0.9h}{D_o^4 - d_o^4} + \frac{l_l + 0.9h}{D_l^4 - d_l^4} + \frac{0.93r}{hb^3} \right) \tag{11}$$

Jackobsonova jednačina:

$$l_E = D_o^4 \left(\frac{l_o + 0.27D_o}{D_o^4 - d_o^4} + \frac{l_l + 0.27D_l}{D_l^4 - d_l^4} + \frac{0.07\left(l_l + 0.27D_l\right)^3}{D_l^4 - d_l^4} + \frac{0.7r}{hb^3} \right) \tag{12}$$

Southwellova jednačina:

$$l_E = D_o^4 \left(\frac{l_o}{D_o^4 - d_o^4} + \frac{l_l}{D_l^4 - d_l^4} + \frac{0.93r}{hb^3} + \frac{rl_l}{\left(D_l^4 - d_l^4\right)\dfrac{0.588 + l_l\left(D_l^4 - d_l^4\right)}{hb\left(h^2 + b^2\right)} + r} \right) \tag{13}$$

Heldtova jednačina:

$$l_E = D_o^4 \left(\frac{l_o + 0.4h}{D_o^4 - d_o^4} + \frac{1.096 l_l}{D_l^4 - d_l^4} + \frac{1.28r}{hb^3} \right) \tag{14}$$

Carterova jednačina:

$$l_E = D_o^4 \left(\frac{l_o + 0.8h}{D_o^4 - d_o^4} + \frac{0.75 l_l}{D_l^4 - d_l^4} + \frac{1.5r}{hb^3} \right) \tag{15}$$

Jednačine (8–15) dobijene su tako što su realni oblici ramena zamenjeni paralelopipedima, pri čemu je ukupan ugao uvijanja kolena zbir uglova uvijanja letećeg i oslonačkog rukavca i uglova savijanja ramena. Iz tog uslova određena je ekvivalentna krutost prema obrascu (5). Torzione krutosti letećeg i oslonačkog rukavca računaju se iz poznatog izraza za torzionu krutost vratila kružnog poprečnog preseka [8]. Krutost ramena određuje se na osnovu savojne deformacije ramena. Na ovaj način dobijena je polazna jednačina za određivanje ekvivalentne krutosti i dužine jednog kolena kolenastog vratila [6]. Zbog uprošćavanja oblika ramena ta jednačina je davala veće vrednosti krutosti. Uvođenjem različitih korekcija dobijene su i različite jednačine za ekvivalentnu dužinu kolena kolenastog vratila.

Ekvivalentne krutosti složenih geometrijskih oblika, kakvo je kolenasto vratilo motora, mogu se određivati i metodom konačnih elemenata (MKE). U tu svrhu se projektuje solid model jednog kolena, ukoliko je kolenasto vratilo izvedeno sa jednakim kolenima. Međutim, i ova metoda zahteva određena pojednostavljenja koja neće bitno uticati na rezultat, a odnose se na pojedine radijuse zaobljenja i otvore. Programski paket CAD (Computer Aided Design) omogućava određivanje ekvivalentne krutosti metodom konačnih elemenata.

Ekvivalentni moment inercije

Da bi se sve mase realnog sistema zamenile koncentrisanim masama (ili diskovima) mora se ispuniti uslov jednakosti kinetičkih energija realnog i ekvivalentnog sistema [1], [6], [12]:

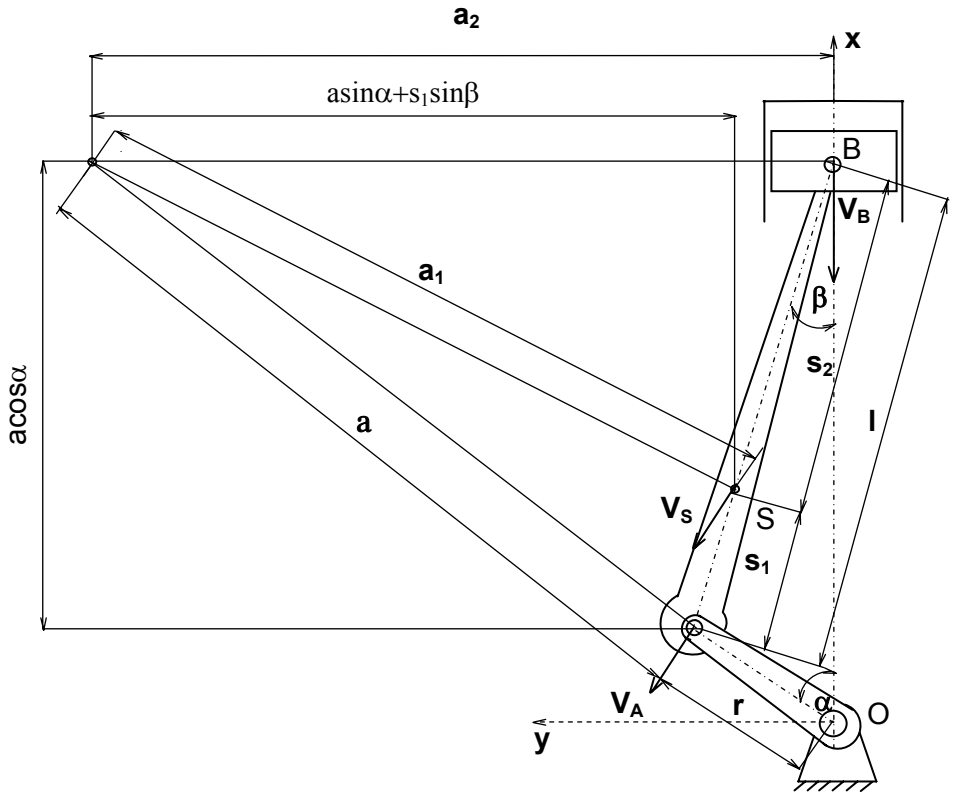
$$\frac{1}{2}[I\omega^2]_E = \frac{1}{2}[I\omega^2]_R \tag{16}$$

gde je: I – moment inercije [kgm^2],
ω – ugaona brzina vratila [rad/s].

Indeksi E i R se odnose na ekvivalentan, odnosno realan sistem.

Za linijske (nerazgranate) sisteme ovaj uslov se svodi na jednakost momenata inercije ekvivalentnog i realnog sistema. Pod linijskim sistemima podrazumevaju se sistemi sa jednim ili više vratila, koji nemaju prenosnike snage. Za elemente sistema koji imaju pravilne geometrijske oblike lako se određuju momenti inercije. U suprotnom, element složenog geometrijskog oblika se rastavlja na prostije oblike čiji se momenti inercije mogu lako odrediti. Suma pojedinačnih momenata inercije predstavlja moment inercije elementa složenog geometrijskog oblika. Momenti inercije mogu se određivati i pomoću crteža, a u nekim slučajevima i eksperimentalno. Moment inercije propelera najčešće se određuje eksperimentalnom metodom pomoću klatna [1], [9]. Posebna poteškoća javlja se pri određivanju ukupnog momenta iner-

cije kolena kolenastog vratila, koje je posredstvom klipnjače povezano sa klipnom grupom. Zbog toga će se analizirati prost klipni mehanizam motora (sl. 2), sastavljen od kolena (AO), klipnjače (AB) i klipa (B).



Slika 2 – Prost klipni motorni mehanizam

Koleno vrši rotaciono kretanje oko ose kroz tačku (O) i ima konstantan moment inercije za tu osu. Moment inercije sistema klipnjača–klip zavisi od ugla kolena kolenastog vratila α. Ukupan moment inercije za jedno koleno kolenastog vratila je zbir momenta inercije kolena i momenta inercije sistema klipnjača–klip. Moment inercije kolena dobija se kao zbir momenata inercije njegovih delova (rame, oslonački i leteći rukavac). Zbog pravolinijski oscilatornog kretanja klipne grupe i dela klipnjače na koleno kolenastog vratila se prenosi inercijalna sila ovih elemenata, kao inercijalni moment. Uz pretpostavku da su ovi elementi kruti, njihovi momenti inercije mogli bi se odrediti korišćenjem poznatih izraza iz dinamike. Međutim, zbog ravanskog kretanja klipnjače, određivanje njenog momenta inercije je složeno, pa se u praksi pribegava određenim uprošćenjima. U tom smislu

se masa klipnjače najčešće zamenjuje sa dve koncentrisane mase u tačkama (A) i (B). Deo mase klipnjače redukovan u tačku (A), na osi velike pesnice, vrši rotaciono kretanje, a deo mase klipnjače redukovan u tačku (B), na osi male pesnice, vrši pravolinijski oscilatorno kretanje.

Redukovani moment inercije sistema klipnjača–klip, u odnosu na osu kolenastog vratila, može se dobiti iz izraza za kinetičku energiju. Ova energija sastoji se od kinetičkih energija klipnjače (17) i klipne grupe (18), koje su date izrazima:

$$E_{k\check{c}} = \frac{1}{2} m_{k\check{c}} V_S^2 + \frac{1}{2} m_{k\check{c}} \rho_{k\check{c}}^2 \dot{\beta}^2 \tag{17}$$

$$E_{kg} = \frac{1}{2} m_{kg} V_B^2 \tag{18}$$

gde je: $E_{k\check{c}}$ – kinetička energija klipnjače [J],
E_{kg} – kinetička energija klipne grupe [J],
$m_{k\check{c}}$ – masa klipnjače [kg],
m_{kg} – masa klipne grupe [kg],
$\rho_{k\check{c}}$ – poluprečnik inercije klipnjače u odnosu na težište [m],
V_S – brzina težišta klipnjače [m/s],
V_B – brzina klipne grupe [m/s],
$\dot{\beta}$ – ugaona brzina klipnjače [rad/s].

Ako se tačka (P) izabere za centar obrtanja klipnjače, čije je težište u tački (S), onda se brzine tačaka (A), (S) i (B) prikazuju izrazima:

$$V_1 = a \cdot \dot{\beta} = r \cdot \dot{\alpha} \tag{19}$$

$$V_S = a_1 \cdot \dot{\beta} \tag{20}$$

$$V_B = a_2 \cdot \dot{\beta} \tag{21}$$

gde je: r – dužina ramena kolena kolenastog vratila [m],
α – ugaona brzina kolena kolenastog vratila [rad/s].

Rastojanja a, a_1 i a_2, u izrazima (19-21), prikazana su na sl. 2.

Iz jednačina (19) i (20) dobija se brzina težišta klipnjače:

$$V_S^2 = \left(\frac{a_1}{a} \right)^2 r^2 \dot{\alpha}^2 \tag{22}$$

Rastojanja a i a_1 mogu se izraziti pomoću sledećih jednačina:

$$a = l \frac{\cos\beta}{\cos\alpha} \tag{23}$$

$$a_1^2 = s_2^2 \cos^2\beta + \left(a \sin\alpha + s_1 \sin\beta \right)^2 \tag{24}$$

gde je: l – dužina klipnjače [m].

Ako se kinetička energija sistema klipnjača–klip izrazi preko redukovanog momenta inercije I_{kk}, sledi:

$$E = E_{k\check{c}} + E_{kg} = \frac{1}{2} I \dot{\alpha}^2 \tag{25}$$

gde je: E_{kk} – kinetička energija sistema klipnjača–klip [J],
I_{kk} – redukovani moment inercije sistema klipnjača–klip [kgm^2].

Ako se izraz (25) izjednači sa sumom jednačina (17) i (18), uz korišćenje jednačina (22), (23) i (24) dobija se izraz za redukovani moment inercije sistema klipnjača–klip:

$$I = m_{k\check{c}} r^2 \left[\left(\frac{s_2}{l} \right)^2 \cos^2 \alpha + \left(\sin \alpha + \frac{s_1}{l} \cos \alpha tg\beta \right)^2 \right] + m_{k\check{c}} \rho_{k\check{c}}^2 \delta^2 \frac{\cos^2 \alpha}{\cos^2 \beta} + \mathrm{m_{kg}} r^2 \left(\sin \alpha + \cos \alpha tg\beta \right)^2 \tag{26}$$

gde je: $cos\,\beta = \sqrt{1 - \delta^2 \, sin^2 \, \alpha}$, $\quad tg\beta = \dfrac{\delta sin\alpha}{\sqrt{1 + \delta^2 \, sin^2 \, \alpha}}$,

δ – kinematska karakteristika motora ($\delta = \dfrac{r}{l}$, sl. 2),

s_1 – rastojanje između ose letećeg rukavca i težišta klipnjače (sl. 2) [m],
s_2 – rastojanje između ose osovinice klipa i težišta klipnjače (sl. 2) [m].

Iz formule (26) zaključuje se da je redukovani moment inercije funkcija ugla kolenastog vratila koja se može i nacrtati. Ova funkcija je parna i periodična sa periodom 2π i može se razviti u red [6]. Za tačno određivanje redukovanog momenta inercije sistema klipnjača–klip mora se poznavati poluprečnik inercije klipnjače, a njegovo tačno određivanje predstavlja poteškoću zbog složenog oblika klipnjače.

Neki autori predlažu da se masa klipnjače zameni sa tri koncentrisane mase, raspoređene u tačkama (A), (B) i (S) (sl. 2.). Hafner je utvrdio da se pravi maksimalna greška od 5% ako se klipnjača zameni sa dve umesto sa tri mase [3].

U praksi se češće primenjuju približne formule za određivanje redukovanog momenta inercije sistema klipnjača–klip [7]:

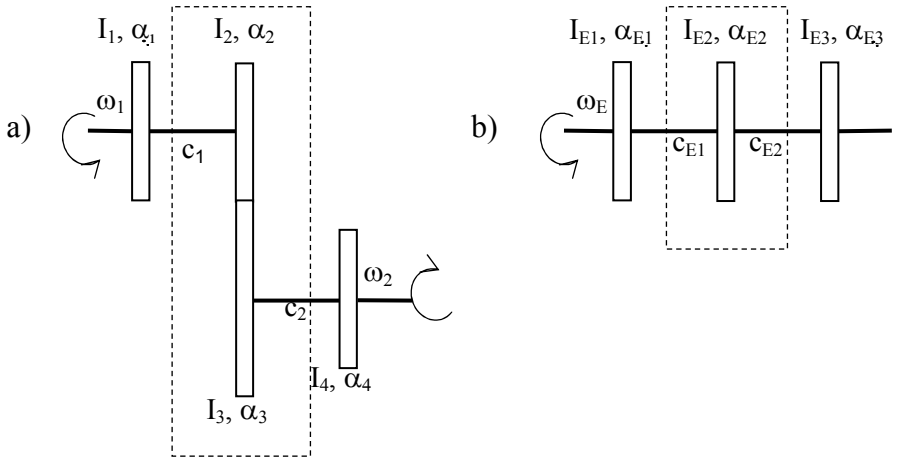
$$I = I_k + \left(m_{k\check{c}}^A + 0.5 m_B \right) r^2 \tag{27}$$

gde je: $\mathrm{m_{k\check{c}}^A}$ – masa rotirajućeg dela klipnjače [kg],
m_B – masa klipne grupe i dela klipnjače koji vrši pravolinijski oscilatorno kretanje [kg].

Ukupan redukovani moment inercije sistema koleno–klipnjača–klip dobija se sabiranjem redukovanog momenta inercije jednog kolena i redukovanog momenta inercije sistema klipnjača–klip. Kod motora sa „V“ rasporedom cilindara treba uzeti u obzir obe klipne grupe i obe klipnjače, vodeći računa o načinu na koje su one spojene sa kolenom kolenastog vratila.

Ekvivalentni moment inercije razgranatih sistema

Sistemi kod kojih se obrtni moment prenosi sa jednog na drugo vratilo pomoću zupčanika nazivaju se razgranati sistemi. Pri analizi torzionih oscilacija ovakvih sistema potrebno je sistem spregnutih vratila zameniti jednim ekvivalentnim vratilom. U sistemu brodske propulzije najčešće se obrtni moment sa jednog vratila prenosi na drugo pomoću jednostepenog zupčastog prenosnika. Šematski prikaz realnog i ekvivalentnog sistema prenosa snage sa jednostepenim reduktorom prikazan je na sl. 3. Realan sistem sastoji se od dva vratila, pogonskog i gonjenog, koji se obrću ugaonim brzinama ω_1 i ω_2. Na ovim vratilima nalaze se po dva diska, pri čemu dva spregnuta diska predstavljaju zupčanike reduktora, a preostala dva prirubnice vratila. Deformacije zupčastog para realnog sistema sa sl. 3. se zanemaruju.



Slika 3 – Šematski prikaz realnog (a) i ekvivalentnog (b) sistema prenosa snage sa jednostepenim reduktorom

Da bi se ovakav realan sistem zamenio ekvivalentnim mora se ispuniti uslov jednakosti kinetičkih i potencijalnih energija realnog i ekvivalentnog sistema. Prema oznakama na sl. 3. kinetička i potencijalna energija realnog sistema su [5]:

$$E_p = \frac{1}{2}\left[c_1 \left(\alpha_2 - \alpha_1\right)^2 + c_2 \left(\alpha_4 - \alpha_3\right)^2 \right] \tag{28}$$

$$E_k = \frac{1}{2}\left(I_1 \dot{\alpha}_1^2 + I_2 \dot{\alpha}_2^2 + I_3 \dot{\alpha}_3^2 + I_4 \dot{\alpha}_4^2 \right) \tag{29}$$

gde je: I_i – momenti inercije diskova realnog sistema (i = 1,4) [kgm^2],
α_i – uglovi obrtanja diskova realnog sistema (i = 1,4) [rad],
$\dot{\alpha}_i$ – ugaone brzine diskova realnog sistema (i = 1,4) [rad/s],
c_1, c_2 – torzione krutosti pogonskog i gonjenog vratila realnog sistema [Nm/rad].

Prenosni odnos zupčastog para *i* može se izraziti i preko odgovarajućih uglova obrtanja ili ugaonih brzina:

$$i = \frac{\alpha_2}{\alpha_3} = \frac{\dot{\alpha}_2}{\dot{\alpha}_3} \tag{30}$$

$$E_k = \frac{1}{2}\left[I_1 \dot{\alpha}_1^2 + \left(I_2 + \frac{I_3}{i^2} \right) \dot{\alpha}_2^2 + I_4 \dot{\alpha}_4^2 \right] \tag{31}$$

Uvrštavajući jednačinu (30) u jednačine (28) i (29) dobija se:

$$E_p = \frac{1}{2}\left[c_1 \left(\alpha_2 - \alpha_1\right)^2 + c_2 \left(\alpha_4 - \frac{\alpha_2}{i} \right)^2 \right] \tag{32}$$

Da bi se zadovoljio uslov jednakosti kinetičkih i potencijalnih energija realnog i ekvivalentnog sistema (sl. 3), moraju se ispuniti sledeći uslovi:

$$\begin{aligned} &\alpha_{e1} = \alpha_1, \quad \alpha_{e2} = \alpha_2, \quad \alpha_{e3} = \alpha_4 i, \quad \mathrm{I}_{e1} = I_1, \quad \mathrm{I}_{e2} = I_2 + \frac{I_3}{i^2}, \\ &\mathrm{I}_{e2} = \frac{I_4}{i}, \quad \mathrm{c}_{e1} = c_1, \quad \mathrm{c}_{e2} = \frac{c_2}{i^2} \end{aligned} \tag{33}$$

gde je: I_{Ei} – momenti inercije diskova ekvivalentnog sistema (i=1,3) [kgm^2],
α_{Ei} – uglovi obrtanja diskova ekvivalentnog sistema (i=1,3) [rad],
cE1, cE2 – torzione krutosti odsečaka vratila ekvivalentnog sistema [Nm/rad].

Ako se izrazi (33) smene u jednačine (31) i (32) dobija se kinetička i potencijalna energija ekvivalentnog sistema sa jednim vratilom:

$$E_k = \frac{1}{2}\left[I_{E1}\dot{\alpha}_{E1}^{2} + I_{E2}\dot{\alpha}_{E2}^{2} + I_{E3}\dot{\alpha}_{E3}^{2} \right] \tag{34}$$

$$E_p = \frac{1}{2}\left[c_{E1}\left(\alpha_{E2} - \alpha_{E1}\right)^2 + c_{E2}\left(\alpha_{E3} - \alpha_{E2}\right)^2 \right] \tag{35}$$

Analiza pobudnog momenta

Prinudne torzione oscilacije elastičnog sistema nastaju pod dejstvom periodičnog pobudnog momenta, pri čemu je frekvencija prinudnih oscilacija jednaka frekvenciji pobudnog momenta. Elementi klipnog mehanizma motora opterećeni su promenljivim momentima, koji pobuđuju kolenasto vratilo na torziono oscilovanje. Iz analize sila klipnog motornog mehanizma poznato je da se pobudni moment sastoji od momenta gasnih sila i momenta inercijalnih sila:

$$M(\alpha) = M_g(\alpha) + M_{in}(\alpha) \tag{36}$$

gde je: M_g – moment gasnih sila [Nm],
M_{in} – moment inercijalnih sila [Nm],
α – ugao obrtanja kolenastog vratila [rad].

Sile težine se zanemaraju zbog svoje male veličine, u odnosu na gasne i inercijalne, a sile trenja se uzimaju u obzir preko spoljašnjeg prigušenja [13, 14, 15].

Promenljivost pobudnog momenta uglavnom zavisi od: taktnosti motora, broja i međusobnog rasporeda cilindara, veličine masa koje pravolinijski osciluju, broja obrtaja i opterećenja. Tok promene pobudnog momenta je složena periodična funkcija, kako po uglu obrtanja kolenastog vratila za jedan radni ciklus, tako i sa aspekta promene režima rada. Da bi se analizirao uticaj pobudnog momenta na torzione oscilacije, neophodno je izvršiti njegovu harmonijsku analizu. Harmonijskom analizom se složen periodičan signal torzionog momenta predstavlja sumom prostoperiodičnih (sinusoidalnih) signala (harmonika) različitih amplituda, početnih faza i perioda (sl. 4). Svaki od harmonika izaziva prinudne oscilacije torzionog sistema, tako da se sabiranjem otklona od ravnotežnog položaja, izazvanih elementarnim torzionim momentima, dobija ukupan otklon jednak otklonu usled složenog torzionog momenta. Kako se pri promeni radnih režima motora pobudni momenti od gasnih i inercijalnih sila menjaju na različite načine, može se vršiti i odvojena harmonijska analiza ovih momenata [7].

