

UNIVERZITET U BEOGRADU FAKULTET ORGANIZACIONIH NAUKA

Nastavno-naučnom veću

Predmet: Podobnost teme i kandidata Ranka Petrovića za izradu doktorske disertacije.

Odlukom 05-01 бр. 3/133-6 od 28. 09. 2022. godine, imenovani smo za članove Komisije za ocenu podobnosti teme i kandidata Ranka Petrovića za izradu doktorske disertacije i naučne zasnovanosti teme „**MODEL EDUKACIONE PLATFORME ZA ISPITIVANJE UTICAJA SATELITSKOG LINKA NA USPEŠNOST MISIJE BEZBEDNOSNO-KRITIČNIH HCP SISTEMA KOJI SE OSLANJAJU NA IOT SENZORSKE MREŽE**“

Na osnovu materijala priloženog uz Zahtev kandidata, Komisija podnosi sledeći

R E F E R A T

1. PODACI O KANDIDATU

1.1. Biografski podaci

Ranko Petrović rođen je 25.2.1985. u Beogradu. Završio je Trinaestu beogradsku gimnaziju 2004. godine. Iste godine upisuje Elektrotehnički fakultet Univerziteta u Beogradu – Odsek za telekomunikacije i informacione tehnologije, koji završava 2012. godine sa prosečnom ocenom 8.62 odbranivši diplomski rad „Digitalna forenzika multimedijalnih signala“. Master studije upisuje 2012. godine na Elektrotehničkom fakultetu – Odsek za telekomunikacije i informacione tehnologije i završava 2014. sa prosečnom ocenom 10,00, odbranivši master rad „Pregled tehnika digitalne forenzike u detekciji copy-move napada na sliku“. Doktorske studije na Fakultetu organizacionih nauka Univerziteta u Beogradu, izbornu područje Informacione tehnologije na smeru Informacioni sistemi i kvantitativni menadžment, upisao je 2016. godine. Trenutni prosek Ranka Petrovića na doktorskim studijama je 10,00.

Od 2014. Ranko Petrović je zaposlen u Vlatacom insitutu visokih tehnologija gde trenutno radi na poziciji sistem arhitekta. Aktivno je učestvovao u planiranju, dizajnu i implementaciji više međunarodnih komercijalnih projekata vezanih za kontrolu i nadzor morske i kopnene granice. Osim komercijalnih projekata, takođe radi i u sektoru za istraživanje i razvoj. Od strane Vlatacom insituta izabran je u zvanje „istraživač pripravnik“ 2015. godine.

Autor je ili koautor više radova iz oblasti informacionih tehnologija koji su objavljeni u domaćim i međunarodnim časopisima i na konferencijama. Učestvovao je u razvoju četiri tehnička rešenja, od kojih treba izdvojiti dva kategorije M81. Kandidat takođe ima i iskustvo u nastavi s obzirom da ima ulogu mentora u okviru stručne profesionalne prakse koju Vlatacom insitut za visoke tehnologije redovno organizuje za studente završnih godina tehničkih fakulteta. Tečno govori, čita i piše engleski jezik.

1.2. Stečeno naučnoistraživačko iskustvo

U nastavku će biti predstavljene naučnoistraživačke aktivnosti kandidata. One se odnose na prikaz položenih ispita i objavljene radove u časopisima i na konferencijama.

Sledi prikaz položenih predmeta na doktorskim studijama sa ocenama i ESPB bodovima:

Naziv predmeta	Ocena	ESPB
Metodologija naučno-istraživačkog rada	10 (deset)	10
Zaštita računarskih sistema – odabrana poglavlja	10 (deset)	10
Napredne biometrijske tehnologije	10 (deset)	10
Multimedijalne komunikacije – odabrana poglavlja	10 (deset)	10
Multimediji – odabrana poglavlja	10 (deset)	10
Interakcija čoveka i računara – odabrana poglavlja	10 (deset)	10
Odabrana poglavlja iz tehnika zaštite u računarskim mrežama	10 (deset)	10
Metodologija naučno-istraživačkog rada u tehničko-tehnološkim naukama	10 (deset)	10
Sistemi zaštite informacionih sistema	10 (deset)	10

Ranko Petrović je 30. septembra 2022. godine odbranio pristupni rad pod nazivom: „**MODEL EDUKACIONE PLATFORME ZA ISPITIVANJE UTICAJA SATELITSKOG LINKA NA USPEŠNOST MISIJE BEZBEDNOSNO-KRITIČNIH HCP SISTEMA KOJI SE OSLANJAJU NA IOT SENZORSKE MREŽE**“.

1.3. Spisak radova

Ranko Petrović je autor ili koautor u sledećim naučnim publikacijama:

1. Radovi objavljeni u vrhunskim naučnim časopisima međunarodnog značaja (M21):

- R. Petrović, D. Simić, D. Drajić, Z. Čiča, D. Nikolić, and M. Perić, “Designing laboratory for IoT communication infrastructure environment for remote maritime surveillance in equatorial areas based on the Gulf of Guinea field experiences,” *Sensors*, vol. 20, no. 5, Feb. 2020, doi: 10.3390/s20051349.

2. Radovi objavljeni u istaknutim naučnim časopisima međunarodnog značaja (M22):

- R. Petrović, D. Simić, Z. Čiča, D. Drajić, M. Nerandžić, D. Nikolić, “IoT OTH maritime surveillance service over satellite network in equatorial environment: Analysis, design and deployment,” *Electronics*, vol. 10, no. 17, Aug. 2021, doi: 10.3390/electronics10172070

3. Radovi objavljeni u vrhunskim časopisima nacionalnog značaja (M51)

- M. Pavlović, B. Stojanović, R. Petrović, S. Puzović, and S. Stanković, “Optimal hog cell to image ratio for robust multi-sensor face recognition systems,” *Serbian Journal of Electrical Engineering*, vol. 16, no. 3, pp. 387–403, 2019, doi: 10.2298/SJEE1903387P.
- R. Petrović and I. Reljin, “Uloga forenzike u otkrivanju zloupotrebe digitalne slike,” *Crimen - casopis za krivicne nauke*, vol. 8, no. 1, pp. 22–43, 2017