1) Pobudni moment od gasnih sila

Iz dinamike klipnog motornog mehanizma (sl. 2) poznat je izraz za moment od gasnih sila [7], [10]:

$$M_g(\alpha) = p(\alpha) r \frac{D_k^2 \pi \sin(\alpha+\beta)}{4\cos\beta} \tag{37}$$

gde je: M_g – moment gasnih sila [Nm],
Δp – razlika pritiska gasa u cilindru i pritiska ispod klipa u kućištu motora [Pa],
D_k – prečnik klipa [m],
r – dužina ramena kolena kolenastog vratila [m],
α – ugao obrtanja kolenastog vratila [rad],
β – ugao otklona klipnjače u odnosu na osu cilindra [rad].

Za četvorotaktni motor period obrtnog momenta od gasnih sila je 4π, pa se može razviti u Furijeov red [13]:

$$M_g = M_{g0} + \sum_{k=1}^{\infty} a_k \cos\frac{k}{2}\alpha + \sum_{k=1}^{\infty} b_k \sin\frac{k}{2}\alpha\ , \qquad M_{g0} = \frac{1}{4\pi}\int_0^{4\pi} \mathrm{M_g d}\alpha,$$
$$a_k = \frac{1}{2\pi}\int_0^{4\pi} \mathrm{M_g}\cos\frac{k}{2}\alpha \mathrm{d}\alpha, \quad b_k = \frac{1}{2\pi}\int_0^{4\pi} \mathrm{M_g}\sin\frac{k}{2}\alpha \mathrm{d}\alpha, \tag{38}$$

gde je: k = 1, 2, 3,.. red pobude.

Amplituda M_k i fazni ugao φ_k harmonika k-tog reda mogu se izračunati na osnovu sledećih izraza:

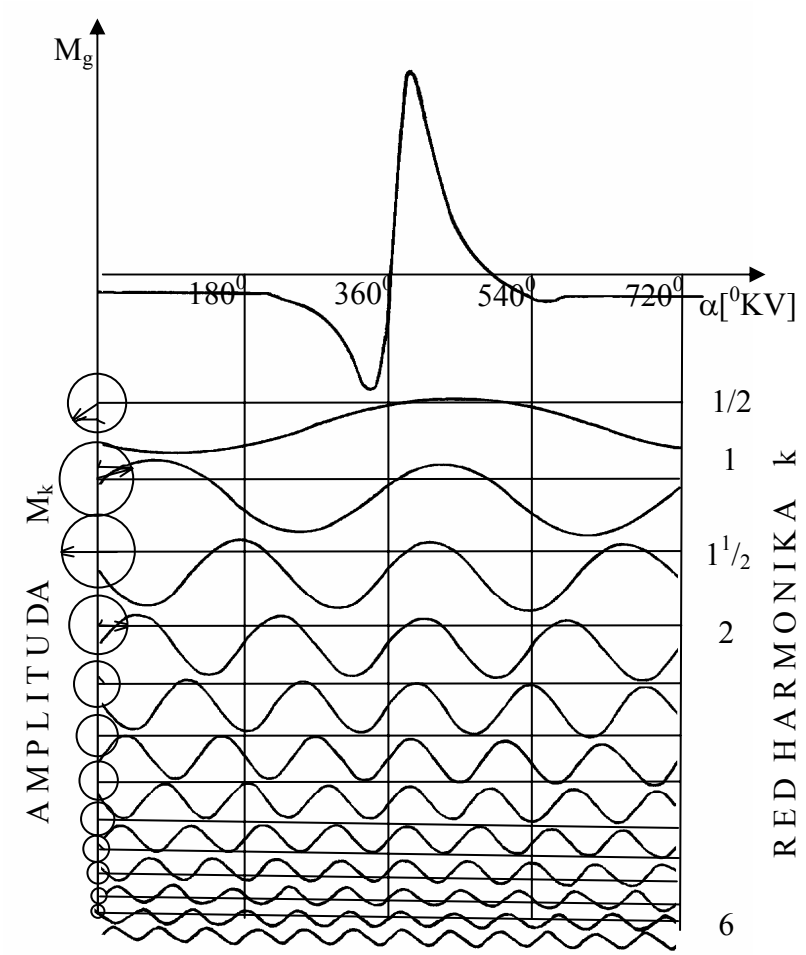
$$M_k = \sqrt{a_k^2 + b_k^2}\ , \qquad \varphi_k = arctg\frac{a_k}{b_k} \tag{39}$$

U tom slučaju se izraz (38) može pojednostaviti:

$$M_g = M_{g0} + \sum_{k=1}^{\infty} M_k \sin\left(\frac{k}{2}\alpha + \varphi_k\right) \tag{40}$$

Srednji obrtni moment od gasnih sila M_{g0} izaziva samo početni otklon od ravnotežnog položaja, tako da se može zanemariti. Iako je ugaoni položaj kolena kolenastog vratila određen uglom obrtanja ωt i uglom oscilovanja θ, obično se uzima da obrtni moment od gasnih sila zavisi samo od ugla obrtanja. Koeficijenti a_k i b_k (amplitude harmonika k-tog reda) mogu se odrediti na osnovu snimljenog toka pritiska u cilindru ili korišćenjem empirijskih formula.

Pri harmonijskoj analizi obrtnog momenta od gasnih sila obično se razmatraju harmonici do 12. ili do 18. reda. Ovako veliki broj harmonika uzima se u obzir zbog činjenice da vrednosti amplituda harmonika sporo opadaju sa porastom reda harmonika (sl. 4).



Slika 4 – Harmonijska analiza obrtnog momenta od gasnih sila jednog cilindra

Red harmonika k predstavlja broj punih oscilacija (perioda) nekog harmonika, koje se izvrše u toku jednog obrtaja kolenastog vratila motora. Odnosno, red harmonika se može definisati i kao broj pobudnih impulsa po jednom obrtaju kolenastog vratila. Potrebno je napomenuti da se red harmonika ne određuje po periodu radnog ciklusa, već po jednom

obrtaju kolenastog vratila. Kod četvorotaktnog motora se radni ciklus, pa i kriva momenta od gasnih sila, prostire na dva obrtaja kolenastog vratila, usled čega se javljaju harmonici reda 1/2, 1, 3/2, 2, .., koji se nazivaju motorni harmonici. Kod dvotaktnih motora radni ciklus se odvija za jedan obrtaj kolenastog vratila, pa se ne javljaju harmonici čiji redovi nisu celobrojni brojevi.

Da bi se izbegli komplikovani i skupi postupci snimanja toka stvarnog pritiska u cilindrima motora, za određivanje amplituda pobude od sile gasova i inercijalnih sila često se koriste različite približne metode (Maass i Klier, Wilson, Vihert, i dr.) [2], [4]. Analizirajući ove poluempirijske metode za proračun amplituda harmonika pobude M_k, može se doći do zaključka da je metoda koju su dali Maass i Klier najprihvatljivija, jer obuhvata veliki broj relevantnih parametara motora.

2) Pobudni moment od inercijalnih sila

Mase pokretnih delova klipnog mehanizma motora (sl. 2) izložene su promenljivom kretanju, usled čega se javljaju inercijalne sile, koje opterećuje motorske elemente i izazivaju oscilacije. Sa aspekta uravnotežavanja motora najveći problem predstavljaju inercijalne sile pravolinijski oscilatornih masa (klipna grupa i deo klipnjače redukovan na osu osovinice klipa). Pobudni moment od inercijalnih sila pravolinijski oscilatornih masa je periodična funkcija, sa periodom 2π, što odgovara jednom obrtaju kolenastog vratila. Ovaj moment može se razviti u Furijeov red, pri čemu se javljaju samo harmonici čiji su redovi celi brojevi. Međutim, u praksi se češće koristi sledeći približan izraz za pobudni moment od inercijalnih sila pravolinijski oscilatornih masa, dobijen bez razvijanja u Furijeov red [7]:

$$M_{in} \approx m_0 r^2 \dot{\alpha}^2 \left(\frac{\delta}{4} \sin\alpha - \frac{1}{2} \sin 2\alpha - \frac{3\delta}{4} \sin 3\alpha - \frac{\delta^2}{4} \sin 4\alpha \right) \tag{41}$$

gde je: M_{in} – pobudni moment od inercijalnih sila [Nm],

$\dot{\alpha}$ – ugaona brzina kolenastog vratila motora [rad/s],

m_0 – masa pravolinijski oscilatornih elemenata [kg],

r – poluprečnik kolena kolenastog vratila [m],

d – kinematska karakteristika motora (d = r/l, sl. 2).

Tok krive pobudnog momenta od inercijalnih sila pravolinijski oscilatornih masa blizak je harmonijskom, pa amplitude harmonika brzo opadaju sa porastom reda harmonika. Zbog toga je dovoljno posmatrati samo prva četiri harmonika. Iz izraza (41) se vidi da najveću amplitudu ima drugi harmonik, dok su amplitude prvog i četvrtog harmonika veoma male.

3) Pobudni moment kod višecilindričnog motora

Ukupan pobudni moment koji deluje na jedno koleno je, prema jednačini (36), suma pobudnog momenta od gasnih i inercijalnih sila. Ako se oba momenta razviju u red onda se ukupni moment može predstaviti pomoću reda čiji članovi imaju različite amplitude i faze. Ako se pretpostavi da su radni ciklusi u svim cilindrima višecilindričnog motora jednaki, onda su i pobudni momenti koji deluju na svim kolenima kolenastog vratila jednaki, ali fazno pomereni. Fazno pomeranje zavisi od geometrijske izvedbe motora i redosleda paljenja. Ugaoni razmak paljenja α_p određuje se iz uslova da se u toku jednog radnog ciklusa izvrši paljenje u svim cilindrima. Za četvorotaktni motor razmak paljenja je:

$$\alpha_p = \frac{4 \cdot \pi}{Z} \tag{42}$$

gde je: α_p – ugaoni razmak paljenja [°]
Z – broj cilindara.

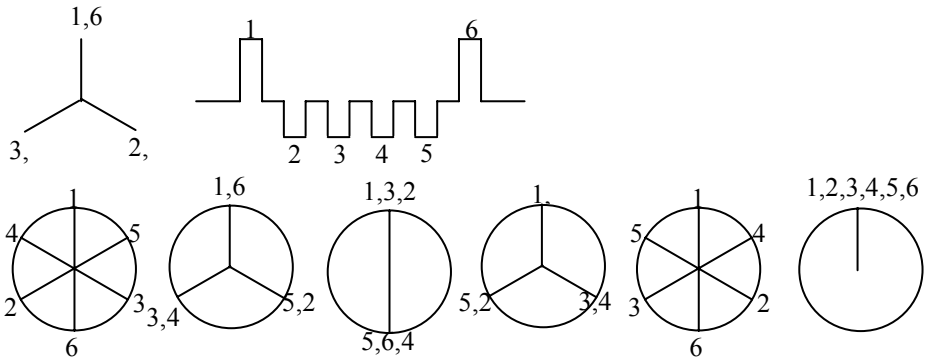
Ukupan pobudni moment, koji deluje na j-tom kolenu kolenastog vratila, može se predstaviti redom sa m harmonika [6]:

$$M(\alpha) = M_g(\alpha) + M_{in}(\alpha) = \sum_{k=1}^{m} \mathrm{M_{gk}} \sin\left(\frac{k}{2}\alpha + \varphi_{gk} - \phi_{jk}\right) + \sum_{k=1}^{m} \mathrm{M_{ink}} \sin\left(\frac{k}{2}\alpha - \phi_{jk}\right) \tag{43}$$

gde je: M_{gk} – amplituda k-tog harmonika pobudnog momenta od gasnih sila [Nm],
M_{ink} – amplituda k-tog harmonika pobudnog momenta od inercijalnih sila [Nm],
φ_{gk} – faza k-tog harmonika pobudnog momenta od gasnih sila [°],
ϕ_{jk} – faza k-tog harmonika pobudnog momenta koji deluje na j-tom kolenu kolenastog vratila [°] ($\phi_{jk} = 0$ za $j = 1$, $k = 1$),
α – ugao obrtanja kolenastog vratila [°].

Amplituda i faza k-tog harmonika pobudnog momenta od gasnih sila određuju se na osnovu izraza (39). Faze k-tog harmonika pobudnog momenta od gasnih i inercijalnih sila su jednake. Faza k-tog harmonika pobudnog momenta koji deluje na j-tom kolenu određuje se iz faznog dijagrama.

Crtanje faznog dijagrama biće objašnjeno na četvorotaktnom šestocilindričnom linijskom motoru sa razmakom paljenja od 120° i redosledom paljenja 1-5-3-6-2-4 (sl. 5).



k = 0.5; 3.5; 6.5; 9.5 k = 1; 4; 7; 10 k = 1.5; 4.5; 7.5; 10.5 k = 2; 5; 8; 11 k = 2.5; 5.5; 8.5; 11.5 k = 3; 6; 9; 12

Slika 5 – Raspored kolena četvorotaktnog šestocilindričnog linijskog motora i fazni dijagram harmonika pobudnog momenta

Fazni dijagram za (Z+i)-ti harmonik identičan je sa faznim dijagramom za i-ti harmonik, pa je dovoljno nacrtati samo prvih *Z* faznih dijagrama. Fazni (vektorski) dijagram se crta tako da se faze pobude na različitim kolenima nanose respektivno u odnosu na referentno koleno. Ciklus motora se prikazuje kružnicom, pri čemu se kao referentno koleno obično uzima prvo koleno. Harmonik reda k = 1/2 menja se sa frekvencijom ciklusa, pa za jedan obrtaj kolenastog vratila obavi samo pola ciklusa. Iako je peto koleno ugaono pomereno za 120° u odnosu na prvo, odgovarajući vektor momenta na ovom kolenu biće ugaono pomeren za 60° u odnosu na vektor momenta na prvom kolenu. Vektor pobudnog momenta za harmonik reda k = 1 dva puta brže rotira od vektora momenta za harmonik reda k = 1/2. To je posledica činjenice da harmonik reda k = 1 za jedan obrtaj kolenastog vratila napravi pun ciklus. Vektor pobudnog momenta na petom kolenu biće pomeren za ugao od 120° u odnosu na prvo koleno. Fazni uglovi harmonika ostalih redova dobijaju se tako što se fazni ugao harmonika reda k = 1 pomnoži sa redom harmonika čiji se fazni ugao želi odrediti. Pri proračunu torzionih oscilacija važno je poznavati fazni pomak, između amplituda momenata k-tog reda na prvom i i-tom kolenu, kako bi se odredili efekti pojedinih harmonika.

Harmonici kod kojih je red jednak ili deljiv sa brojem paljenja za jedan obrtaj kolenastog vratila nazivaju se glavnim, a glavni harmonik najnižeg reda je osnovni harmonik. U slučaju šestocilindričnog četvorotaktnog motora glavni su harmonici 3, 6, 9,.. reda, dok je harmonik 3. reda osnovni. Glavni harmonici su najopasniji, jer su u fazi na svim cilindrima (vektori u faznom dijagramu su kolinearni, sl. 5).

Fazni dijagrami linijskih motora mogu se primeniti i za motore sa „V“ rasporedom cilindara, ukoliko su im identični rasporedi kolena kolenastog vratila.

Zaključak

Zamenom realnog mehaničkog sistema za prenos snage sa kolenastog vratila brodskog motora na propeler odgovarajućim ekvivalentnim sistemom dobija se idealizovan i uprošćen torzionooscilatorni sistem, koji se sastoji od vratila zanemarljive mase sa određenim brojem koncentrisanih masa odgovarajućih momenata inercije. Od tačnosti kojom se definiše ekvivalentan sistem, odnosno od tačnosti kojom se određene ekvivalentne dužine, krutosti i momenti inercije elemenata ekvivalentnog sistema, te tačnosti kojom je izvršena analiza prinude zavisi i tačnost izračunatih frekvencija sopstvenih oscilacija i frekvencija prinudnih oscilacija.

Literatura

[1] Jankov, R., Blažić, Ž.: Ispitivanje i analiza torzionih oscilacija u sistemu za prenos snage za pogon ventilatora guseničnog vozila, Mašinski fakultet, Beograd, 1999.

[2] Filipović, I.: Torzione oscilacije motora sa unutrašnjim sagorijevanjem, Mašinski fakultet, Sarajevo, 1998.

[3] Hafner, K. E., Maass, H.: Torsionsschwingungen in der verbrennungskraftmaschinen, Springer-Verlag, Wien, New York, 1986.

[4] Wilson, W. K.: Practical solution of torsional vibration problems, Chapman & Hall, London, 1963.

[5] Vuković, J., Obradović, A.: Linearne oscilacije mehaničkih sistema, Mašinski fakultet, Beograd, 2007.

[6] Milašinović, A.: Uticaj translatornih masa krivajnog mehanizma na torzione oscilacije kolenastog vratila, Magistarski rad, Banja Luka, 2001.

[7] Živković, M.: Motori sa unutrašnjim sagorevanjem, II deo, Mašinski fakultet, Beograd, 1983.

[8] Rašković, D.: Otpornost materijala, Građevinska knjiga, Beograd, 1990.

[9] Šretner, J.: Brodski motori s unutarnjim izgaranjem, Fakultet strojarstva i brodogradnje, Zagreb, 1972.

[10] Tomić, M., Petrović, S.: Motori sa unutrašnjim sagorevanjem, Mašinski fakultet, Beograd, 1994.

[11] Trifković, D.: Istraživanje torzionih oscilacija u sistemu prenosa snage sa brodskog dizel motora na propeler, Magistarski rad, Mašinski fakultet, Beograd, 2004.

[12] Jankov, R.: Simulacija i eksperimentalno ispitivanje torzionih oscilacija, Mašinski fakultet, Beograd, 2002.

[13] Harker, R.: Generalized methods of vibration analyzis, University of Wisconsin, Madison, 1983.

[14] Trifković, D., Petrović, Ž., Dobratić, P.: Rezultati proračuna torzionih oscilacija u sistemu brodske dizel motorne propulzije, Vojnotehnički glasnik br. 3/2008, str. 102–119, ISSN: 0042–8469, Beograd.

[15] Trifković D., Nikolić R., Petrović Ž.: Rezultati merenja torzionih oscilacija u sistemu propulzije brodskog dizel motora, Vojnotehnički glasnik br. 6/2005, str. 86–93, ISSN: 0042–8469, Beograd.

DETERMINATION OF THE EQUIVALENT TORSIONAL VIBRATION SYSTEM

Summary:

The procedure of replacing the elements of a complex torsional vibration system of ship diesel engine propulsion with simplified equivalent ones with the same dynamic characteristics is shown in this work. The given procedure comprises the methods for the determination of equivalent lengths, stifnesses and moments of inertia based on the equality between kinetic and potential energy of real and equivalent elements of the system. Additionally, the exciting moments which excite forced torsional vibrations of the considered system are analysed.

Introduction

Two basic principles for forming and solving equations of vibration are often used in engineering practice. The first one, presented here, implies simplification and idealization of a mechanical system for transmission of power from the ship engine onto the propeller. A real system is substituted with a simplified one with the same dynamic characteristics called an equivalent torsional oscillating system. The equivalent system consists of shaft segments with a constant diameter and negligible mass, but with the stiffness corresponding to the real and concentrated masses. This idealization leads to the model with finite degrees of freedom (DOF) the movement of which is described by the system of ordinary differential equations.

The equivalent length and stiffness

Equivalent lengths are determined from the condition that the potential energies of the real shaft segment and the equivalent one are equal. This condition results in equal torsional stiffness of the real shaft segment and the equivalent one.

The equivalent moment of inertia

In order to sabstitude all masses of the real system with concentrated ones or disks, the condition of equality of kinetic energies of the real system and the equivalent one must be fulfilled. For linear systems this condition leads to equality of the moment of inertia of the equivalent system and the real one. The sum of the single moments of inertia presents the moment of inertia of the elements of a complex geometric shape. The moment of inertia can be defined graphically or, in some specific cases, experimentally. For example, the moment of inetia of the propeller is often defined experimentally by the method of pendulum. A particular difficulty appears during defining the total moment of inertia of the crank of crankshaft linked to the piston by the connecting rod.

While analyzing torsional vibrations of these systems, it is necessary to substitute the system of coupled shafts with an equivalent shaft.

The analyses of the moment of excitation

In order to analyze the influence of the moment of excitation on torsional vibration, its harmonic analysis must be performed. With this method, a complex periodical signal of torsional vibration can be represented by a sum of simple periodical signals (harmonics) with different amplitudes, phases and periods.

1) The gas forces moment of excitation

During the analysis of the gas forces moment, the harmonics up to 12th or 18th order are usually considered. In order to avoid complex and expensive procedures of recording pressure in engine cylinders, different approximate methods for determining amplitudes of the excitation from the gas and inertial forces are often applied. The analysis of these quasi-empirical formulae can lead to the conclusion that the Maass and Klier methods are the most acceptable ones, because they include numerous engine parameters.

2) The inertial forces moment of excitation

The principle of change of the moment of excitation of inertial forces, originated from linear oscillating masses, is similar to the harmonics principle. Therefore, the amplitudes of harmonics decrease steeply as the order of harmonics increases, so it is enough to consider the first four harmonics.

3) The multicylinder moment of excitation

The total moment of excitation on one crank is the sum of the moment of excitation of gas and inertial forces. If both moments are expanded into a series, then the total moment can be represented by a series with different amplitudes and phases of the members. If we assume that all operating cycles in the cylinders are equal, then all the moments of excitation on all cranks of the crankshaft are equal too, but phase- shifted.

Key words: *torsional vibrations, ship diesel engine propulsion system*

Datum prijema članka: 23. 01. 2009.

Datum dostavljanja ispravki rukopisa: 16. 12. 2009

Datum konačnog prihvatanja članka za objavljivanje: 18. 12. 2009.

PRIMENA FUZZY LOGIKE I VEŠTAČKIH NEURONSKIH MREŽA U PROCESU DONOŠENJA ODLUKE ORGANA SAOBRAĆAJNE PODRŠKE

Pamučar D. *Dragan,*
Vojna akademija, Prodekanat za planiranje i organizaciju nastave, Beograd

UDC: 356.257:004.89

Sažetak:

Ključna tačka u procesu upravljanja saobraćajem u Vojsci Srbije jeste proces donošenja odluke. U radu je predstavljen neuro-fuzzy model kao podrška procesu odlučivanja, koji uspešno oponaša proces odlučivanja organa saobraćajne podrške.

Ključne reči: *odlučivanje, neuro-fuzzy, pristup, ANFIS*.

Uvod

Upravljački proces u svakoj organizaciji odvija se donošenjem odgovarajućih odluka i njihovim pretvaranjem u akcije. To znači da se proces upravljanja često izjednačava sa procesom odlučivanja, što ukazuje na veliki značaj odlučivanja u procesu upravljanja organizacijama. Od pravilnosti odlučivanja, odnosno od toga koliko su pravilno preduzete akcije, zavisi efikasnost upravljanja, kao i funkcionisanje i razvoj svake organizacije [1].

Organizacioni sistem u kojem se vrši upravljanje je i Vojska Srbije. Organi koji su u njoj uspostavljeni, a među kojima su i organi saobraćajne službe, svakodnevno su u prilici da donose odluke. Nivoi značaja odluka u Vojsci su različiti, od dnevno-operativnih do strategijskih. Međutim, značaj samog procesa odlučivanja i donošenja odluka su podjednaki bez obzira na to o kom nivou odluka se govori.

Organi saobraćajne podrške ponekad se nalaze u situaciji da imaju samo jednu akciju i tada se donošenje odluke svodi na prihvatanje ili odbacivanje te akcije. Međutim, često se organi saobraćajne podrške nalaze u situaciji da rangiranjem više ponuđenih akcija dođu do zaključka koja je najbolja i koju treba izabrati. Samo rangiranje svodi se na vrednovanje ponuđenih akcija, a izbor sledi na osnovu najbolje pokazanih rezultata određene akcije.

dpamucar@gmail.com

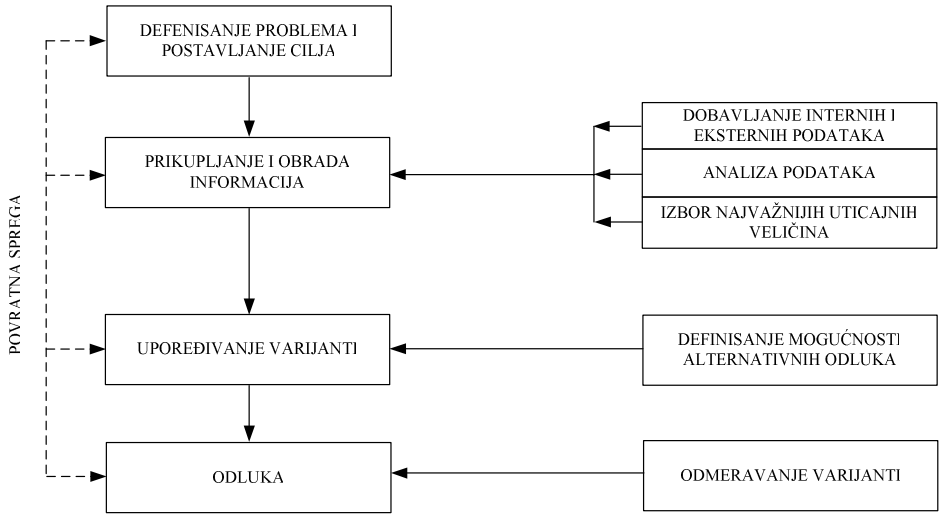
Ovakvi zaključci nameću potrebu da se procesu odlučivanja i donošenju odluka pristupa pažljivo i sistematski, bez obzira na to o kakvim se odlukama radi, jer bilo koja pogrešna odluka vodi slabljenju borbene gotovosti Vojske Srbije.

Proces odlučivanja u vojnoj organizaciji

U najvećem broju slučajeva u vojnoj organizaciji do procesa odlučivanja dolazi u uslovima neraspolaganja relevantnim informacijama, u situacijama veće ili manje neodređenosti o budućim dejstvima okruženja, o efektima pojedinih varijanti i dr.

Odlučivanje, kao postupak u procesu rukovođenja, ima drugačiji i specifičniji značaj nego ostali postupci. Ono povezuje zaključak (rešenje), kao završetak misaonog procesa sa akcijom kao početkom realizacije. Zbog takvog svog značaja, odlučivanje delimično pripada pripremi rukovođenja, a delimično pripremi akcije. To znači da odlučivanje povezuje dve oblasti ljudske delatnosti: intelektualni rad i materijalnu realizaciju, teoriju i praksu. To pokazuje da je odlučivanje ključni postupak u procesu rukovođenja [2], [8].

Da bi se struktura procesa odlučivanja u vojnoj organizaciji u potpunosti shvatila, neophodno je proces odlučivanja razložiti na logičke elemente – faze (slika 1).



Slika 1 – Struktura procesa odlučivanja u vojnoj organizaciji [3]

Proces odlučivanja ne odvija se uvek preko svih tih elemenata i istim redosledom. U toku procesa dejstvo elemenata ne može da se veže isključivo za pojedine faze procesa, već se njihov uticaj prepliće, ponavlja i dopunjuje. Takođe, njihov intenzitet se menja od situacije do situacije.

Proces odlučivanja u vojnoj organizaciji sadrži određene elemente[3]. To su:

– ciljevi,
– kriterijumi,
– formulacija problema,
– alternative,
– modeliranje i
– sprovođenje odluke.

Odluke se donose radi dostizanja određenih ciljeva. Utvrđivanje ciljeva sistema nije lak zadatak i obično zahteva da se obave prethodna proučavanja čitavog niza informacija. Pod ciljem u vojnoj organizaciji podrazumevaju se zadaci koje mora ostvariti posmatrani vojni sistem – vojna jedinica. Cilj može biti, na primer, sposobnost nanošenja određene štete protivniku. Veoma bitno za vojnu organizaciju, pa i za ostale organizacije, jeste da u trenutku donošenja odluke mora efikasno funkcionisati.

Kriterijum je mera postizanja zadatog cilja i on mora uvek imati kvantitativni karakter. Može se reći da svaki problem ima svoj najbolji kriterijum. U vojnom sistemu je izbor pravog kriterijuma za različite situacije odlučivanja veoma kompleksan problem zbog neodređenosti. Najčešći kriterijumi u vojnim sistemima su: vreme izvršenja zadatka, odnos očekivanih gubitaka, verovatnoća postizanja cilja, matematičko očekivanje zadatka, itd.

Modeli predstavljaju sastavni deo procesa donošenja odluke, jer se pomoću njih u celinu mogu povezati ciljevi, varijante, rezultati i kriterijumi određenog problema odlučivanja.

Sprovođenje odluke nedvosmisleno ukazuje na nedostatke donete odluke. Međutim, ako je organizacija sprovođenja odluke loša, izostaće očekivani efekti, bez obzira na to da li je odluka dobra ili loša. To je naročito karakteristično za vojne odluke u uslovima organizacije i izvršenja borbenih dejstava.

Osnovni pojmovi o veštačkoj inteligenciji

Veštačka inteligencija je naučna oblast u kojoj se izučavaju izračunavanja kojima bi se omogućila percepcija, rezonovanje i činjenje.

Ekspertni sistemi veštačke inteligencije su lanci znanja povezani međusobnim pravilima. Pretraživanje, tokom zaključivanja, odvija se u svim pravcima i grana se kroz strukturu baze znanja, nalik stablu. Sa porastom dubine pretraživanja raste i širina „stabla“.

Veštačka inteligencija može da se klasifikuje u brojne kategorije i podvrste, među kojima izdvajamo fuzzy logiku (Fuzzy Logic) i veštačke neuronske mreže.

Fuzzy logika

Fuzzy logiku predstavio je Lotfi Zadeh 1965. godine, a u kontrolu sistema uveo je E. Mamdani 1976. godine. Još tada je ovaj pristup privukao zavidnu pažnju. Iako se za jednostavnije sisteme fuzzy pristup pokazao kao veoma efikasan i jasno prilagođen ljudskom poimanju stvari, za komplikovanije sisteme se pokazao kao veoma zahtevan. Naime, za realizaciju kontrolera u tom slučaju je potrebno mnogo resursa – i vremenskih i intelektualnih.

Fuzzy logika je kao koncept mnogo prirodniji nego što se to na prvi momenat vidi. Naime, postoje situacije u kojima znanje o sistemu nije moguće reprezentovati na apsolutno precizan način. Da bi se reprezentovalo znanje o ovakvim sistemima moramo da se odreknemo klasične (binarne) logike u kojoj je nešto ili tačno ili netačno (crno ili belo) i da koristimo fuzzy logiku (sve je nijansa sive boje).

Klasična teorija skupova polazi od stava da neki element *x* iz razmatranog (univerzalnog) skupa X pripada ili ne pripada konkretnom skupu A. Slično razdvajanje postoji u klasičnoj logici: iskaz je istinit ili lažan i isključuje se treća mogućnost. Pripadnost je uslovljena karakteristikom elementa, odnosno uslovom koji element skupa X treba da ispuni da bi pripadao skupu A. Na primer, u skupu realnih brojeva, $X = R$, može se definisati skup A čiji su elementi brojevi između 170 i 190

$$A = \left\{ x \middle| x \in R, 170 \le x \le 190 \right\} \tag{1}$$

Prema ovoj definiciji, broj 169,9 ne pripada skupu A, a broj 175 pripada.

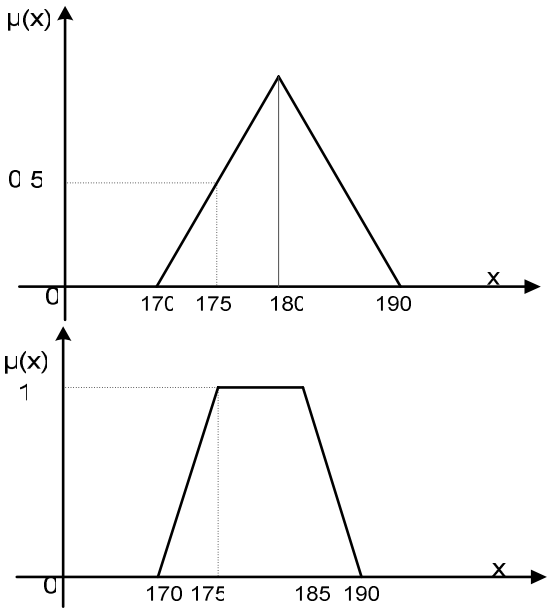
U svakodnevnom životu, posebno u govoru, često se koriste izrazi koji opisuju skupove čije su granice nejasne i rasplinute, tako da se za neke elemente univerzalnog skupa ne može jednostavno zaključiti da li ispunjavaju uslov pripadnosti konkretnom skupu. Za takve izraze se u mekom računanju (soft computing) koristi termin *lingvističke promenljive.* U mekom računjanju koristi se tolerantnost na nepreciznost, neizvesnost i delimičnu istinu da bi se postigla robustnost, niski troškovi rešavanja i bolja usklađenost modela i rešenja sa realnošću. Primeri lingvističkih promenljivih su: ljudi srednjeg rasta, velike zarade, brzi automobili, mala rastojanja, itd. Ako navedeni atributi (srednji, veliki, brzi, mala) označavaju uslove koji elementi razmatranih skupova (ljudi, zarade, automobili, rastojanja) treba da ispune da bi se odredili konkretni podskupovi (ljudi srednjeg rasta, velike zarade, brzi automobili, mala rastojanja), onda je očigledno da nema dovoljno informacija da bi se to jednoznačno obavilo [4].

Teorija fuzzy skupova kao fundamentalno nov pojam uvodi kontinualnu *funkciju pripadnosti* $\mu_A(x)$. Ova funkcija pokazuje koliko $x \in X$ ispunjava uslov pripadnosti skupu A. U klasičnoj teoriji ona može da ima jed-

nu od dve vrednosti, 1 i 0, tj. element pripada ili ne pripada skupu A. U teoriji fuzzy skupova funkcija pripadnosti može da ima bilo koju vrednost između 0 i 1. Ukoliko je $\mu_A(x)$ veće, utoliko ima više istine u tvrdnji da element x pripada skupu A, odnosno element x u većem stepenu ispunjava uslove pripadnosti skupu A. Za funkciju pripadnosti mora da važi $0 \le \mu_A(x) \le 1$, za svako $x \in A$, tj. $\mu_A : X \to [0,1]$. Formalno, fuzzy skup A se definiše kao skup uređenih parova.

$$A = \left\{ \left(x, \mu_A(x) \right) \middle| x \in X, 0 \le \mu_A(x) \le 1 \right\} \tag{2}$$

X je univerzalni skup ili skup razmatranja na kojem je definisan fuzzy skup *A* a $\mu_A(x)$ je funkcija pripadnosti elementa *(x)* skupu *A*. Svaki fuzzy skup je kompletno i jedinstveno određen svojom funkcijom pripadnosti (slika 2).



Slika 2 – Mogući oblici funkcije pripadnosti fazzy skupu

Nekoliko mogućih oblika funkcije pripadnosti fuzzy skupu ljudi srednjeg rasta prikazano je na slici 2. Na slici se vidi da čovek visine 175 cm pripada skupu ljudi srednjeg rasta sa različitim stepenom pripadnosti, zavisno od izabrane funkcije pripadnosti.

Često se univerzalni skup koristi za definisanje više fuzzy skupova kao u slučaju problema klasifikacije ljudi prema visini. Tada je uobičajeno da se funkcije pripadnosti ovih fuzzy skupova prikažu na jednoj slici.

Fuzzy logika se najčešće koristi za modelovanje složenih sistema u kojima je primenom drugih metoda veoma teško utvrditi međuzavisnosti koje postoje između pojedinih promenljivih. Modeli zasnovani na fuzzy logici sastoje se od „**If** – **Then“** („**Ako** – **Onda“**) pravila. „**If** – **Then“** pravila međusobno su povezana izrazom „**Else“** („**ili“**). Primer algoritma aproksimativnog rezonovanja predstavlja sledeći skup pravila:

If Vrednost **X** Velika
Then Vrednost **Y** Mala
Else
If Vrednost **X** Srednja
Then Vrednost **Y** Srednja
Else
If Vrednost **X** Mala
Then Vrednost **Y** Velika

Ako deo predstavlja ulazno stanje (engleski nazivi raznih autora su: *condition, antecedent part* ili *premise).* Ovde fuzzy propozicija predstavlja premisu.

Onda deo je izlazno stanje (engleski nazivi raznih autora su *conclusion ili consecvent prt).* Fuzzy propozicija u ovom delu predstavlja zaključak. On može da bude u složenom obliku i tada sistem ima više izlaznih promenljivih.

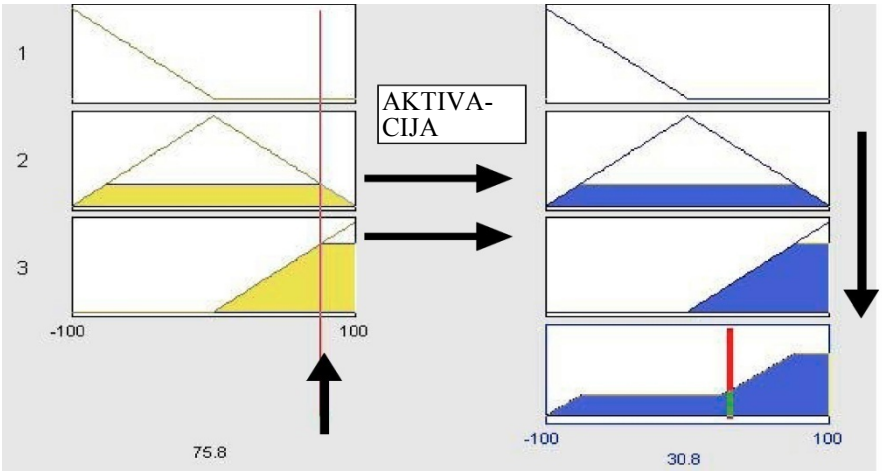
Veći broj pravila u kojim se rečima opisuje rešenje nekog problema predstavlja *bazu pravila ili ekspertska pravila.* Zbog lakšeg razumevanja pravila se pišu u pogodnom redosledu, mada on suštinski nije bitan. Pravila su povezana veznikom **Ili**, koji se često ne navodi.

Kao što vidimo iz ovih jednostavnih pravila vrednost izlazne promenljive **Y** uslovljena je vrednošću ulazne promenljive **X**. Ulazna promenljiva **X** naziva se fuzzy promenljivom. Do vrednosti fuzzy promenljive dolazi se merenjem, posmatranjem i veoma često subjektivnom procenom zasnovanom na iskustvu i intuiciji.

Aproksimativno rezonovanje je forma fuzzy logike koja sadrži skup pravila rezonovanja čije su premise fuzzy propozicije. Tvorac fuzzy logike Lotfi Zadeh tvrdi da je aproksimativno rezonovanje oblik rezonovanja koje nudi puno prirodniji okvir za ljudsko rezonovanje od tradicionalne dvovrednosne logike [7].

U realnosti najčešće su ulazne vrednosti predstavljene brojem, pri čemu se i izlazna vrednost dobija u isto tako brojčanom obliku. Sa druge strane, u fuzzy sistemu dati sistem je opisan verbalno (kvalitativno) preko produkcionih pravila. Zbog toga, najpre na određeni način konvertujemo (fazifikujemo) te brojevne vrednosti. Nakon toga, mehanizam aproksima-

tivnog rezonovanja ih obradi u fuzzy sistemu kroz faze agregacije, aktivacije i akumulacije [7], [5]. Brojčana izlazna vrednost dobije se procesom defazifikacije. Na slici 3 prikazan je proces aproksimativnog rezonovanja.



Slika 3 – Grafički prikaz procesa aproksimativnog rezonovanja

Modeli zasnovani na fuzzy logici najčešće zahtevaju više iteracija. U prvom koraku se definiše skup pravila i odgovarajuće funkcije pripadnosti. Po sagledavanju dobijenih rezultata vrši se, ukoliko je to potrebno, korekcija pojedinih pravila i/ili funkcija pripadnosti. Zatim se modifikovanim pravilima i/ili funkcijama pripadnosti model ponovo testira.

Veštačke neuronske mreže

Postoje dve kategorije neuronskih mreža: veštačke i biološke neuronske mreže. Predstavnik bioloških neuronskih mreža je nervni sistem živih bića. Veštačke neuronske mreže su po strukturi, funkciji i obradi informacija slične biološkim neuronskim mrežama, ali se radi o veštačkim tvorevinama. Neuronska mreža u računarskim naukama predstavlja veoma povezanu mrežu elemenata koji obrađuju podatke. One su sposobne da izađu na kraj sa problemima koji se tradicionalnim pristupom teško rešavaju. Veštačke neuronske mreže karakteriše paralelna i brza obrada informacija i veliki broj procesnih elemenata mreže. Dobre performanse omogućene su gustim međuvezama jednostavnih procesnih elemenata. Procesni elementi (*neuroni* ili *čvorovi*) korišćeni u neuronskoj mreži su nelinearni. Najjednostavniji neuron sabira N ulaza koji su modifikovani pripadnim težinskim faktorima i šalje rezultat kroz nelinearnost.

Jedna od važnijih osobina neuronskih mreža je njihova sposobnost da uče na ograničenom skupu primera. Kao i njen biološki uzor, veštačka neuronska mreža nije sposobna da reaguje na njoj nepoznati problem samo na osnovu prethodno definisane strukture mreže. Neuronska mreža mora da se obuči.

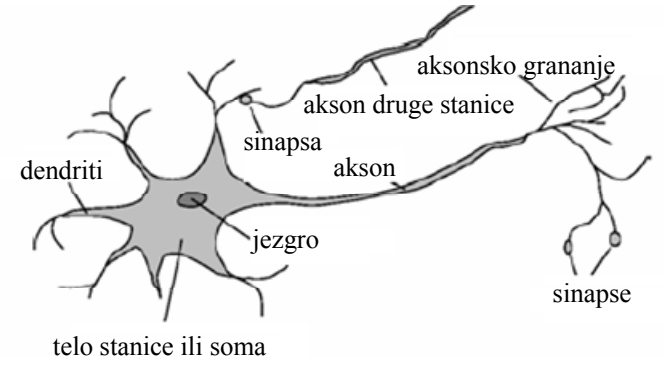
Učenje kod bioloških sistema obavlja se putem regulisanja sinaptičkih veza koje povezuju aksone i dendrite. Učenje događaja putem primera ostvaruje obučavanjem ili treningom, pri čemu se podešavaju težinski koeficijenti veza (sinapsa). Za neuronsku mrežu se kaže da je potpuno obučena, tj. trenirana kada je odgovor mreže na ulazni podatak pri obučavanju u odnosu na očekivani izlaz u željenim granicama odgovarajuće tolerancije greške.

U našem primeru veštačka neuronska mreža biće obučavana konkretnim primerima iz prakse na osnovu kojih dispečeri u jedinicama saobraćajne podrške vrše izbor vozila za izvršenje transpornog zadatka.

Neuronske mreže dobile su ovo ime zato što njihova konfiguracija podseća na mrežu nervnih ćelija koje formiraju ljudski mozak. Princip prosleđivanja impulsa od jedne do druge nervne ćelije u ljudskom nervnom sistemu iskorišćen je kao model prosleđivanja informacija kroz veštačku neuronsku mrežu. U stvari, neuronska mreža je koncipirana na modelu ljudskog mozga i nervnog sistema. Mada je sadašnje naučno saznanje o ljudskom mozgu ograničeno, poznato je dovoljno detalja u anatomskom i fiziološkom smislu da bi se razumelo osnovno funkcionisanje nervnog sistema.

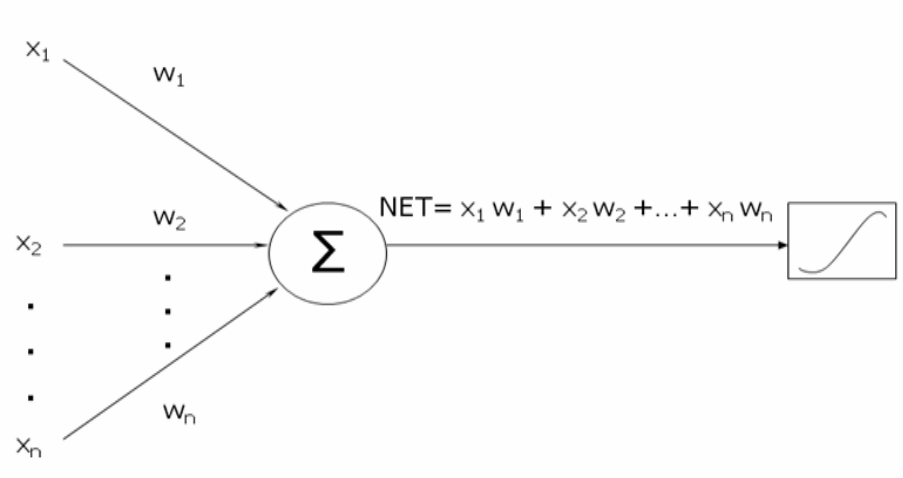
Osnovna jedinica nervog sistema je nervna ćelija ili neuron. Ona ima četiri osnovna dela: ulazni deo ćelije, telo ćelije, izlazni deo ćelije i sinapse.

Ulazni deo ćelije sadrži skup razgranatih niti nazvanih dendriti. Telo ćelije obrađuje signale koje dobija od dendrita, na taj način dobijajući izlazni impuls koji se prosleđuje na sve krajeve razgranate niti nazvane aksonom, koji predstavlja izlazni deo ćelije. Mesto gde se akson dodiruje sa dendritima neke druge ćelije naziva se sinapsa. To je mesto gde se impulsi prenose od jedne do druge nervne ćelije. (Biološki neuron prikazan je na slici 4).



Slika 4 – Prikaz biološkog neurona

Veštački neuroni, kao i biološki, imaju jednostavnu strukturu i imaju slične funkcije kao i biološki neuroni. Telo neurona naziva se čvor ili jedinica (slika 5).



Slika 5 – Prikaz veštačkog neurona

Veštački neuron je jednostavni element procesiranja, koji izvršava jednostavnu matematičku funkciju. Ulazne vrednosti u neuron prikazane su sa $x_1, x_2, ...x_n$, gde je n ukupan broj ulaza u neuron. Svaka ulazna vrednost se prvo množi težinskim koeficijentom $w_{ij},\ j = 1,2,.....n$ gde je i redni broj neurona u neuronskoj mreži. Ovako pomnožene vrednosti zatim se sabiraju i dobija se vrednost p_i [6].

$$p_i = \sum_{j=1}^{n} w_{ij} \cdot x_j \tag{3}$$

Ova se vrednost koristi kao ulaz u nelinearnu funkciju σ, koja zavisi od parametra θ – praga aktivacije. Zavisnost je najčešće takva da se θ oduzima od p_i i pri tom se njihova razlika koristi kao ulaz u nelinearnu funkciju σ. Tako se dobija vrednost izlaza i-tog neurona:

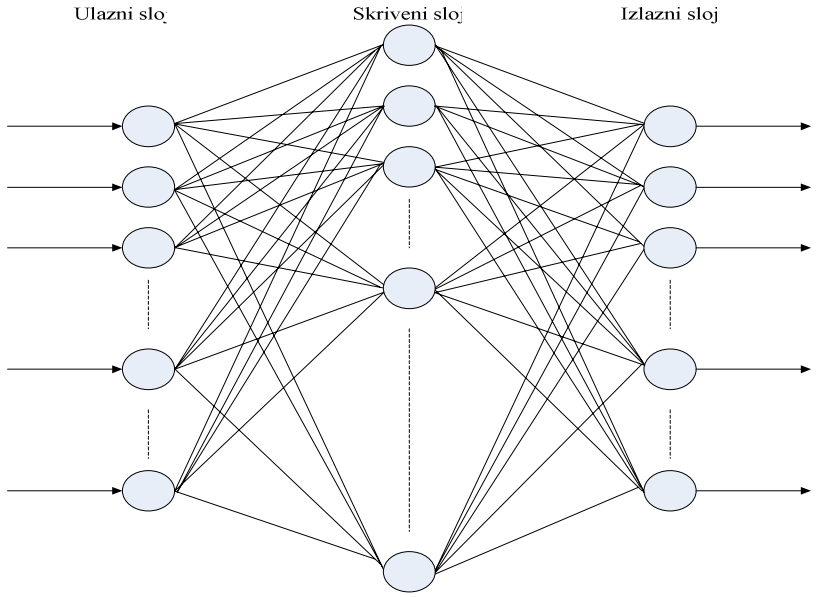
$$y_i = \sigma(p_i - \theta) = \sigma\left(\sum_{j=1}^{n} w_{ij} \cdot x_j - \theta\right) \tag{4}$$

Vrednosti težinskih faktora w_{ij}, $j = 1,2,.....n$ mogu da se menjaju, tj. prilagođavaju ulaznim i izlaznim podacima kako bi se postigla minimalna greška u odnosu na zadate podatke. Ovaj proces prilagođavanja težinskih faktora naziva se učenjem, tj. treniranjem neuronske mreže[6].

Neuronsku mrežu čine:

– arhitektura (topologija) mreže, odnosno način povezivanja neurona,
– prenosna funkcija neurona i
– zakoni učenja.

Arhitekturu veštačke neuronske mreže predstavlja specifično uređenje i povezivanje neurona u obliku mreže (slika 6). Po arhitekturi, neuronske mreže se razlikuju prema broju neuronskih slojeva [6].



Slika 6 – Višeslojna neuronska mreža

ANFIS (Adaptive Neuro Fuzzy Inference System) MODEL

ANFIS model ili fuzzy-neuronske mreže zasnivaju se se na objedinjavanju koncepata fazi logike i veštačkih neuronskih mreža.

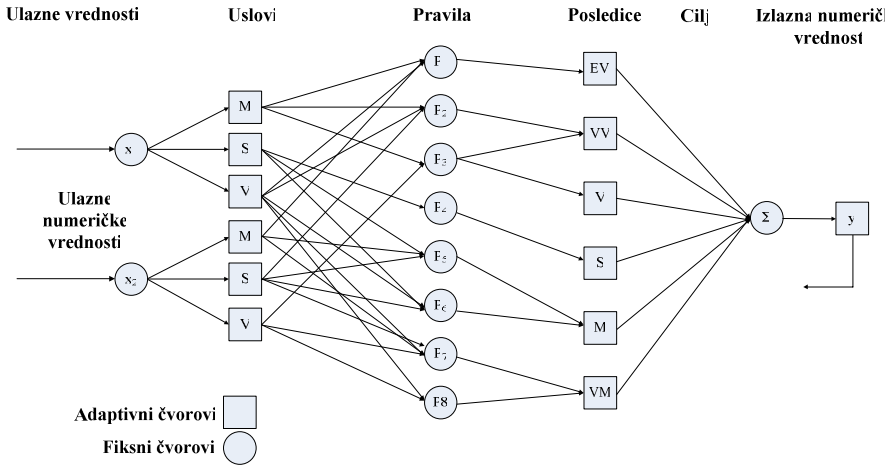
Kod ANFIS modela preuzete su najbolje karakteristike fuzzy sistema i neuronskih mreža.

U ANFIS modelu može da se eksperimentiše, tj. da se menjaju:

– ulazne i izlazne promenljive i njihove funkcije pripadnosti,
– oblik funkcija pripadnosti,
– baza pravila,
– operatori,

– vrsta defazifikacije,
– način obučavanja, tj. učenja ANFIS modela.

Na slici 7 prikazana je opšta struktura adaptivne neuro-fuzzy mreže.



Slika 7 – Opšta struktura adaptivne neuro-fuzzy mreže

Način definisanja modela umnogome zavisi od količine i raspoloživosti prethodnog znanja o procesu. Razlikuju se dva pristupa:

1. Struktura modela prethodno je određena skupom jezičkih pravila koje su formulisali eksperti. Parametri u strukturi mogu da se podešavaju korišćenjem dostupnih ulazno-izlaznih podataka o procesu (tzv. *neuro-fuzzy modelling).*

2. Ukoliko ne postoji prethodno znanje o procesu, neizraziti model se konstruiše samo na temelju ulazno-izlaznih podataka, uz očekivanje da će izvedena pravila omogućiti naknadnu interpretaciju ponašanja sistema. Koriste se tzv. *fuzzy-clustering* tehnike.

Mogućnost prikaza fuzzy modela u obliku neuronske mreže najčešće se koristi u postupcima automatskog određivanja parametara fuzzy modela na osnovu raspoloživih ulazno-izlaznih podataka. Neuro-fuzzy model je poseban oblik troslojne neuronske mreže sa prostiranjem signala unapred. Prvi sloj predstavlja ulazne varijable, srednji (skriveni) sloj fuzzy pravila, a treći sloj izlazne varijable. Fuzzy skupovi definisani su u obliku težinskih veza između čvorova. Iako neki modeli koriste više od tri sloja i fuzzy skupove prikazuju kao aktivacijske funkcije, moguće je i te modele transformisati u troslojnu arhitekturu.

U adaptivnim čvorovima vrše se podešavanja radi smanjenja greške koja se dobija na izlazu iz modela. Greška predstavlja razliku između poznatih izlaznih vrednosti i vrednosti koje se dobijaju na izlazu iz neuro-fuzzy mreže.

Signali na mreži prostiru se unapred, a greške se prostiru unazad. Time se izlazna numerička vrednost približava optimalnoj, tj. traženoj vrednosti.

Primena anfis modela u procesu donošenja odluke organa saobraćajne podrške

Da bi se zadovoljili zahtevi velikog broja korisnika saobraćajno-transportne usluge u miru i ratu, a da pri tome budu najefikasnije i prioritetno zadovoljene potrebe Vojske, mora da postoji odgovarajuća organizacijska struktura koja će sve to uspešno realizovati. Ta struktura može uspešno da funkcioniše ukoliko u svom sastavu ima upravne i izvršne organe. Na ovom principu formirani su i organi saobraćajne podrške Vojske Srbije.

Organ saobraćajne podrške prima zadatke od pretpostavljene komande. Po prijemu zadatka pristupa proučavanju i shvatanju zadatka. Nakon prikupljanja podataka neophodno je da organ saobraćajne podrške formuliše alternativna rešenja, kao i da izvrši rangiranje – vrednovanje i odbacivanje onih rešenja koji ne zadovoljavaju definisane kriterijume. Proces donošenja odluke organa saobraćajne podrške mogu da pojednostave razne metode vrednovanja.

U narednom delu rada prikazana je mogućnost primene veštačkih neuronskih mreža i fuzzy logike u procesu donošenja odluke organa saobraćajne podrške.

Dispečeri u svakoj transportnoj jedinici Vojske Srbije susreću se sa donošenjem odluka pri rešavanju planiranih i tekućih zadataka. Ova složenost zahteva podršku sistema odlučivanja.

Jedinice saobraćajne podrške svakog dana primaju veliki broj zahteva od ostalih jedinica Vojske Srbije koje žele da prevezu različite vrste tereta ka različitim odredištima. Svaki transportni zahtev je okarakterisan većim brojem atributa, među kojima su najznačajniji vrsta robe, količina robe (težina i zapremina), mesto utovara i istovara, željena vremena utovara i/ili istovara i rastojanje na koje se roba prevozi.

Pošto u voznim parkovima jedinica saobraćajne podrške figurišu različiti tipovi vozila dispečeri moraju svakodnevno da donose odluke o tome koji tip vozila je najpogodniji za izvršenje zadatka. Kriterijumi na osnovu kojih organ saobraćajne podrške vrši izbor i donosi odluku o tome koje motorno vozilo (m/v) treba uputiti na zadatak su:

– pouzdanost,
– prohodnost,
– iskorišćenje nosivosti i
– cena po tonskom kilometru.

Pouzdanost se definiše kao verovatnoća da će neki sistem izvršiti namensku funkciju u datom intervalu i pod datim uslovima. S obzirom na to da je period zanavljanja m/v u Vojsci veliki teško je i održavati pouzdanost m/v na zavidnom nivou.

Prohodnost je veoma bitna karakteristika vojnih m/v zbog toga što se teret često transportuje po alternativnim, terenskim i neprohodnim putevima, što dolazi do izražaja na terenskim vežbama i u ratnim uslovima kada korišćenje komunikacija nije omogućeno.

Pod iskorišćenjem nosivosti podrazumeva se odnos količine tereta i deklarisane nosivosti vozila izražen u procentima. Nosivost vozila koja su na upotrebi u Vojsci je različita. Problem predstavlja slaba popunjenost jedinica vozilima manje nosivosti, pa je organ saobraćajne podrške prinuđen da na zadatak upućuje vozila veće nosivosti nego što je potrebno, čime se postiže malo iskorišćenje nosivosti i dodatno se povećavaju troškovi transporta.

Cena po tonskom kilometru danas je možda i najvažniji kriterijum pri izboru m/v. Različita je za sve marke i tipove m/v koja se nalaze u Vojsci, a razlog je različita potrošnja dizel goriva, maziva, kao i amortizacija ostalih troškova.

Iskusni dispečeri najčešće imaju izgrađene kriterijume koje koriste da bi izabrali vozilo čije konstrukcione i tehničko-eksploatacione karakteristike zadovoljavaju uslove za prevoz određene vrste tereta.

U većini slučajeva ova faza procesa odlučivanja organa saobraćajne podrške svodi se na iskustvena znanja donosioca odluke. Međutim, problem se javlja kada odluku o angažovanju određenog tipa vozila treba da donese lice koje ne poseduje dovoljno iskustva. Ovaj problem može da bude rešen izradom ANFIS modela, primenom ANFIS editora koji se nalazi u sastavu MatLab-ovog Fuzzy Logic Toolbox-a.

Fazzy skupovima mogu da se kvantifikuju lingvističke, tj. kvalitativne i neprecizne informacije. Zato fazzy rezonovanje može da se koristi kao tehnika kojom se dispečerova opisna heuristička pravila prevode u automatsku strategiju upravljanja, tj. odlučivanja.

Integralni deo ANFIS modela je fuzzy sistem zaključivanja. Zamišljeno je da se fuzzy sistem (slika 8) sastoji od četiri ulazne lingvističke promenljive: **pouzdanost**, **prohodnost**, **iskorišćenje nosivosti** i **cena po tonskom kilometru** i jednom izlaznom lingvističkom promenljivom **preferencija dispečera** da određeni transportni zahtev opsluži određenim tipom vozila.

Opisani kriterijumi prikazani su u tabeli 1:

Tabela 1

Kriterijumi za vrednovanje ponuđenih m/v za izvršenje zadatka

Oznaka kriterijuma	Kriterijum	min	max	Numerical	Lingvistic
K_1	Pouzdanost		•		•
K_2	Prohodnost		•		•
K_3	Iskorišćenje nosivosti		•	•	
K_4	Cena po tonskom kilometru	•			•

Skup kriterijuma K_i (i = 1,..,4) čine dva podskupa:

– K^+ – podskup kriterijuma benefitnog tipa, što znači da je veća vrednost kriterijuma poželjnija, tj. bolja i

– K^- – podskup kriterijuma troškovnog tipa, što znači da je manja vrednost poželjnija, tj. bolja.

Kriterijum **iskorišćenje nosivosti** dat je kao numerička vrednost, a kriterijumi **pouzdanost, prohodnost** i **cena po tonskom kilometru** kao lingvistički deskriptori.

Interval poverenja ulazne promenljive **iskorišćenje nosivosti** kreće se u brojčanom intervalu [0,100], pošto se **iskorišćenje nosivosti** m/v izražava u procentima od 0% do 100%.

Ulazne promenljive **pouzdanost, prohodnost** i **cena po tonskom kilometru** predstavljene su lingvističkim deskriptorima iz skupa S = {l_1, l_2, ...,l_i}, i = 1,..,T, gde je:

– l_i – moguća vrednost lingvističke varijable čija se vrednost kreće u intervalu [0,1] i

– T – konačan broj lingvističkih deskriptora.

Svaka lingvistička varijabla definisana je kao fuzzy broj koji je definisan kao (a_i, b_i, α_i, β_i), gde a_i i b_i predstavljaju interval u kojem funkcija pripadnosti fuzzy broja ima vrednost 1.0.Vrednosti α_i i β_i predstavljaju levu i desnu distribuciju funkcije pripadnosti od vrednosti u kojoj funkcija pripadnosti fuzzy broja dostiže maksimalnu vrednost.

U našem primeru broj lingvističkih promenljivih je T = 7: „vrlo malo“ (very low – VL), „malo“ (low – L), „srednje malo“ (medium low – ML), „srednje“ (medium – M), „srednje veliko“ (medium high – MH), „veliko“ (high – H) i „vrlo veliko“ (very high – VH).

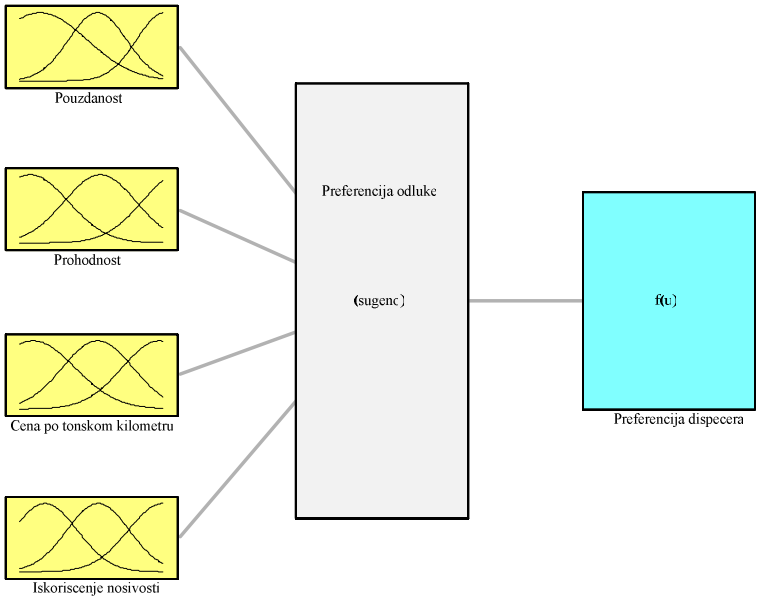
Dakle, skup S lingvističkih deskriptora predstavljen je kao:

$$S=\{l_1=VL,\ l_2=L,\ l_3=ML,\ l_4=M,\ l_5=MH,\ l_6=H,\ l_7=VH\}$$

Primenom metode za poređenje diskretnih fuzzy skupova [4] transformišu se lingvistički iskazane vrednosti kriterijuma b_i, i = 1,..,T, a zatim se vrši njihova normalizacija prema izrazu:

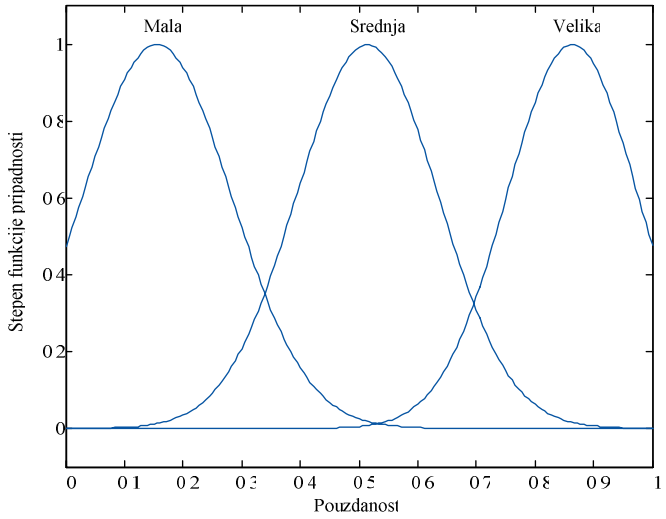
$$L_i = b_i / b_i^{max},\ b_i^{max} = \max b_i \qquad (5)$$

Vrednost izlazne promenljive **preferencija dispečera** nalazi se u intervalu [0,1].



Slika 8 – Prikaz opšteg modela fuzzy sistema

U ANFIS modelu, za svaku ulaznu promenljivu, određene su po tri lingvističke vrednosti, osim izlazne promenljive koja ima pet lingvističkih vrednosti. Ulazna promenljive imaju funkcije pripadnosti koje su označene kao: mala, srednja i velika, dok izlazna promenljiva ima funkcije pripadnosti koje su označene kao: vrlo mala, mala, srednja, velika i vrlo velika.

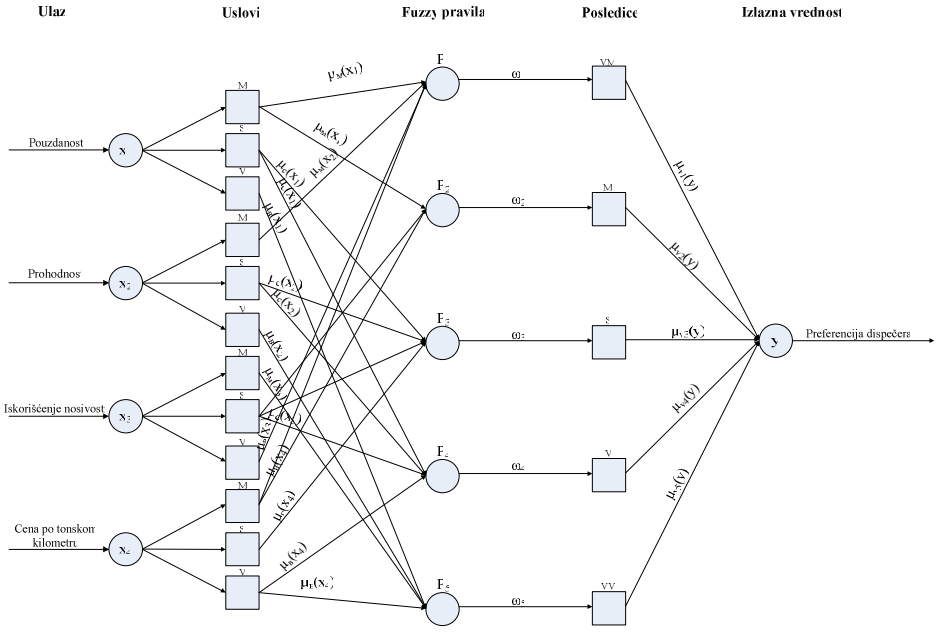


Slika 9 – Prikaz funkcije pripadnosti u obliku gausove krive

Osnovni problem sa kojim se susreće analitičar pri razvoju fuzzy sistema jeste određivanje baze fazzy pravila i parametara funkcija pripadnosti fazzy skupova koji opisuju ulazne i izlazne promenljive. U mnogim primenama fazzy sistema za upravljanje saobraćajem konačni skup pravila i izbor funkcija pripadnosti koje opisuju kategorije ulazno-izlaznih lingvističkih promenljivih dobijaju se eksperimentisanjem. U fuzzy sistemu, kao funkcije pripadnosti, izabrane su Gausove krive (slika 9), pošto se njihovim podešavanjem obezbeđuje najmanja greška na izlazu iz ANFIS modela.

Radi poboljšanja performansi razvijenog fazzy sistema kojim se vrši raspoređivanje vozila na transportne zadatke izvršeno je preslikavanje fuzzy sistema u adaptivnu neuronsku mrežu sa prostiranjem signala unapred. Osnovni cilj neuro-fuzzy modeliranja jeste smanjivanje uloge dispečera pri konstruisanju fuzzy sistema i oslanjanje na konkretne primere donetih odluka u praksi pri izboru motornog vozila za izvršenje zadatka.

Razvijeni fuzzy sistem preslikan je u petoslojnu adaptivnu neuronsku mrežu koja je prikazana na slici 10.



Slika 10 – Struktura petoslojne adaptivne mreže sa prostiranjem signala unapred

Ulaznim slojem, koji ima četiri čvora, ulazne vrednosti jednostavno prenose ka skrivenom sloju. Ulazne vrednosti adaptivne neuronske mreže su pouzdanost (x_1), prohodnost (x_2), iskorišćenje nosivosti(x_3) i cena po tonskom kilometru (x_4). Prvi čvor ulaznog sloja povezan je sa prva tri

čvora skrivenog sloja. Drugi čvor ulaznog sloja povezan je sa tri sledeća čvora prvog sloja, itd.

Čvorovi prvog sloja predstavljaju verbalne kategorije ulaznih promenljivih koje su kvantifikovane fuzzy skupovima. Svaki čvor prvog sloja je adaptivan čvor. Pošto su fuzzy pravila izražena u obliku „Ako *uslov* Tada *posledica*“, kategorije ulaznih promenljivih koje su kvantifikovane fuzzy skupovima (koje čine uslov ili prvi deo pravila) prikazane su adaptivnim čvorovima prvog sloja.

Broj čvorova u drugom sloju jednak je broju fuzzy pravila. Svaki fiksni čvor ovog sloja računa minimalnu vrednost od četiri ulazne vrednosti. Izlazne vrednosti čvorova drugog sloja su značajnosti pravila. Na primer, izlazna vrednost prvog čvora u drugom sloju je $\omega_1 = \min \{\mu_m(x_1), \mu_m(x_2), \mu_v(x_3), \mu_n(x_4)\}$.

Treći sloj ima pet adaptivnih čvorova koji predstavljaju preferenciju dispečera („vrlo mala“, „mala“, „srednja“, „velika“ i „vrlo velika“) da određeni transportni zahtev opsluži određenim tipom vozila. Svaki čvor ovog sloja računa presek odgovarajućeg fuzzy skupa (koji predstavlja *posledicu* ili drugi deo fuzzy pravila) sa maksimalnom vrednošću ulaznih značajnosti pravila.

Jedini čvor četvrtog sloja je fiksni čvor kojim se računa izlazni rezultat fuzzy sistema. To je fuzy skup sa određenim stepenima pripadnosti mogućih vrednosti preferencije dispečera da na transportni zadatak uputi razmatrani tip vozila $\mu_m(y) = \max\{ \mu_{v1}(y), \mu_{v2}(y), \mu_{v3}(y), \mu_{v4}(y), \mu_{v5}(y)\}$. Defazifikacija se vrši u čvoru petog sloja. Izlazna vrednost „O“ je realni broj koji se nalazi u intervalu [0,1].

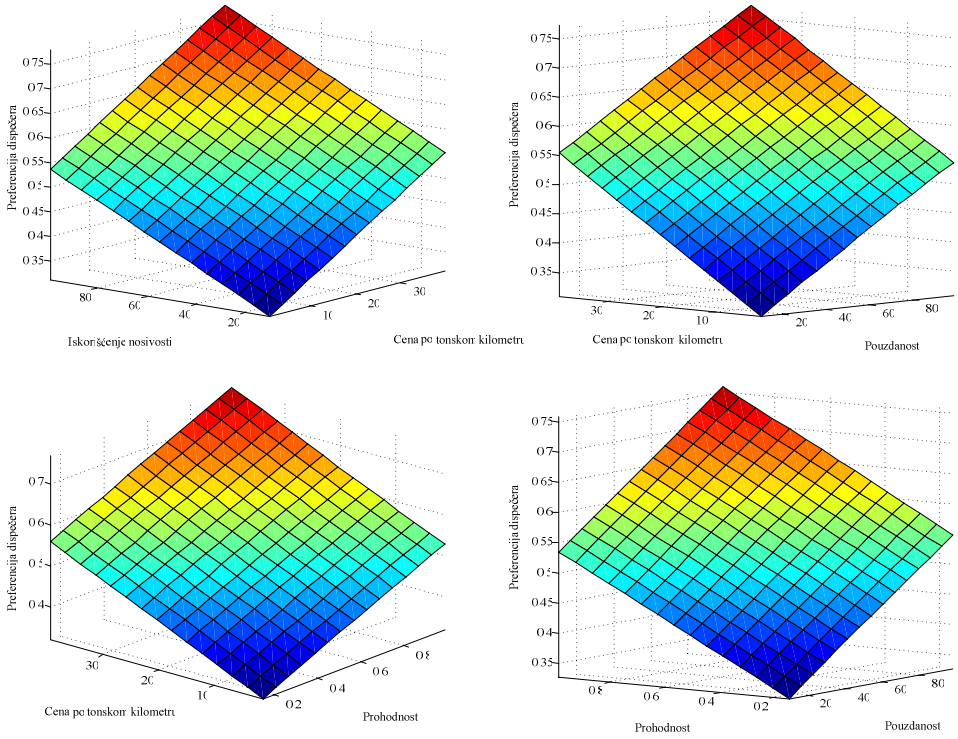
Obučavanjem neuronske mreže numeričkim primerima donetih odluka prilagođavaju se polazni oblici ulazno-izlaznih funkcija pripadnosti fazi skupova. Promena funkcija pripadnosti vrši se u adaptivnim čvorovima. Cilj obučavanja adaptivne neuronske mreže jeste reprodukcija dispečerskih odluka.

Adaptivna neuronska mreža obučavana je pomoću Backpropagation algoritma. Neuro-fuzzy modeliranje zahteva posedovanje upotrebljivih numeričkih podataka. Poverenje u dobijeni rezultat se povećava ukoliko raspolažemo dovoljno velikim reprezentativnim uzorkom koji bi se koristio za obučavanje.

Predožena neuronska mreža obučavana je na 100 primera dispečerskih odluka. Skup podataka (odluke dispečera) za obučavanje neuronske mreže dobijen je anketiranjem dispečera koji imaju radno iskustvo od najmanje 10 godina na poslovima organizacije saobraćaja u jedinicama Vojske Srbije. Podaci iz trening skupa periodično se propuštaju kroz mrežu. Dobijene vrednosti na izlazu iz mreže upoređuju se sa očekivanim podacima. Ukoliko postoji razlika između dobijenih i očekivanih podataka prave se modifikacije na vezama između neurona radi smanjenja greške, tj. razlike između trenutnog i željenog izlaza. Ulazno-izlazni skup

se ponovo predstavlja mreži zbog daljeg podešavanja težina. Neuronska mreža je obučena ako može uspešno da rešava zadatke za koje je obučavana. Nakon obučavanja ona može da generalizuje nove ulazne podatke za koje nije obučavana.

Obučavanjem neuronske mreže dobijene su vrednosti preferencije dispečera koje odgovaraju preferenciji dispečera u praksi. Greška koja se javlja na izlazu iz neuronske mreže je zanemariva, pošto iznosi 0,0003, što je približno jednako nuli. Iz grafičkog prikaza skupa mogućih rešenja opisanog ANFIS modela (slika 11) vidi se da sistem poseduje dovoljnu osetljivost, potrebnu kontinuiranost i postepenost izlaza.



Slika 11 – Grafički prikaz skupa mogućih rešenja ANFIS modela

Petoslojna adaptivna mreža testirana je na 15 primera dispečerskih odluka. S obzirom na vrstu tereta, pri obradi transportnih zahteva razmatrana su vozila nosivosti preko 2 t i to: V_1 = TAM 4500/5000, V_2 = FAP 1314, V_3 = TAM 110 T7, V_4 = TAM 150 T11, V_5 = FAP 2026 i V_6 = TAM 80 T5. U tabeli 2 prikazan je odnos dispečerskih odluka u praksi i izlaza iz ANFIS modela.

Tabela 2

Uporedni prikaz dispečerskih odluka i ANFIS modela

Broj transportnog zahteva	Izbor vozila za određeni transportni zahtev	
	Dispečer	ANFIS
1.	V_1	V_1, V_2
2.	V_5	V_5
3.	V_1	V_1, V_2
4.	V_4	V_4
5.	V_4	V_4
6.	V_5	V_5
7.	V_2	V_2
8.	V_5	V_5
9.	V_1	V_1
10.	V_1	V_1
11.	V_1	V_1, V_2
12.	V_4	V_4
13.	V_6	V_6
14.	V_6	V_6
15.	V_5	V_5

Zaključak

Razvojem ANFIS modela omogućeno je da se dispečerova strategija raspoređivanja vozila na transportne zadatke transformiše u automatsku kontrolnu strategiju. Performanse razvijenog sistema zavise od broja iskusnih dispečera, kao i sposobnosti analitičara da nakon duge komunikacije sa njima formuliše strategiju odlučivanja.

Sagledavajući performanse obučene neuronske mreže, tj. prilagođenih fuzzy sistema i dobijene rezultate, može se zaključiti da ANFIS model može da reprodukuje odluke dispečera sa velikom tačnošću, a samim tim i da raspoređuje vozila na ispunjenje transportnih zadataka kao i dispečer.

Literatura

[1] Jovanović, P.: Menadžment – teorija i praksa, Grafoslog, Beograd, 1996.

[2] Jovanović, B.: Uvod u teoriju vojnog rukovođenja, VIZ, Beograd, 1984.

[3] Stojiljković, M.: Proces donošenja odluke, VIZ, Beograd, 1975.

[4] Teodorović, D., Kikuchi, S.: Fuzzy skupovi i primene u saobraćaju i transportu, Saobraćajni fakultet, Beograd, 1994.

[5] Kandel, A.: Fuzzy expert systems“, CRC Press, 1991.

[6] MacKay, J. C. D.: Information theory, inference and learning algorithms, Cambridge University Press, 2003.

[7] Fuzzy CLIPS: http://www. iit. nrc. ca, jun 2008.

[8] Božanić, D., Pamučar, D., Vrednovanje lokacija za uspostavljanje mosnog mesta prelaska preko vodenih prepreka primenom FUZZY logike, Vojnotehnički glasnik br. 1/2010, str. 129–145, ISSN 0042-8469, Beograd.

USING FUZZY LOGIC AND NEURAL NETWORKS DURING A DECISION MAKING PROCES IN TRANSPORT

Summary:

Logistics systems in the Serbian Armed Forces are built in order to ensure and maintain combat readiness. During combat actions the structure of logistics forces, equipment and resources is organized in order to ensure success in combats and operations. Progress in information security and transport technology makes it possible for a soldier to switch mass for speed and to be sure that everything will work well. The spectrum of a full support means the support to a soldier from the supply source to the place where it will be needed. In order to obtain appropriate systems for logistics support, the systems which meet requirements and which are adjusted in accordance with environment changes and new requests are created, notably models based on the operational research methods.

The key point in the process of transport management in the Serbian Armed Forces is a decision making process. On a daily basis, the units of transport support obtain a large number of requests from other units of the Serbian Armed Forces demanding the transport of different types of load to different destinations. Each transport request is characterized with a number of attributes such as: type of goods, quantity (weight and volume), places of loading and unloading, expected time for loading and/or unloading and distance to which goods have to be transported. This paper shows a neuro-fuzzy model as a support to the decision making process. This model successfully imitates the decision making process of the transport support officers. As a result of the research, it is shown that the suggested adaptable fuzzy system, which has ability to learn, has a possibility to imitate the decision making process of transport support officers and to show the level of competence comparable with the level of their competence.

Decision making process in the military organization

In most cases, in the military organization, the decision making process is carried out in the conditions when the relevant information are not available. For the military organization, as well as for other organizations, it is very important to function efficiently in the moment of decision making.

A very important stage in the decision making process is a selection of criteria. In the military system, the selection of the proper criteria for different situations is a very complex problem. The most often criteria in the military systems are: assignment accomplishment time, expected losses, goal achievement probability, mathematical assignment expectation, etc.

Basic ideas of artificial intelligence

Expert systems of artificial intelligence are interconnected chains of knowledge. The artificial intelligence can be classified in numerous categories and subtypes, among which we emphasize Fuzzy Logic and artificial neuron networks.

Fuzzy logic

In a wider sense, fuzzy logic is a synonym for a fuzzy set theory, the theory referring to the class of objects with unclear borders and different degrees of membership. It has to be emphasized that the essence of fuzzy logic is considerably different from the essence of the traditional logic system.

This logic, based on clear and precisely fixed rules, relies on the sets theory. An element belongs or does not belong to the set, which means that sets have clearly fixed borders.

Contrary to the conventional logic, in the fuzzy logic the membership of an element in the set is not defined with precision but is expressed in, e. g., percentage. The fuzzy logic is very close to the human perception.

Artificial neuron networks

Neuron networks got their name because their configuration reminds of the neuron network which forms the human brain. The principle of transmitting impulses from one nerve cell to another in the human nervous system was used as a model of transmitting information through the artificial neuron network. The artificial neuron networks are characterized by parallel and fast data processing and numerous networks process elements. Good performances are provided by the dense interconnections of simple process elements. One of the important characteristics of the neuron networks is their ability to learn on a limited number of examples.

ANFIS (Adaptive Neuro Inference System) MODEL

The ANFIS model and fuzzy neuron networks are based on uniting the concepts of fuzzy logic and artificial neuron networks. The ANFIS model assumed the best characteristics of a fuzzy system and neuron networks.

Application of the anfis model in decision making process of the transport support authorities

The units of transport support every day get a large number of requests from other units of the Serbian Armed Forces which want to transport different types of load to different destinations. The criteria which the transport support authorities use in selection of the motor vehicle which will be sent on an assignment are: reliability, road serviceability, capacity and price per ton kilometer.

The solution of the described problem is presented in the paper by creating the ANFIS model using the ANFIS editor from the MatLab Fuzzy Logic Toolbox.

Key words: *Decision making, neuro-fuzzy aproach, ANFIS.*

Datum prijema članka: 17. 02. 2009.
Datum dostavljanja ispravki rukopisa: 26. 01. 2010.
Datum konačnog prihvatanja članka za objavljivanje: 28. 01. 2010.

UPRAVLJANJE RIZICIMA KAO PREDUSLOV INTEGRISANOG MENADŽMENT SISTEMA U ORGANIZACIJI

Karović M. *Samed,* Vojna akademija, Katedra menadžmenta u odbrani, Beograd,
Komazec M. *Nenad*, Vojna akademija, Centar za obuku studenata KoV, Beograd

UDC: 005.334

Sažetak:

Upravljanje rizikom predstavlja sastavni deo upravljačkih odluka. U uslovima kada postoji realna opasnost od gubitka ljudskih života, rušenja objekata, požara ili finansijske štete, upravljanje rizikom obezbeđuje da se ograničeni resursi (a oni su uvek ograničeni) usmere ka smanjenju opasnosti ili njihovoj potpunoj eliminaciji.

Upravljanje rizicima ne ograničava se samo na pojedinačnu zaštitu ljudi, sredstava ili životne sredine, već se kao univerzalna alatka može iskoristiti i pri izgradnji integrisanog sistema menadžmenta. U teoriji je integrisani sistem menadžmenta skoro u potpunosti definisan, dok je u praksi tek na početku razvoja i primene.

U radu se daje pristup formalizovanom sistemu menadžmenta, sa aspekta projektovanja integrisanog sistema menadžmenta (IMS) kao i okvir tog postupka i ukazuje na značaj upravljanja rizicima koji ugrožavaju opstanak organizacije.

Ključne reči: *rizik, analiza rizika, integracija*.

Uvod

Opstanak i život bilo koje organizacije zasnovan je na potrebi postojanja sistema menadžmenta, što proizilazi iz prirode i okruženja u kojem egzistira organizacija, a koje je, u suštini, takvo da nužno nameće potrebu za tzv. integrisanim menadžment sistemom (IMS). Iako je sam proces uvođenja ili prelaska na IMS najosetljiviji period u jednoj organizaciji, prednosti postojanja jednog takvog sistema su višestruke.

Integrisani menadžment sistem ne povlači za sobom nestanak već postojećih menadžment sistema u jednoj organizaciji, već se može shvatiti kao njihovo unapređenje u jedan savršeniji, jednostavniji i funkcional-

karovic.samed@gmail.com

niji menadžment sistem. U tom kontekstu se i razmatra upravljanje rizicima kao elemenat integrisanog menadžment sistema i predstavlja univerzalno oruđe za rešavanje neželjenih posledica.

Postojeći sistemi menadžmenta kvaliteta

Sa razvojem i napretkom formalizovanih (standardizovanih) menadžment sistema (kao što su menadžment sistem za kvalitet – QMS, menadžment sistem za životnu okolinu – EMS, menadžment sistem za zdravstvenu zaštitu i bezbednost na radu – OHSMS i menadžment sistem za rizik – RM), nastala je i potreba za postojanjem integrisanog menadžment sistema – IMS. On bi obuhvatao, kako formalizovane, tako i neformalizovane (finansijski, ljudski resursi, upravljački, logistički, i sl.) menadžment sisteme u jednoj organizaciji. Postojeći sistemi menadžmenta su u velikoj meri razrađeni do detalja sa postojanjem preciznih uputstava za njihovu primenu i implementaciju. Ako se tome doda i vojna organizacija koju karakteriše visoki stepen centralizacije, može se naslutiti koliko je taj segment menadžmenta značajan. U daljem tekstu se daju osnovne karakteristike određenih sistema menadžmenta bez kojih se ne može ni zamisliti egzistencija današnjih organizacija bilo koje vrste.

Menadžment sistem za kvalitet

Menadžment sistem za kvalitet (QMS/ISO 9000) opšti je nivo koji objašnjava, veoma jasnim terminima, neophodne komponente sistema za upravljanje kvalitetom (Quality Management System- QMS). Prednost ISO 9000 je što ne „*nameće*“, ne definiše kako nešto da se uradi, već samo zahteva da organizacija usmeri svoj menadžment sistem da odgovori na zahteve ISO 9001:2000 i da se fokusira na kupce i tržište. Deskriptivan je po prirodi, a takođe je primenljiv i kao baza za smanjenje rizika. Ovaj internacionalni standard takođe je primenljiv za sve tipove organizacija: proizvodne organizacije, banke, bolnice, rudnike, vladu i državne službe, vojsku, policiju, itd. Paralelno sa izdavanjem ISO 9000, Evropa je napredovala ka potpuno integrisanom tržištu, tako da je danas bar ISO 9000 potreban za plasiranje proizvoda na tržište Evropske unije. Važno je napomenuti da ISO 9000 nije standard za proizvode. To je sistemski standard i njegova osnovna uloga je da obezbedi korisne, internacionalno prihvaćene modele za primenu QMS-a. Standard ISO 9000 zahteva učešće cele organizacije i obuhvata poslovni i operativni ciklus. Organizacije koje imaju sertifikovan standard

ISO 9000 poznate su po svojoj doslednosti, pouzdanosti i dostižu reputaciju kroz primenu tog standarda. Pridržavanjem zahteva ISO 9000 šalje se snažna poruka da kompanija ozbiljno shvata kvalitet. To je dovoljno da opredeli korisnike usluga da odabere ciljanu kompaniju, a ne konkurentsku.

Menadžment sistemi za životnu okolinu

Menadžment sistemi za životnu okolinu (Enviromental Management Systems-EMS) predstavljaju globalnu strukturu koja je orijentisana na kratkoročni i dugoročni uticaj proizvoda, usluga i procesa organizacije na okruženje, odnosno na životnu okolinu. Glavni cilj je da organizacija podrži zaštitu životne sredine i sprečavanje njenog zagađenja, a da to bude u ravnoteži sa društvenim i ekonomskim potrebama. To je veoma značajno i sa vojnog aspekta, posebno u fazi izvođenja vojnih operacija sa upotrebom sredstava ratne tehnike, raznih vrsta projektila i sl.

Danas postoji velika zabrinutost za pitanje čuvanja okoline, a sve je veće zalaganje da oni koji zagađuju svoje okruženje budu i odgovorni za to. Za našu zemlju je karakteristično da u tom segmentu ne zaostaje mada kampanje koje prate aktivnosti na zaštiti životne sredine ne daju efikasne rezultate. To se može videti na svakom koraku, što je posledica i kulturne svesti ljudi.

Kao rezultat nastao je ISO 14000 koji predstavlja internacionalni standard za menadžment životnom okolinom. Zasniva se na pretpostavci da je ekonomski razvitak moguć samo u zdravom okruženju. Navedeni standardi nisu specifični ni za jednu granu industrije posebno, mogu biti jednako dobro primenjeni i na druge organizacije, državnu administraciju, a posebno na vojnu organizaciju.

Komponente EMS-a su dizajnirane da budu u skladu, koliko je to moguće, sa komponentama QMS-a. Menadžment kvalitetom ima za cilj ostvarenje zahteva kupaca, efikasnost procesa proizvodnje i kontinualno unapređivanje, dok EMS ima iste ove ciljeve, pa i više: zahtevi kupca su prošireni tako da obuhvataju zahteve vezane za zaštitu životne okoline, takođe, kontinualno unapređivanje nije podstaknuto samo očekivanjima kupca već i prioritetima i ciljevima organizacije. Standard ISO 14000 ne zamenjuje ISO 9000, niti zamenjuje propise, zakonske odredbe prema kojima organizacija treba da se upravlja, već omogućava sistem za praćenje, kontrolu i unapređivanje procesa koji se odnose na ove zahteve. Dakle, ISO 14000 je paket koji vezuje obavezne zahteve za menadžment sistem koji je sačinjen od ciljeva i programa orijentisanih na ostvarivanju obaveznih zahteva vezanih za prevenciju zagađenja i kontinualno unapređivanje zdrave životne okoline.

Menadžment rizikom

Rizik predstavlja potencijalni problem. Pojavljuje se u svim sferama rada jedne organizacije, pa je zbog toga neophodno analizirati ili, bolje rečeno, upravljati njime. Po ISO terminologiji (Risk management terminology paper – ISO/RMTP), rizik je: „Kombinacija mogućnosti (verovatnoće) nekog događaja i njegove posledice“,[1] a u nekim situacijama rizik je „devijacija od očekivanog“. Organizacije se suočavaju sa raznim oblicima rizika, tako da se javila potreba za postojanjem sistema menadžmenta koji će posebno tretirati rizike. Kasnije se, takođe, javila potreba za standardizacijom ovog sistema menadžmenta, tako da su u pojedinim zemljama, kao što su Kanada, Australija, Novi Zeland, Velika Britanija, itd., i formirani navedeni standardi.

Menadžment rizikom omogućava identifikaciju potencijalnih rizika i predviđanje njihove pojave, kao i preduzimanje adekvatnih mera za smanjivanje, ublažavanje ili eliminaciju rizika. Isto tako, tretira faktore koji mogu zaustaviti realizovanje planiranih zadataka i sprečava da dođe do „prekretnica“, naročito u negativnom smeru. Menadžment rizikom pokušava da predvidi probleme i da isplanira načine da smanji šansu njihovih izbijanja i ublaži posledice mogućih problema. Princip menadžmenta rizikom jeste da rizik treba biti dodeljen strani koja to najbolje rešava ili umanjuje. Druga veoma važna funkcija menadžmenta rizikom je što preventivno deluje na opasnosti koje nastaju kroz inovacije.

Standardi za menadžment rizikom

Nacionalni standardi za menadžment rizikom prvi put su se pojavili u Australiji i Novom Zelandu 1995. godine, zatim u Kanadi 1997. godine i u Velikoj Britaniji 2000. godine. Druge zemlje i regije (kao što je Evropa) trenutno proučavaju slične standarde, dok Međunarodna organizacija za standardizaciju (ISO) priprema listu opštih definicija vezanih za pojmove menadžmenta rizikom.

Postojeći standardi za menadžment rizikom su:

1) Australijsko–novozelandski standard za menadžment rizikom – AS/NZS 4360:2000 koji pruža opšti okvir za uspostavljanje procesa menadžmenta rizikom i iznosi proceduru koja se može primeniti da bi se uspostavila identifikacija i procenjivanje rizika, analize i praćenja rizika i komunikacija vezana za rizik.

2) Kanadski vodič za menadžment rizikom CAN/CSA-Q850 koji predstavlja više javni dokument o riziku nego uputstvo o upravljanju rizikom.

3) Britanski standard – BS 6079–3:2000, kao konvencionalan, obuhvata prošle i sadašnje prakse u upravljanju rizicima, ali ne poseduje razrađene načine za upravljanje rizicima u budućnosti.

[1)] International Standard Organization – ISO TC 223/SC.

Što se tiče ISO standarda, ideja o uspostavljanju standarda, koji će se upravo baviti rizikom, nastala je 1996. godine. Predloženo je da se standard AS/NZS 4360 prihvati kao gotovo rešenje ISO standarda za Risk management. Tokom godina, nažalost, nije se odmaklo od predložene ideje. Za sada je menadžment rizikom zvanično obuhvaćen kroz seriju standarda ISO 9000:2000 i ISO 1400:1996.

Menadžment sistem za zdravstvenu zaštitu i bezbednost na radu

Menadžment sistem za zdravstvenu zaštitu i bezbednost na radu (OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM-OHSMS) jeste metod upravljanja hazardima i rizicima vezanim za zdravstvenu zaštitu i bezbednost na radu. On može biti jednostavan ili kompleksan, može biti detaljno dokumentovan ili delimično opisan i isto tako razvijen u samoj organizaciji ili baziran na nekom modelu. Ono što ga čini sistemom je povezanost i raspoređivanje procesa da bi se stvorio ponovljiv i prepoznatljiv način upravljanja zdravstvenom zaštitom i bezbednošću na radu. Zbog finansijskih i poslovnih razloga mnoge organizacije idu ispod minimalnih zahteva regulisanih zakonom o zaštiti na radu, dok organizacija sa efektivnim programom za bezbednost i zdravstvenu zaštitu ima pozitivan povraćaj ulaganja.

Standardi primene OHSMS-a obezbeđuju određene koristi koje se mogu iskazati: smanjenjem broja povreda zaposlenih putem prevencije i kontrole opasnosti na mestu rada; smanjenjem rizika velikih nesreća – akcidenata; ispunjenjem rastućih očekivanja zaposlenih, čime se obezbeđuje visokokvalifikovana radna snaga puna entuzijazma i predanosti poslu; smanjenjem materijalnih gubitaka izazvanih nezgodama i prekidom proizvodnje; smanjenjem troškova osiguranja, kao i smanjenjem gubitaka usled odsutnosti radnika; otvaranjem mogućnosti za uspostavljanje integrisanog menadžment sistema, uključujući kvalitet, okolinu i higijenu i zdravstvenu zaštitu; porast imidža kompanije i kod zaposlenih i u okruženju.[2]

Navedeni pozitivni elementi iskazani kroz te vrednosti univerzalno važe za sve organizacije i vrednosti koje se stvaraju u tim organizacijama. Poseban segment se ispoljava u vojnoj organizaciji, koja u sebi integriše pozitivne elemente i neposredno ih implementira kroz praktičnu delatost.

Izvesno vreme postoji urgentan zahtev za prepoznatljivom specifikacijom sistema menadžmenta zdravstvenom zaštitom i bezbednošću na radu, za procenu i sertifikaciju OHSMS-a**.** Ipak, postoji nedovoljno slaganje u okviru formalnih procesa za razvijanje standarda pri britanskim standardima, evropskim standardima i internacionalnim standardima. To je dovelo do razvijanja mnogih specifikacija za menadžment sisteme, i od nacionalnih tela

[2] International Standard Organization – OHSAS 18001.

za standardizaciju i od nezavisnih grupa. Trenutno postoje dva razvijena sistema za mendžment zdravstvenom zaštitom i bezbednošću na radu – BS 8800 i OHSAS 18001, koji su zasnovani na evropskim standardima, a postoji i Australijsko-novozelandski standard AS/NZS 4801:1999.

Britanski standard BS 8800 je šema menadžmenta za zdravstvenu zaštitu i sigurnost na radu internacionalno priznata i može biti bazirana na EMS standardu ISO 14001. Sa BS 8800 organizacija može izabrati da implementira i druge menadžment sisteme kao što su ISO 9000 i ISO 14000, što znači da ISO 9001, ISO 14001 i BS 8800 mogu da koegzistiraju i da budu povezani u jedan menadžment sistem, poznat kao IMS – Integrisani Menadžment Sistem.

Za mnoge korisnike to je samo tehničko pitanje, ali za druge to je pravi problem. Organizacija koja nema sertifikovan sistem menadžmenta kvalitetom (QMS), ili sistem zaštite životne okoline (EMS), ali želi formalni sistem menadžmenta za zdravstvenu zaštitu i bezbednost na radu, koji procenjuje treća strana, nema prepoznatljivu platformu za beleženje svog uspeha u zadovoljenju zahteva. Kao rešenje i odgovor na te zahteve ponuđen je OHSAS 18001 (Occupational Health and Safety Assessment Series). Sistem menadžmenta za zdravstvenu zaštitu i bezbednost na radu OHSAS 18001 formirala je i izdala asocijacija nacionalnih tela za standardizaciju, sertifikacionih tela i specijalnih konsultanata. Zvanično, OHSAS 18001 objavljen je aprila 1999. godine i obuhvata principe iznete u BS 8800 uputstvu.[3]

Sistem menadžmenta za zdravstvenu zaštitu i bezbednost na radu AS/NZS 4801:1999 jeste specifikacija sa uputstvom za upotrebu. Ovaj standard bliže objašnjava zahteve za OHSMS kako bi omogućio organizaciji da formuliše politiku i ciljeve, uzimajući u obzir zakonske obaveze i informacije o OH&S (Occupational Health and Safety Assessment) riziku. Taj standard se odnosi na one OH&S nesreće i slične rizike koji organizacija kontroliše i čiji se uticaj očekuje. Međutim, ne daje specifične ishode primenjenih mera.

Integrisani sistem menadžmenta

Najnoviji koncepti koje organizacije otkrivaju su: kontinualno unapređivanje, samoocenjivanje, zadržavanje kupaca i obraćanje pažnje na ono što kupci cene. Međutim, ne treba odbacivati stare metode koje se mogu koristiti ponovo. Svi koncepti su važne komponente sistema koji se naziva *Integrisani Menadžment Sistem – IMS*.

Integrisanje znači kombinovanje, postavljanje internih menadžment sistema u jedan sistem, ali ne kao odvojene komponente. Da bi ovi sistemi bili integralni deo menadžment sistema kompanije, treba da postoje kompaktne veze između procesa.[4]

[3] www.riskinfo.com
[4] www.riskreports.com

Kada se govori o sistemu prvenstveno se misli na povezanost između komponenata da bi se postigao postavljeni cilj. Te komponente obuhvataju organizaciju, resurse i procese. Takođe su i ljudi, oprema i kultura deo sistema, kao i politika i praksa.

Integrisani Menadžment Sistem – IMS integriše sve komponente poslovanja u koherentni sistem, da bi se omogućilo ostvarenje njegove svrhe i misije. Sve komponente treba da formiraju celinu za koju postoje određeni razlozi. To su:

1. Smanjenje ponavljanja, a ujedno i troškova.
2. Smanjenje rizika, povećanje profitabilnosti.
3. Uravnoteženje problematičnih ciljeva.
4. Eliminisanje problematične odgovornosti i odnosa.
5. Pomeranje orijentacije na poslovne ciljeve.
6. Formalizacija neformalizovanih sistema.
7. Harmonizacija i optimizacija prakse.
8. Poboljšavanje komunikacije unutar organizacije i sa okolinom.
9. Olakšavanje obuke i razvoja.
10. Povećavanje konkurentnosti.[5]

Aktuelni trend je prvenstveno usmeren na razvoj formalizovanih modela za parcijalne menadžment sisteme, kao što su: QMS, EMS, OHSMS, RM, itd. Pored ovih u organizacijama egzistiraju i neformalizovani (nestandardizovani) parcijalni menadžment sistemi, kao što su: finansije, kadrovi, marketing, informacioni sistemi, računovodstvo, logistika. Postojanje takvih sistema stvorilo je ideju o postojanju totalnog menadžment sistema: *Totalni menadžment sistem organizacije predstavlja jedinstveni model menadžmenta koji obuhvata: opšti menadžment (neformalizovane parcijalne menadžment sisteme) i formalizovane (standardizovane) parcijalne menadžment modele.*

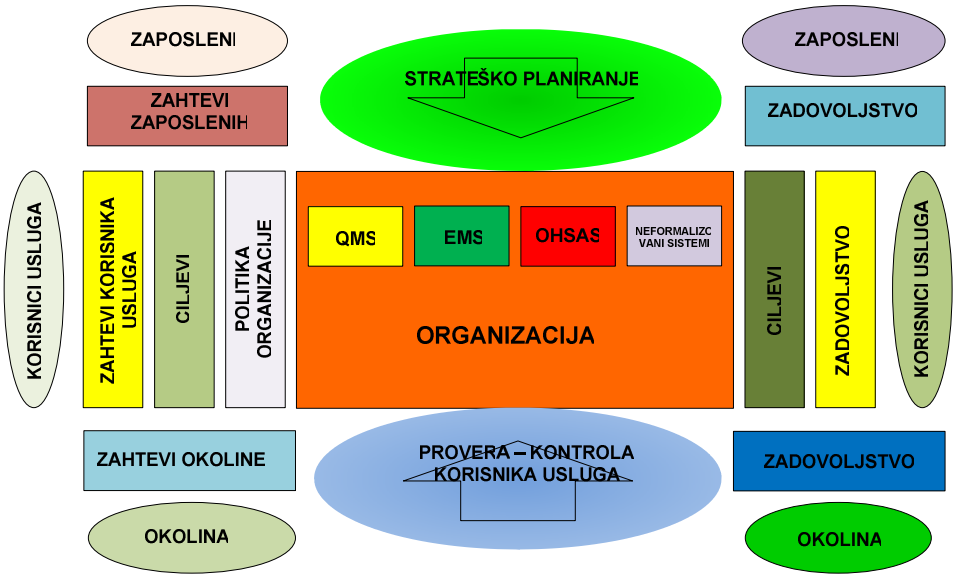
S obzirom na prisutnost analize rizika u svim sferama organizacije nametnula se ideja da upravo upravljanje rizikom objedinjuje menadžment sisteme jedne organizacije u IMS.

Integrisani menadžment sistem zasnovan na upravljanju rizikom

Polazeći od vizije i misije određene organizacije potrebno je jasno utvrditi šta organizacija radi, odnosno koje su osnovne sposobnosti bitne. Treba utvrditi šta je bitno za konkretnu organizaciju, dakle sistem vrednosti. U sledećem koraku treba identifikovati rizične operacije za ostvarenje postavljenih ciljeva. Pošto se radi o integrisanom sistemu, neophodno je identifikovanje rizika sa stanovišta kvaliteta, zaštite na radu i konačno

[5] www.iqa.org

zaštite životne sredine. Neophodno je kvantifikovati rizike kako bi se rangirali i da bi bio definisan prioritet korektivnih mera. Po utvrđivanju registra identifikovanih i kvantifikovanih rizika sprovode se mere. Na osnovu ideje za formiranje IMS preko upravljanja rizikom moguće je formirati model IMS za organizaciju upravo iz okruženja, tako da se na primeru jedne naučnoistraživačke organizacije može videti kako se za već postojeće formalizovane i neformalizovane menadžment sisteme može preći na IMS (sl. 1) upravo preko upravljanja rizikom, što u principu predstavlja najlakši i najbezbolniji način za uvođenje IMS u jednu organizaciju.



Slika 1 – Projektovani model IMS-a za naučnoistraživačku organizaciju

Analiza rizika – preduslov za primenu integrisanih sistema menadžmenta

Od pojave standarda serije ISO 9000:1987 nametnula se praksa da se sistemi menadžmenta grade samo oko tih standarda i to osloncem na jednostavan recept – „propiši šta radiš i pokaži da se držiš toga što si propisao“. Rezultat takvog pristupa je gomila papira koja je retko imala upotrebnu vrednost. Nove tehnologije, metodi rada, organizacija, menadžment i sve ono što utiče na efikasan rad jednog sistema donelo je 1994. reviziju tih standarda, a 2000. još jednu. U međuvremenu, 1997. godine objavljena je i serija ISO 14000. Dve godine kasnije pojavljuje se specifikacija OHSAS 18001, prema kojoj se i dalje nemarno odnosimo, što rezultira velikim bro-

jem slučajeva povređivanja na radu, ali i slučajeva sa smrtnim ishodom. Uzimajući ukupna dešavanja na svojoj teritoriji, 1993. Evropska unija propisuje obaveznu primenu HACCP sistema radi proizvodnje bezbedne hrane.

U vezi s procesom priključenja Evropskoj uniji zakonodavno telo Republike Srbije donelo je određene zakone:

– Zakon o javnim nabavkama uvodi zahteve za posedovanje sertifikata prema ISO 9001 ili ISO 17025;

– Zakon o zaštiti životne sredine nalaže primenu programa zaštite, analogno standardu ISO 14001. Inspekcija rada i inspekcija zaštite na radu počinju koordinirano da sprovode kontrolu primene Zakona o radu i Zakona o zaštiti na radu.

Predlog Zakona o veterinarstvu uvodi obaveznost primene HACCP sistema (slično se očekuje i za biljnu proizvodnju). Odjednom se pojavljuje potreba da organizacija – ako sebe smatra ozbiljnom – zadovolji niz specifičnih zakona i primeni nekoliko prilično komplikovanih sistema menadžmenta (uz izuzetak HACCP, koji važi samo za organizacije u lancu proizvodnje, prerade i distribucije hrane).

Na raspolaganju je nekoliko strategija:

– primeniti svaki sistem menadžmenta odvojeno ili jedan za drugim;

– dopuniti postojeći sisteme menadžmenta kvalitetom tako da zadovolji zahteve ostalih standarda,

– graditi jedinstven, celovit sistem menadžmenta koji istovremeno zadovoljava i zakonske zahteve i zahteve relevantnih standarda.

Prvi način je neprihvatljiv – organizacija ima jedan poslovni sistem i jednog top menadžera, pa treba da ima i jedan sistem menadžmenta. Drugi način biće moguće primeniti ako i samo ako je organizacija u potpunosti primenila procesni pristup i obezbedila da se procesi odvijaju unutar granica prihvatljivosti. Uz retke izuzetke sistem koji je prevashodno „pravljen“ radi sertifikacije ne može se dopunjavati izvan onoga što je potrebno za sertifikaciju, jer po pravilu uopšte ne odslikava procese u poslovnom sistemu.

Preostaje samo treći način, ali pod određenim uslovima. Prvi korak je da se uspostavi ispravna hijerarhija zahteva i očekivanja interesnih grupa u odnosu na koje se sistem gradi, pri čemu se uspostavlja sledeći redosled: zahtevi zakona i drugih propisa; zahtevi korisnika; potrebe preduzeća; zahtevi i potrebe društvene zajednice (okruženja u kojem organizacija radi); zahtevi standarda za sisteme menadžmenta (ako nam treba sertifikat).

Drugi korak je da se odabere pravi metod rada na projektu, koji uključuje, redom: stručna i naučna znanja; tehničke standarde i propise; dobru proizvođačku praksu (pravila „branše); logiku konkretnog posla (zanat).

Kao što se vidi, u prvom koraku odgovara se na pitanje zašto se nešto radi i pri tome standardi za sisteme menadžmenta nisu na prvom mestu.

U drugom koraku treba odgovoriti kako se radi, a tu npr.: standard ISO 9001 nije od pomoći.

Jedan takav sistem prikazan je na slici 2, gde standardi ISO 14004 i ISO 9004 ukazuju na to da sertifikacija ne sme biti u prvom planu. Prvo treba uspostaviti dobar sistem, jer ako on postoji i zadovoljava potrebe interesnih strana lako ga je sertifikovati.

Pri stvaranju ovakvog sistema treba poći od identifikacije onoga što je zajedničko za sve zakone i standarde, a tu se na makronivou odmah uočavaju četiri komponente: projektovanje/identifikacija procesa; analiza rizika; dokumentacija; obuka.

Sva četiri elementa čvrsto su međusobno povezana i uslovljena. Na primer, način odvijanja procesa dovodi do pojave određenih rizika; obrnuto – zbog mogućih rizika proces se mora odvijati na precizno utvrđeni način. Slično važi za veze između drugih komponenti. Upravo u ovim međuvezama krije se odgovor na često postavljano pitanje: „Koliko dokumenata treba da postoji u sistemu ISO 9000?“. Ne postoji odgovor na ovo pitanje, jer ne postoji „sistem ISO 9000“ već samo „sistem standarda ISO 9000“, ali ako se pitanje ispravno postavi: „Koliko dokumenata treba da postoji u poslovnom sistemu?“ onda je odgovor lak – onoliko koliko je potrebno da se pridruženi rizici svedu na minimum. Tamo gde rizika nema, ili tamo gde uvežbanost izvršilaca garantuje da će se procesi uvek kretati unutar prihvatljivih granica – dokument ne mora da postoji.

Međutim, pošto se prilikom pripreme za sertifikaciju prema ISO 9001 analiza rizika po pravilu ne sprovodi, opet se srećemo sa problemima preterane ili nedovoljne dokumentovanosti sistema. Kako, dakle, sprovesti analizu rizika?

Postupak sprovođenja analize rizika

Prema ISO standradu „Rizik je verovatnoća da će se neki neželjeni događaj desiti kao posledica nekog drugog događaja“.[6] Rizik se može definisati i kao verovatnoća gubitka, štete, povrede, itd., usled nekog neželjenog događaja. Dakle, može se govoriti o nizu uslovnih verovatnoća:

– verovatnoća nastanka početnog događaja (da ventil otkaže, npr. usled lošeg održavanja);

– verovatnoća nastanka neželjenog događaja (verovatnoća da baš tada pritisak vodene pare raste preko normale);

– verovatnoća da opasnost traje dovoljno dugo da dođe do pucanja cevi/kotla;

– verovatnoća da se u okolini gde se desio akcident nađu ljudi baš u trenutku pucanja cevi/kotla, itd.

Kada su u pitanju tehnički sistemi, u principu je moguće govoriti o matematičkoj verovatnoći (matematičkom očekivanju), jer se može doći do podataka koji se odnose na parametre sigurnosti funkcionisanja. Slično važi za finansijska

[6] ISO standard.

ulaganja gde postoje razrađene metode predikcije. U ostalim slučajevima govori se o verovatnoći tipa „Možda će se desiti…“ – kako proceniti verovatnoću da će bačeni opušak izazvati požar? Postoje gledišta da su verovatnoće bilo kog događaja – željenog i neželjenog – 50%: ili će se desiti ili neće, što u suštini jeste tačno ako se ne uzimaju različiti faktori koji utiču na postojanje rizika, a čijom se analizom može bliže utvrditi da li će verovatnoća rasti ili opadati.

Pored verovatnoće nastanka neželjenog događaja, analiza rizika podrazumeva i procenu posledica, pri čemu se razmatraju posledice po ljude i domaće životinje, životnu sredinu, imovinu (pokretnu i nepokretnu) i finansije. Sam postupak analize rizika je poznat i detaljno dokumentovan u stručnoj literaturi i podzakonskim aktima, npr. u Pravilniku o proceni rizika na radnim mestima i u radnoj okolini ili Pravilniku o metodologiji za procenu opasnosti od hemijskog udesa i od zagađivanja životne sredine, merama pripreme i merama za otklanjanje posledica. I u pomenutim pravilnicima procedure su definisane načelno, što otvara prostor svakoj organizaciji da definiše procenu rizika, uzimajući u obzir svoje specifičnosti, ali uz poštovanje opšteprihvaćenih metoda za analizu rizika.

Opšti postupak analize rizika sastoji se od sledećih faza:

– I FAZA: priprema kataloga proizvoda i usluga i identifikacija koji od njih eventualno imaju svojstvo opasnih ili otrovnih materija (konsultovati objavljene pravilnike o razvrstavanju) ili mogu izazvati neželjenu situaciju, npr. nezadovoljstvo korisnika, povredu ili smrt pacijenta, itd.;

– II FAZA: analiza procesa u organizaciji (identifikacija aktivnosti, ulaza, izlaza, vlasnika procesa, postojećih pravila prema kojima se ti procesi odvijaju i resursa koji u njima učestvuju).

Prioriteti i stepen razrade zavise od faktora koji učestvuju u tim procesima, kao na primer:

1. Sigurno prvo treba preduzeti mere za bezbedno skladištenje opasnih materija, dok se slavine koje cure rešavaju u drugom krugu.

2. Procena rizika koji se pridružuju pojedinim procesima i aktivnostima i to istovremeno po svim aspektima:

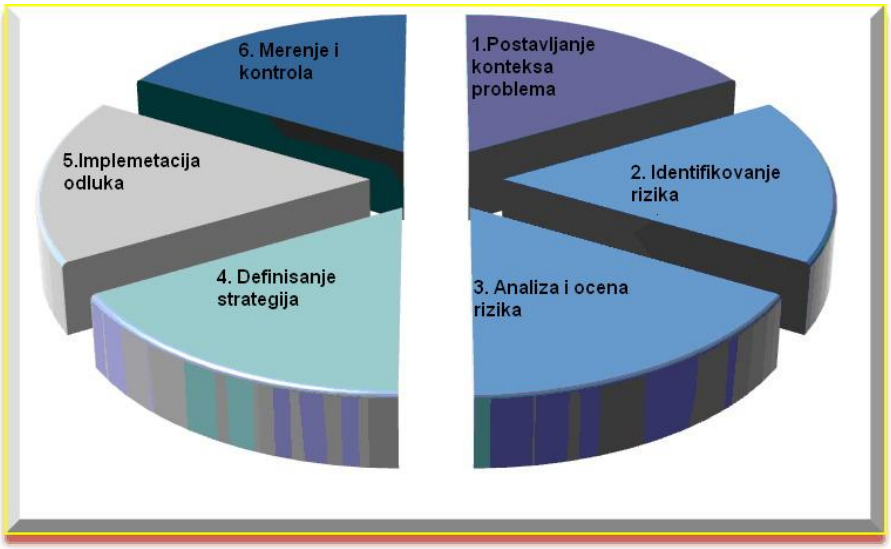
– kvalitet proizvoda/usluge,
– životna sredina,
– bezbednost ljudi,
– zaštita imovine,
– zaštita informacionih resursa.

3. Priprema plana po svim aspektima:

– za održavanje rizika u prihvatljivim granicama kada se proces normalno odvija (npr. dimnjak, kada je ispravan, ispušta xx kg/pepela u atmosferu). Ovaj plan je u stvari, specifikacija kako proces mora da teče, što znači da smo došli do dokumenta sistema menadžmenta kvalitetom prema ISO 9001. Ako je procenjeno da rizika nema – ne mora da postoji ni plan, ni dokument QMS;

– za vraćanje procesa u prihvatljive granice ako dođe do neželjene situacije ili udesa. Ovaj plan treba da uključi tehničke, organizacione i druge mere koje su u skladu sa problemom.

4. Kontinuirana kontrola sprovođenja plana, tj. nadzor nad primenom propisanih postupaka (ISO 9001). Kompletan postupak analize rizika po fazama ilustrovan je na slici 2.



Slika 2 – Faze upravljanja rizicima

Analizu rizika realizuje obučeni multidisciplinarni tim, sastavljen od lica koja dobro poznaju proces rada, osobine materija koje se pojavljuju u procesu, pridružene opasnosti i druge tehničke parametre, ali i teoriju organizacije preduzeća, zakone, propise i standarde. Pri sprovođenju analize rizika javlja se nemali problem vođenja zapisa – broj procesa, parametara, kategorija rizika, planova mera, tako je veliki problem i u osrednjoj organizaciji pa je neophodno pomoći se prigodnim softverskim alatima. Softver je praktično neophodan i zato što analiza mora da se završi pripremom scenarija, identifikacijom niza događaja koji su možda malo verovatni, ali ako se dese – dovode do udesa ili katastrofe, određivanjem prioriteta rizika, strategije za odgovor na rizike, itd.

Zaključak

Analiza rizika važan je segment, čija je neizbežnost dokazana svuda gde treba smanjiti neizvesnost pri donošenju važnih odluka. Kada su u pitanju standardi za sisteme menadžmenta, dobro sprovedena analiza obuhvatiće sve aspekte poslovanja i daće smernice za dokumentovanje sistema, za smanjenje uticaja na životnu sredinu i na zaposlene i to istovremeno, jer radna okolina je deo životne sredine.

Procedura sprovođenja analize rizika, subjekti analize, kao i alati koji obezbeđuju validne informacije o postojanju rizika propisani su različitim zakonskim dokumentima, što zavisi od oblasti u kojoj se vrši procena rizika.

Organizacije koje su odvojeno prihvatile sve ili neke od postojećih sistema trebalo bi da uzmu u obzir mogućnost da od tih sistema formiraju IMS. Integracija donosi mogućnost suštinskog poboljšanja poslovne efikasnosti i kvaliteta proizvoda i/ili usluga, kao i poboljšanja postupaka vezanih za životnu okolinu i zdravstvenu zaštitu i bezbednost na radu. Takođe, pomaže organizaciji da jasno definiše ciljeve i strategiju poslovanja, stimuliše inovacije i kreativnost, itd. Ipak, treba imati u vidu da, pored svih mogućnosti koje pruža IMS, proces stvaranja, održavanja i razvoja IMS nije lak. Najvažniji segment ili faktor koji utiče na formiranje IMS predstavljaju rizici u različitim sferama i života i rada.

Konačno, nikakav sistem preventivnih mera, koji se inače zahteva standardom ISO 9001, ne može se uspostaviti ako se prethodno, putem analize rizika, ne utvrdi na šta te mere treba da se odnose.

Literatura

[1] Anđelković, B.: Sistemski pristup u proučavanju radne i životne sredine sredine, Jugoslovenski naučno-stručni skup „Ergonomija 87", Zbornik radova, Kruševac, 1988., str. 95–99.

[2] Keković, Kešetović: Sistemi kriznog menadžmenta, Fakultet za bezbjednost i zaštitu, Banja Luka, 2008.

[3] „Pravilnik o metodologiji za procenu opasnosti od hemijskog udesa i od zagađivanja životne sredine, merama pripreme i merama za otklanjanje posledica, „Sl. glasnik RS", br. 60/94 i 63/94.

[4] Zakon o bezbednosti i zdravlju na radu, Službeni glasnik RS, broj 101/05.

[5] Integrated Environmental Management Systems, Implementation Guide, U. S. Environmental Protection Agency.

[6] http://www.enre. umd. edu/ctrs

[7] http://www.seas. gwy.edu/~irra/index. html

[8] http://www.riskinfo. com.

[9] http://www.riskreports. com

[10] http://www.standards. com. au

[11] http://www.canada. gc. ca

[12] http://www.bsi. org. uk

[13] http://www.dnv. com. sertification/services/OHSAS18001.htm

[14] http://www.dnv. com

[15] http://www.qualitydigest. com

[16] http://www.iqa. org

[17] http://www.bulltek. com

RISK MANAGEMENT AS A PREREQUISITE OF THE INTEGRATED MANAGEMENT SYSTEM IN ORGANIZATIONS

Introduction

Building of the Integrated Management System (IMS) represents a necessity, because it incorporates the existing management systems of an organization according to the ISO standards (The International Organization for Standardization), whose aim is to satisfy managerial and organizational practical work.. The conditions are thus established and the key elements in the field of quality, ecology, security, economy, reliability, compatibility, efficacity and effectiveness are provided.

Existing systems of the quality management

Development and improvement of the formalized management systems required the need for building the Integrated Management System – IMS, which would incorporate formalized and nonformalized management systems in the given organization. This is an important point concerning risk management in an organization such as military. Hereinafter we will talk about the existing management systems based on the ISO 9001 standard.

Quality Managemet System

Quality Management System (Quality Management System – QMS/ISO 9000) is a level that defines the requirements for quality management, which represents the realization of objectives and quality improvement through the management of the activities directed towards customers and market. This is what makes the basic elements for companies to show them the guidelines for actions within the quality structure and using the appropriate quality monitoring.

Environmental Management Systems

Environmental Management System (Environmental Management System – EMS) represents the structure which is oriented towards short-term and long-term influence of products and services of the organization's process on the environment. It is based on the assumption that the economic development is possible to be kept up only within the healthy environment.

Risk Management

Risk Management provides identification of potential risks, anticipation of their occurrence and undertaking measures to prevent them. In other terms, it represents overall of the organizational norms and measures referring to the identification of risk and relation to risk.

Risk Management Standards

The Risk Management Stanardization first appeared in developed countries in the period from 1990–2000. Especially distinctive are:

1. Australian-New Zeland Risk Management Standard AS/N2S4360:2000), which defines the procedures for risk identification and evaluation,
2. Canadian Risk Management Guidebook (CAN/CSA-Q850), which is at the same time the public document about risk and risk management and
3. British Standard (BS6079–3:2000) includes past and current knowledge on risk management.

The current condition of risk management in our country incorporates the series of standards ISO 9000:2000, ISO 1400:1996, because the harmonizing with the standards ISO 31000 has not been carried out.

Occupational and Health Safety Management System

Occupational and Health Safety Management System (OHSMS) represents the request for hazards and risk management in the field of occupational and health safety.

The standards of the OHSMS application are useful for reduction of work-connected injuries, prevention and reduction of danger at wok, etc.

Integrated management system

The Integrated Management System (IMS) incorporates all business components in a synchronized system, thus realizing the mission and vision of an organization.

The current trend is directed to the development of formalized models for partial management systems.

Integrated Management System based on Risk Management

The work of an organization, i. e. its purpose, is defined as the mission of a particular organization. In these terms, the risk operations for achieving objectives are defined, e. g. using the model for the creation of IMS Risk Management. This is the easiest and the least painful method of introducing the IMS in an organization.

Risk analysis – prerequisite for the integrated management system application

After ISO 9000:1989 series standard had appeared, practice imposed management systems relying, basically, on the concept 'stipulate what you do and show that you hold on to what you have stipulated'. This did not produce good results, so year 2000 saw the revision, which resulted in a great number of particular standards.

Procedure of carrying out risk analysis

Except for the evaluation of occurrence probability, risk analysis includes evaluation of the consequences on human and material resources, environment and finance. The risk analysis procedure itself is known and documented in the professional literature and legal documents.

The risk analysis is carried out by trained multidisciplinary teams familiar with the work process and technical parameters.

Conclusion

The Integrated Risk Management System (IMS) establishes conditions for risk management and risk analysis. The defined standards in the fields significant for an organization are thus provided. Standardization is important from the aspect of defining the integrated risk management system, which provides monitoring of relevant and potential risks, and potential losses in particular.

Key words: *risk, risk analysis, integration.*

Datum prijema članka: 05. 06. 2009.

Datum dostavljanja ispravki rukopisa: 13. 10. 2009.

Datum konačnog prihvatanja članka za objavljivanje: 15. 10. 2009.

YU INFO 2010 – KONFERENCIJA O RAČUNARSKIM NAUKAMA I INFORMACIONIM TEHNOLOGIJAMA

Terzić R. *Miroslav,* Vojna akademija, Katedra vojnih elektronskih sistema, Beograd

Ovogodišnja međunarodna konferencija YU INFO 2010, 16. po redu, održana je na Kopaoniku, u hotelu „Konaci“ od 3. do 6. marta 2010. godine. Izvršni organizator bilo je Informaciono društvo Srbije, koje je, po mišljenju učesnika, nastavilo tradiciju dobre organizacije.

YU INFO predstavlja redovni godišnji sastanak domaćih i inostranih stručnjaka iz različitih oblasti informaciono-komunikacionih tehnologija (ICT) u najlepšem zimskom ambijentu Kopaonika. Učesnici konferencije imali su priliku da se kroz raznovrsne programske forme upoznaju sa iskustvima najboljih, kao i novim proizvodima, rešenjima i trendovima iz oblasti ICT-a.

Pre održavanja ovogodišnje konferencije štampan je zbornik apstrakata na 116 strana, dok je zbornik radova prikazan na CD-u. Urednici zbornika radova su profesor dr Miodrag Ivković (koji je bio i predsednik organizacionog odbora) i mr Dušan Korunović. U predgovoru zbornika konstatovano je da je za konferenciju prijavljeno 220 rada. Nakon stručnih recenzija za prezentaciju na skupu i objavljivanje u zborniku radova odabrano je 193 radova. U pisanju tih radova učestvovali su domaći i strani autori (ukupno iz šest zemalja: Srbija – 180; Slovenija – 5; BiH – 5; SAD –1; Crna Gora – 1; Hrvatska – 1), podeljeni u 10 sesija (S) i četiri poster-sesije (P): S 1.1, S1.2 i P2 - E-society; S 2.1 i P2 – Informacioni sistemi; S 3.1. i P2 – Razvoj softvera i alati; S 4.1, S 4.2 i P4 – Veštačka inteligencija; S 5.1, S 5.2. i P1 – Računarske mreže i telekomunikacije; Komponente, sistemi i inžinjering; S 7.1, S 7.2 I P3 – Primenjena informatika; S 8.1 i P4 – Zaštita podataka i pravni aspekti. Takođe, u zborniku radova nalaze se i dva rada po pozivu (prof. Dr Nikola Šerbedžija, Fraunhofer FIRST, *Kako da sačuvamo privatnost kada ne znamo šta je ugrožava;* Srđan Krčo, PhD, ERICSSON, *SmartCity: A place to live Concepts, technologies and services*).

Od 180 radova u zborniku, 20 radova ili oko 11% predstavljaju radovi pripadnika Ministarstva odbrane (MO) i Vojske Srbije (VS), koji su razvrstani u četiri sesije: Računarske mreže i telekomunikacije – 8 radova; E-society – 6 radova; Primenjena informatika – 4 rada; Zaštita podataka i pravni aspekti – 2 rada. Tih 20 radova rezultat su rada 39 autora. Najviše radova bilo je u sesiji Računarske mreže i telekomunikacije (7 radova).

terzicmiroslav@yahoo.com

Od radova pripadnika Vojske najviše radova, odnosno autora (10), bilo je iz Vojne akademije (VA), što svakako ukazuje na aktivnost VA kao obrazovno-naučne ustanove VS, ali i značaj koji istraživači u VA pridaju informacionim tehnologijama. Osim VA, radove su izlagali i pripadnici Uprave za telekomunikacije i informatiku (J6) VS i Tehničkog opitnog centra. Većina radova rezultat je timskog rada.

Tokom trajanja konferencije realizovana je radionica (Workshop) pod nazivom „Upravljanje IT projektima“ u trajanju od tri nastavna časa. Veći deo pripadnika MO i VS bio je prisutan i aktivno je učestvovao u radionici.

Ukratko, ovde je dat pregled naziva radova pripadnika MO i VS po sesijama, prema redosledu u zborniku radova, bez ulaženja u njihov sadržaj. Koautori nekih radova rade na fakultetima ili drugim institucijama van MO i VS.

Sesija Računarske mreže i telekomunikacije:

1. Suša Vladimir (Vojska Srbije):

Definisanje procesa uvođenja mreže za upravljanje telekomunikacionim sistemima,

2. Terzić Miroslav (Vojna akademija): Analiza karakteristika bluetoth tehnologije sa aspekta implementacije u sistemima C3,

3. Tubin Ivan (Vojna akademija): Primena programskog paketa „Matlab“ u analizi efikasnosti ometanja radio-veza,

4. Denda Zoran (Vojska Srbije, CKISIP): Jedno rešenje primene softvera u procesu projektovanja i održavanja računarskih mreža,

5. Pavlović Boban (Vojna akademija): Analiza karakteristika algoritama rutiranja u manet mrežama,

6. Bajčetić Jovan (Vojna akademija): Simulacija Handover procedure IEEE 802.16 standarda uz pomoć NS2 simulatora,

7. Zavodnik Gorazd (Vojna akademija): Prilog analizi bezbednosti komunikacija primenom bluetooth tehnologije,

8. Đokić Aleksandar (Vojna akademija): Višedimenzionalne trelis kodovane modulacije.

Sesija E-society:

1. Bobar Zoran (Uprava za odnose sa javnošću MO): Sistem za analizu medija primenom Bussiness to government (B2G) servisa,

2. Jovanović Aleksandar (Vojska Srbije): Informacioni sistem Centra za fizičku kulturu Vojne akademije u eternet okruženju,

3. Lalović Komlen (Generalštab Vojske Srbije): Definisanje poslovno inteligentnih struktura – izrada i korišćenje centralnog sistema podataka,

4. Sekulić Goran (Ministarstvo odbrane Republike Srbije): Komparativna analiza savremenih java web aplikacionih okvira,

5. Gredić Veselin (Tehnički opitni centar, Beograd): Razvoj sistema za upravljanje tiristorskim mostom zasnovanog na mikrokontroleru atmega128.

Sesija Primenjena informatika:

1. Jovanović Boriša (Centar za primenjenu matematiku i elektroniku): JPSEC – standardno okruženje za zaštitu slika u JPEG 2000 formatu,
2. Bujaković Dimitrije (Vojna akademija): Kepstralna analiza zvučnih signala,
3. Miljković Milan (Vojna akademija): Primer daljinskog određivanja položaja pokretnog objekta,
4. Mihić Željko (Brigada veze, Uprava za telekomunikacije i informatiku, J-6, GŠ, Vojska Srbije): Informacioni sistem za vođenje evidencije o vozilima auto voznog parka Vojne akademije,

Sesija Zaštita podataka i pravni aspekti:

1. Andrić Milenko (Vojna akademija): Analiza radarskih signala pomoću entropije,
2. Fejsov Nikola (Vojna akademija): Unapređenje alata za steganografiju.

Na konferenciji su prikazana dostignuća iz oblasti informacionih tehnologija, kao i prezentacije kompanija čije su osnovne delatnosti informacione tehnologije.

Osim predavanja i prezentacija realizovan je i društveni program kroz SAGA party i basket turnir – TEHNICOM COMPUTERS. U finalu turnira u basketu ekipa Vojne akademije pobedila je ekipu Poreske uprave i osvojila prvo mesto.

Cilj učešća pripadnika MO i VS na ovoj veoma značajnoj konferenciji potpuno je postignut, jer su, pored saopštavanja rezultata istraživanja, vođene veoma plodne diskusije u kojima su sagledani zajednički problemi, razmenjena mišljenja i iskustva, te razmatrana moguća rešenja tih problema.

Izlaganje radova na ovakvim i sličnim konferencijama, kao i razmena mišljenja i iskustava sa naučnim radnicima iz drugih naučnih i obrazovnih institucija svakako ima pozitivan uticaj na naučni i stručni nivo rada u MO i VS.

Datum prijema članka: 10. 03. 2010.

Datum konačnog prihvatanja članka za objavljivanje: 12. 03. 2010.

SAVREMENO NAORUŽANJE I VOJNA OPREMA

Vazduhoplovne snage Ujedinjenog Kraljevstva isprobavaju novu vrstu operatera bespilotnih letelica[*]

Bespilotnim letelicama Reaper upravljaju iskusni vojni piloti kao operateri. Da li će tako biti i u budućnosti?

Britanski *RAF* (*Royal Air Force*) započeo je program probne obuke nove generacije operatera bespilotnih letelica. Hipoteza koju treba da potvrdi (ili opovrgne) taj eksperimentalni programom glasi: da bi operater uspešno upravljao bespilotnom letelicom dovoljno je da razmišljanja na vazduhoplovni način (da poseduje privatnu pilotsku licencu i sl.), ali ne mora da ima iskustvo neposrednog pilotiranja krilatim borbenim platformama.

Program obuke kreiran je za četiri osobe i izvodi se na letelicama *MQ-1 Predator*. U prvoj fazi, polaznici se obučavaju kako da upravljaju letelicom i izvršavaju namenske zadatke, a u sledećoj, složenijoj fazi obuke, te novostečene veštine primeniće u realističnom ambijentu, i to bi se realizovalo tokom druge polovine 2010. godine. Iskustva i pouke stečene tokom

[*] Prema podacima iz „Jane's Defence Weekly", Volume 47, Issue 11, 17 March 2010.

ovog eksperimentalnog programa koristiće se u razvoju i projektovanju novih letećih platformi na daljinsko upravljanje. Starešina *RAF-a*, koji je zadužen da prati obuku i prikuplja iskustva i pouke, komandant vinga Džuls Bol (*Jules Ball*) kaže: „Ne znamo kako će izgledati vazduhoplovne snage za 20 do 50 godina. Možda će u najvećem procentu biti zastupljeni avioni kojima će se daljinski pilotirati i zbog toga nam je potreban ovakav program obuke tokom koga ćemo doći do odgovora na pitanje, da li piloti koji daljinski upravljaju bespilotnim letelicama moraju da prođu kroz isti nivo provera i obuke kao i piloti za avione JSF (*Joint Strike Fighter*) i Typhoon“.

Ministarstvo odbrane Češke odabralo novu jurišnu pušku[*]

Ministarstvo odbrane Češke odlučilo je da u naoružanje čeških oružanih snaga uvede novu jurišnu pušku *CZ 805 Bren*, koju proizvodi *Ceská zbrojovka*, i za realizaciju tog posla uspešno su okončani svi neophodni pregovori.

Puška *CZ 805 Bren A-1*, kalibra 5,56 mm, sa prigušivačem, kolimatorskim nišanom *Meopta ZD-DOT* i pojačivačem slike *Meopta NV-MAG 3*

Puška CZ 805 pobedila je u javnom nadmetanju belgijskog konkurenta FN Herstal SCAR i ugovorena je kupovina 7.937 komada tog oružja, koje zadovoljava NATO standard 5,56 x 45 mm, i 397 komada CZ 805 G-1 40 mm, sa potcevnim bacačima granata, nišanskim uređajima, pomoćnim elementima i municijom. Prema izveštaju Ministarstva odbrane, ta puška se u potpunosti uklapa u projekat „Vojnik 21. veka“ i postepeno će istiskivati iz naoružanja postojeću pušku Vz. 58.

[*] Prema podacima iz „Jane's International Defence Review“, Volume 43, April 2010.

Jurišna puška CZ 805 je modularno, višenamensko, višekalibarsko oružje, koje se lako rekonfiguriše iz originalne jurišne puške u kratkocevni karabin ili dugocevnu snajpersku pušku. Njen primarni kalibar je 5,56 x 45 mm ali se može adaptirati za postojeću standardnu municiju 7,62 x 39, koju koristi Češka armija. To se postiže zamenom cevi, zatvarača, držača okvira i okvira za municiju. Puška funkcioniše na principu klipa sa preuzimanjem gasa iz cevi preko regulatora i rotirajućeg zatvarača.

Puška je prilagođena standardu MIL-STD-1913 i ima montažne šine na gornjoj, donjoj i obe bočne strane na koje se mogu montirati razni dodaci i izvršiti potrebne nadogradnje. Kundak je adaptibilan sa mogućnošću podešavanja dužine, bočnog preklapanja ili potpunog uklanjanja. Može se bezbedno koristiti i desnom i levom rukom, a regulator vatre omogućava pucanje jedinačno, kratkim rafalom od dva metka ili punima rafalom, sa teorijskom mogućnošću ispaljivanja 760 metaka u minuti. Težina prazne puške je 3,58 kg, a napunjene sa okvirom od 30 metaka – 4,265 kilograma.

Prvi *STARLite* radari dostavljeni KoV-u SAD[*]

Northrop Grumman je dostavio prva dva radara AN/ZPY-1 *STARLite* kopnenoj vojsci SAD i time započeo da ispunjava ugovor, vredan 78,5 miliona dolara, o kupovini ukupno 33 *STARLite* radarska sistema, koji treba da se isporuče do aprila 2011. godine. Planirano je da ti radari budu ugrađeni na bespilotnu letelicu (BL) KoV – *ERMP* (*Extended Range/Multi-Purpose*) i mornaričku BL – *Fire Scout*.

Planirano je da se *STARLite* radari ugrade na *ERMP*

[*] Prema podacima iz „Jane's Defence Weekly", Volume 47, Issue 7, 17 February 2010.

Dostava radara započeta je po okončanju 18-mesečnog kvalifikacionog testiranja i nezavisnih verifikacionih testiranja performansi koja je uradio Centar KoV SAD za testiranje i evaluaciju.

STARLite radar ima malu masu i namenjen je za podršku taktičkih operacija pomoću zemaljskog indikatora pokretnih ciljeva (*GMTI – ground moving target indicator*) i radara sa sintetičkom blendom (*SAR – synthetic aperture radar*), koji funkcionišu u svim vremenskim uslovima, noću i danju. Opremljen je softverskim paketom koji obezbeđuje interfejs sa komandnom zemaljskom stanicom gde se izlazni signal sa *GMTI* i *SAR* spreže sa standardnim vojnim mapama.

SAR sistemi obezbeđuju sposobnost osmatračkog pokrivanja široke teritorije (čak i u uslovima letenja iznad oblaka) slikom visoke rezolucije, sa udaljenosti većih od dosega elektrooptičkih infracrvenih senzora, dok *GMTI* mod prekriva digitalnu mapu pozicijama pokretnih ciljeva.

Priredio *Milan* Babić

POZIV I UPUTSTVO AUTORIMA O NAČINU PRIPREME ČLANKA

Uputstvo autorima o načinu pripreme članka za objavljivanje u *Vojnotehničkom glasniku* urađeno je na osnovu Akta o uređivanju naučnih časopisa, Ministarstva za nauku i tehnološki razvoj Republike Srbije, evidencioni broj 110-00-17/2009-01, od 09. 07. 2009. godine. Primena ovog Akta prvenstveno služi unapređenju kvaliteta domaćih časopisa i njihovog potpunijeg uključivanja u međunarodni sistem razmene naučnih informacija. Zasnovano je na međunarodnim standardima ISO 4, ISO 8, ISO 18, ISO 215, ISO 214, ISO 18, ISO 690, ISO 690-2, ISO 999 i ISO 5122, odnosno odgovarajućim domaćim standardima.

Vojnotehnički glasnik je naučni časopis Ministarstva odbrane Republike Srbije, koji objavljuje naučne i stručne članke, kao i tehničke informacije o savremenim sistemima naoružanja i savremenim vojnim tehnologijama. Časopis prati jedinstvenu intervidovsku tehničku podršku Vojske na principu logističke sistemske podrške, oblasti osnovnih, primenjenih i razvojnih istraživanja, kao i proizvodnju i upotrebu sredstava NVO, i ostala teorijska i praktična dostignuća koja doprinose usavršavanju pripadnika Ministarstva odbrane i Vojske Srbije.

Vojnotehnički glasnik je, na osnovu analize Centra za evaluaciju u obrazovanju i nauci – CEON (http://ceon.rs/) i odluke Ministarstva za nauku i tehnološki razvoj Republike Srbije, svrstan u kategoriju naučni časopisi (M53). Usvojene liste domaćih časopisa mogu se videti na:
http://www.nauka.gov.rs/cir/index.php?option=com_content&task=view&id=930&Itemid=43

Podaci o kategorizaciji mogu se pratiti i na sajtu KOBSON-a (Konzorcijum biblioteka Srbije za objedinjenu nabavku):
http://nainfo.nb.rs/kobson.82.html ili http://nainfo.nb.rs/kategorizacija. Pristup ovoj stranici omogućen je samo sa računara koji su priključeni na internet preko Akademske računarske mreže.

Kategorizacija časopisa izvršena je prema Pravilniku o postupku i načinu vrednovanja i kvantitativnom iskazivanju naučnoistraživačkih rezultata istraživača, koji je propisao Nacionalni savet za naučni i tehnološki razvoj (Službeni glasnik RS, broj 38/2008). Detaljnije informacije mogu se pronaći na sajtu Ministarstva za nauku:
http://www.nauka.gov.rs/cir/index.php?option=com_content&task=view&id=621&Itemid=37

U skladu sa ovim pravilnikom i tabelom o vrsti i kvantifikaciji individualnih naučnoistraživačkih rezultata (u sastavu Pravilnika), objavljeni rad u *Vojnotehničkom glasniku* vrednuje se sa 1 (jednim) bodom. Časopis se prati u kontekstu Srpskog citatnog indeksa – SCindeks (baza podataka domaćih naučnih časopisa – detalji dostupni na sajtu http://scindeks.nb.rs) i podvrgnut je stalnom vrednovanju (monitoringu) u zavisnosti od uticajnosti (impakta) u samoj bazi i, dopunski, u međunarodnim (Thompson-ISI) citatnim indeksima.

Članci se dostavljaju Redakciji elektronskom poštom na adresu vojnotehnicki.glasnik@mod.gov.rs (arial, srpska latinica, veličina slova 11 pt, prored exactly).

Članak treba da sadrži sažetak sa ključnim rečima, uvod, razradu, zaključak, literaturu i rezime sa ključnim rečima na engleskom jeziku (bez numeracije naslova i podnaslova). Obim članka treba da bude do jednog autorskog tabaka (16 stranica formata A4 sa proredom single).

Obrazac za pisanje članka u elektronskoj formi može se preuzeti sa adrese www.dibid.mod.gov.rs/casopisi.php.

Naslov

Naslov treba da odražava temu članka. U interesu je časopisa i autora da se koriste reči prikladne za indeksiranje i pretraživanje. Ako takvih reči nema u naslovu, poželjno je da se pridoda i podnaslov. Naslov treba da bude preveden i na engleski jezik.

Ovi naslovi ispisuju se ispred sažetka na odgovarajućem jeziku.

Tekući naslov

Tekući naslov se ispisuje u zaglavlju svake stranice članka radi lakše identifikacije, posebno kopija članaka u elektronskom obliku. Sadrži prezime i inicijal imena autora (ako autora ima više, preostali se označavaju sa „et al.“ ili „i dr.“), naslove rada i časopisa i kolaciju (godina, volumen, sveska, početna i završna stranica). Naslovi časopisa i članka mogu se dati u skraćenom obliku.

Ime autora

Navodi se puno prezime i ime (svih) autora. Veoma je poželjno da se navedu i srednja slova autora. Prezimena i imena domaćih autora uvek se ispisuju u originalnom obliku (sa srpskim dijakritičkim znakovima), nezavisno od jezika na kojem je napisan rad.

Naziv ustanove autora (afilijacija)

Navodi se pun (zvanični) naziv i sedište ustanove u kojoj je autor zaposlen, a eventualno i naziv ustanove u kojoj je autor obavio istraživanje. U složenim organizacijama navodi se ukupna hijerarhija (na primer, Vojna akademija, Katedra vojnih elektronskih sistema, Beograd). Bar jedna organizacija u hijerarhiji mora biti pravno lice. Ako autora ima više, a neki potiču iz iste ustanove, mora se, posebnim oznakama ili na drugi način, naznačiti iz koje od navedenih ustanova potiče svaki od navedenih autora. Afilijacija se ispisuje neposredno nakon imena autora. Funkcija i zvanje autora se ne navode.

Kontakt podaci

Adresa ili e-adresa autora daje se u napomeni pri dnu prve stranice članka. Ako autora ima više, daje se samo adresa jednog, obično prvog autora.

Kategorija (tip) članka

Kategorizacija članaka obaveza je uredništva i od posebne je važnosti. Kategoriju članka mogu predlagati recenzenti i članovi uredništva, odnosno urednici rubrika, ali odgovornost za kategorizaciju snosi isključivo glavni urednik.

Članci u časopisima se razvrstavaju u sledeće kategorije:

Naučni članci:

1. originalan naučni rad (rad u kojem se iznose prethodno neobjavljivani rezultati sopstvenih istraživanja naučnim metodom);
2. pregledni rad (rad koji sadrži originalan, detaljan i kritički prikaz istraživačkog problema ili područja u kojem je autor ostvario određeni doprinos, vidljiv na osnovu autocitata);
3. kratko ili prethodno saopštenje (originalni naučni rad punog formata, ali manjeg obima ili preliminarnog karaktera);
4. naučna kritika, odnosno polemika (rasprava na određenu naučnu temu, zasnovana isključivo na naučnoj argumentaciji) i osvrti.

Izuzetno, u nekim oblastima, naučni rad u časopisu može imati oblik monografske studije, kao i kritičkog izdanja naučne građe (istorijsko-arhivske, leksikografske, bibliografske, pregleda podataka i sl.) – dotad nepoznate ili nedovoljno pristupačne za naučna istraživanja.

Radovi klasifikovani kao naučni moraju imati bar dve pozitivne recenzije.

Spisak recenzenata Vojnotehničkog glasnika može se videti na adresi www.dibid.mod.gov.rs/casopisi.php.

Ako se u časopisu objavljuju i prilozi vannaučnog karaktera, naučni članci treba da budu grupisani i jasno izdvojeni u prvom delu sveske.

Stručni članci:

1. stručni rad (prilog u kojem se nude iskustva korisna za unapređenje profesionalne prakse, ali koja nisu nužno zasnovana na naučnom metodu);
2. informativni prilog (uvodnik, komentar i sl.);
3. prikaz (knjige, računarskog programa, slučaja, naučnog događaja, i sl.).

Jezik rada

Jezik rada može biti srpski, engleski ili drugi jezik koji se koristi u međunarodnoj komunikaciji u određenoj naučnoj oblasti.

Tekst mora biti jezički i stilski doteran, sistematizovan, bez skraćenica (osim standardnih). Sve fizičke veličine moraju biti izražene u Međunarodnom sistemu mernih jedinica – SI. Redosled obrazaca (formula) označava se rednim brojevima, sa desne strane u okruglim zagradama.

Sažetak (apstrakt) i rezime

Sažetak (apstrakt) jeste kratak informativan prikaz sadržaja članka koji čitaocu omogućava da brzo i tačno oceni njegovu relevantnost. U interesu je uredništava i autora da sažetak sadrži termine koji se često koriste za indeksiranje i pretragu članaka. Sastavni delovi sažetka su cilj istraživanja, metodi, rezultati i zaključak. Sažetak treba da ima od 100 do 250 reči i treba da se nalazi između zaglavlja (naslov, imena autora i dr.) i ključnih reči, nakon kojih sledi tekst članka. Ako je rad napisan na srpskom jeziku poželjno je da se, pored sažetka na srpskom, daje i sažetak u proširenom obliku na engleskom jeziku – kao tzv. rezime (summary). Ovakav rezime treba da bude na kraju članka, nakon odeljka Literatura. Važno je da rezime bude u strukturiranom obliku, a njegova dužina može biti do 1/10 dužine članka (opširniji je od sažetka na srpskom jeziku). Početak ovog rezimea može biti prevedeni sažetak na srpskom jeziku (sa početka članka), a zatim treba da slede prevedeni glavni naslovi, podnaslovi i osnove zaključka članka (literatura se ne prevodi). Potrebno je da se u strukturiranom rezimeu prevede i deo teksta ispod naslova i podnaslova, vodeći računa da on bude proporcionalan njihovoj veličini, a da odražava suštinu.

Nakon rezimea na engleskom jeziku (proširenog sažetka) dodaje se njegov prevod na srpskom, da bi redakcija izvršila proveru i lekturu.

Ključne reči

Ključne reči su termini ili fraze koje adekvatno predstavljaju sadržaj članka za potrebe indeksiranja i pretraživanja. Treba ih dodeljivati oslanjajući se na neki međunarodni izvor (popis, rečnik ili tezaurus) koji je najšire prihvaćen ili unutar

date naučne oblasti. Za npr. nauku uopšte, to je lista ključnih reči Web of Science. Broj ključnih reči ne može biti veći od 10, a u interesu je uredništva i autora da učestalost njihove upotrebe bude što veća. Ključne reči daju se na jezicima na kojima postoje sažeci. U članku se pišu neposredno nakon sažetaka, odnosno rezimea.

Datum prihvatanja članka

Datum kada je uredništvo primilo članak, datum kada je uredništvo konačno prihvatilo članak za objavljivanje, kao i datumi kada su u međuvremenu dostavljene eventualne ispravke rukopisa navode se hronološkim redosledom, na stalnom mestu, po pravilu na kraju članka.

Zahvalnica

Naziv i broj projekta, odnosno naziv programa u okviru kojeg je članak nastao, kao i naziv institucije koja je finansirala projekat ili program, navodi se u posebnoj napomeni na stalnom mestu, po pravilu pri dnu prve strane članka.

Prethodne verzije rada

Ako je članak u prethodnoj verziji bio izložen na skupu u vidu usmenog saopštenja (pod istim ili sličnim naslovom), podatak o tome treba da bude naveden u posebnoj napomeni, po pravilu pri dnu prve strane članka. Rad koji je već objavljen u nekom časopisu ne može se objaviti u *Vojnotehničkom glasniku* (preštampati*),* ni pod sličnim naslovom i izmenjenom obliku.

Tabelarni i grafički prikazi

Poželjno je da naslovi svih prikaza, a po mogućstvu i tekstualni sadržaj, budu dati dvojezično, na jeziku rada i na engleskom jeziku.

Tabele se pišu na isti način kao i tekst, a označavaju se rednim brojevima sa gornje strane. Fotografije i crteži treba da budu jasni, pregledni i pogodni za reprodukciju. Crteže treba raditi u programu word ili corel. Fotografije i crteže treba postaviti na željeno mesto u tekstu.

Navođenje (citiranje) u tekstu

Način pozivanja na izvore u okviru članka mora biti jednoobrazan. U samom tekstu, u uglastim zagradama, obavezno napisati redni broj iz odeljka Literatura sa kraja članka, na mestu na kojem se vrši pozivanje, odnosno citiranje.

Napomene (fusnote)

Napomene se daju pri dnu strane na kojoj se nalazi tekst na koji se odnose. Mogu sadržati manje važne detalje, dopunska objašnjenja, naznake o korišćenim izvorima (na primer, naučnoj građi, priručnicima), ali ne mogu biti zamena za citiranu literaturu.

Lista referenci (literatura)

Citirana literatura obuhvata, po pravilu, bibliografske izvore (članke, monografije i sl.) i daje se isključivo u zasebnom odeljku članka, u vidu liste referenci. Reference se nabrajaju redosledom kojim se navode u tekstu. Reference se ne prevode na jezik rada i navode se u uglastim zagradama. Bibliografski podatak za knjigu sadrži prezime i inicijale imena autora, naziv knige, naziv izdavača, mesto i godinu izdanja. Bibliografski podatak za časopis sadrži prezime i ime

autora, naslov članka, naziv časopisa, broj i godinu izdanja, kao i broj stranice. Naslovi citiranih domaćih časopisa daju se u originalnom, punom ili skraćenom, ali nikako u prevedenom obliku. Pri navođenju internet sajta kao literature navodi se i datum korišćenja. Obavezno je pozivanje na literaturu u samom tekstu članka (takođe se navodi brojevima u uglastim zagradama). Brojevi treba da odgovaraju spisku literature koji je dat u zasebnom odeljku, pri kraju članka.

Veoma je preporučljiva upotreba punih formata referenci koje podržavaju vodeće međunarodne baze namenjene vrednovanju, kao i Srpski citatni indeks, a propisani su uputstvima:

1. APA – Publication Manual of the American Psychological Association,
2. CBE – Council of Biology Editors Manual, Scientific Style and Format,
3. Chicago – The Chicago Manual of Style,
4. Harvard – Harvard Style Manual,
5. Harvard-BS – Harvard Style Manual – British Standard,
6. MLA – Modern Language Association Handbook for Writers of Research Papers i
7. NLM – The National Library of Medicine Style Guide for Authors, Editors, and Publishers.

Takođe, prihvaćeni su i formati dati u uputstvima:

1. American Chemical Society (ACS) Style Guide i
2. American Institute of Physics (AIP) Style Manual.

Nestandardno, nepotpuno ili nedosledno navođenje literature u sistemima vrednovanja časopisa smatra se dovoljnim razlogom za osporavanje naučnog statusa časopisa.

Pored članka dostavlja se propratno pismo u kojem treba istaći o kojoj vrsti članka se radi, koji su grafički prilozi (fotografije i crteži) originalni, a koji pozajmljeni.

U propratnom pismu navode se i podaci autora: ime, srednje slovo, prezime, čin, zvanje, e-mail, adresa poslodavca (VP), kućna adresa, telefon na radnom mestu i kućni (mobilni) telefon, račun i naziv banke, SO mesta stanovanja i JMB građana.

Svi radovi podležu stručnoj recenziji, a objavljeni radovi i stručne recenzije honorišu se prema važećim propisima.

Ako je više autora članka, u propratnom pismu se navodi pojedinačni procentualni udeo radi obračuna honorara.

Adresa redakcije: Vojnotehnički glasnik, 11000 Beograd, Braće Jugovića 19.

E-mail: vojnotehnicki.glasnik@mod.gov.rs.

Odgovorni urednik
Nebojša *Gaćeša*
nebojsa.gacesa@mod.gov.rs
tel.: 011/3349-497

MEDIJA CENTAR „ODBRANA“

• Braće Jugovića 16, 11000 Beograd •
• Telefon: (011) 3201-995, vojni 23-995 •
• Telefaks: (011) 3241-009 •
• Tekući račun: 840-49849-58 • PIB: 102116082 •
• Broj potvrde o evidentiranju za PDV: 135328814 •

POZIV NA PRETPLATU ZA 2010. GODINU

Pretplaćujemo se na časopis:

br. primeraka

1. „Vojnotehnički glasnik“
Godišnja pretplata 896,00 dinara
Prilikom uplate pozvati se na broj: 122742312923054 .....

2. „Novi glasnik“
Godišnja pretplata 1.600,00 dinara
Prilikom uplate pozvati se na broj: 122742312923053 .....

3. „Vojno delo“
Godišnja pretplata 1.184,00 dinara
Prilikom uplate pozvati se na broj: 122742312923051 .....

Pretplatne cene važe do 31. 12. 2010. godine.

Broj primeraka izdanja koja se naručuju upisati u narudžbenicu, a primerak narudžbenice sa dokazom o izvršenoj uplati na gore navedeni tekući račun poslati na gore navedenu adresu.

Kupac ..... tel.: .....…….

Mesto .....

Ulica ..... br. ……...

Potpis naručioca

M. P. .....

Likovno-grafički urednik
mr *Nebojša* Kujundžić
e-mail: nebojsa.kujundzic@mod.gov.rs

Tehničko uređenje
Zvezda Jovanović

Lektor i korektor

Dobrila Miletić, profesor
e-mail: dobrila.miletic@mod.gov.rs

Prevod na engleski
Jasna Višnjić, profesor
e-mail: visnjicjasna@yahoo.com

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

623+355 / 359

VOJNOTEHNIČKI glasnik : naučni časopis Ministarstva odbrane Republike Srbije = Military technical courier : scientific periodical of the Ministry of Defence of the Republic of Serbia / odgovorni urednik Nebojša Gaćeša. - God. 1, br. 1 (1953) - Beograd (Balkanska 53) : Ministarstvo odbrane Republike Srbije, 1953- (Beograd : Vojna štamparija. - 24 cm

Dostupno i na:
http: / / scindeks.nb.rs / journaldetails.aspx?iss
n=0042-8469
Dostupno i na: http: / / dibid.mod.gov.rs. -
Tromesečno
ISSN 0042-8469 = Vojnotehnički glasnik
COBISS.SR-ID 4423938

Cena: 280,00 dinara
Tiraž: 850 primeraka

Na osnovu mišljenja Ministarstva za nauku,
tehnologiju i razvoj Republike Srbije,
broj 413-00-1201/2001-01 od 12. 9. 2001. godine,
časopis „Vojnotehnički glasnik“ je publikacija
od posebnog interesa za nauku.

UDC: Centar za vojnonaučnu dokumentaciju, informacije i bibliotekarstvo (CVNDIB)