4. Radovi objavljeni u časopisima nacionalnog značaja (M52)

- N. Latinović, T. Vuković, R. Petrović, M. Pavlović, M. Kadijević, I. Popadić, M. Veinović, "Implementation challenge and analysis of thermal image degradation on R-CNN face detection," *Telfor Journal*, vol. 12, no. 2, pp. 98–103, 2020, doi: 10.5937/telfor2002098l.
 - R. Petrović, M. Pavlović, B. Stojanović, and S. Puzović, "Prepoznavanje emocija sa slika lica primenom multisenzorskih sistema," *Info M*, vol. 19, no. 70, pp. 38–45, 2019, [Online]. Available: <https://147.91.134.42/index.php/infom/article/view/2363/2331>
 - R. Petrović, "Uloga digitalne forenzike u detekciji copy-move napada na sliku," *Info M*, vol. 16, no. 61, pp. 40–49, 2017, [Online]. Available: <https://147.91.134.42/index.php/infom/article/view/2179/2151>
5. **Zbornici međunarodnih naučnih skupova – saopštenja štampana u celini (M33):**
- R. Petrović, D. Simić, S. Stanković, and M. Perić, "Man-in-the-middle attack based on ARP spoofing in IoT educational platform," *2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, 2021, pp. 307–310, doi: 10.1109/TELSIKS52058.2021.9606392
 - R. Petrović, D. Simić, and M. Perić, "IoT laboratory for supporting different types of secure communications with sensors, with the special emphasis on satellite link," *17th International Symposium on Business and Artificial Intelligence, Symorg 2020*, 2020, pp. 183–192
 - S. Puzović, R. Petrović, M. Pavlović, and S. Stanković, "Enhancement algorithms for low-light and low-contrast images," *2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–6, Mar. 2020, doi: 10.1109/INFOTEH48170.2020.9066316.
 - T. Vuković, R. Petrović, M. Pavlović, and S. Stanković, "Thermal image degradation influence on R-CNN face detection performance," *2019 27th Telecommunications Forum (TELFOR)*, pp. 1–4, Nov. 2019, doi: 10.1109/TELFOR48224.2019.8971128.
 - R. Petrović, B. Stojanović, M. Pavlović, S. Puzović, and S. Stanković, "Thermal imagery noise influence on face recognition performance," *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–5, Mar. 2019, doi: 10.1109/INFOTEH.2019.8717662.
 - M. Pavlović, B. Stojanović, R. Petrović, and S. Stanković, "Fusion of visual and thermal imagery for illumination invariant face recognition system," *14th Symposium on Neural Networks and Applications (NEUREL)*, pp. 1–5, Nov. 2018, doi: 10.1109/NEUREL.2018.8586985.
 - B. Stojanović, S. Puzović, N. Vlahović, R. Petrović, and S. Stanković, "Real-time multi-sensor infrared imagery enhancement," *14th Symposium on Neural Networks and Applications (NEUREL)*, pp. 1–6, Nov. 2018, doi: 10.1109/NEUREL.2018.8587023.
 - K. Knezević, E. Mandić, R. Petrović, and B. Stojanović, "Blur and motion blur influence on face recognition performance," *14th Symposium on Neural Networks and Applications (NEUREL)*, pp. 1–5, Nov. 2018, doi: 10.1109/NEUREL.2018.8587028.
 - M. Nerandžić, S. Trifunović, R. Petrović, B. Stojanović, and M. Perić, "Educational platform for VoIP communication legal eavesdropping," *5th International Conference on Electrical, Electronic and Computing Engineering, IcETRAN*, 2018, pp. 1190–1194
 - R. Petrović, B. Stojanović, M. Pavlović, and S. Stanković, "Thermal-to-Visible Face Recognition for Illumination Invariant Systems," *5th International Conference on Electrical, Electronic and Computing Engineering, IcETRAN*, 2018, pp. 766–771.
 - M. Pavlović, R. Petrović, B. Stojanović, and S. Stanković, "Facial expression and lighting conditions influence on face recognition performance," *5th International Conference on Electrical, Electronic and Computing Engineering, IcETRAN*, 2018, pp. 777–781.
 - A. Valjarević, H. Venter, and R. Petrović, "ISO/IEC 27043:2015 — Role and application," *2016 24th Telecommunications Forum (TELFOR)*, pp. 1–4, Nov. 2016, doi: 10.1109/TELFOR.2016.7818718.
6. **Novo tehničko rešenje primenjeno na međunarodnom nivou (kategorija M81)**

- Miroslav Perić, Predrag Milićević, Nikola Latinović, Ranko Petrović, Zoran Banjac, “Laboratorijsko okruženje za proveru performansi multigigabitskih rešenja za zaštitu saobraćaja”, Tehničko rešenje, 2018, Rukovodilac projekta: dr Miroslav Perić
 - Miljan Vučetić, Dejan Damjanov, Boško Božilović, Zdravko Popović, Ranko Petrović, “Sistem za monitoring aktivnosti u računarskoj mreži zasnovanoj na digitalnim sertifikatima i RADIUS serveru”, Tehničko rešenje, 2018, Rukovodilac projekta: dr Boško Božilović
7. **Novo tehničko rešenje u fazi realizacije (kategorija M85)**
- Ranko Petrović, Miroslav Perić, Boško Božilović, Zdravko Popović, Miljan Vučetić, “Simulator interkontinentalnog i satelitskog prenosa IP komunikacije”, Tehničko rešenje, 2018, Rukovodilac: dr Miroslav Perić
 - Lazar Josipović, Miroslav Perić, Miljan Vučetić, Zdravko Popović, Ranko Petrović, Nikola Tošić, “Primena Google Earth Pro aplikacije za vizuelizaciju FOV-a”, Tehničko rešenje, 2018, Rukovodilac: dr Miroslav Perić

2. OCENA PODOBNOSTI KANDIDATA ZA RAD NA PREDLOŽENOJ TEMI

Na osnovu pokazanih rezultata dosadašnjeg obrazovanja, naučno-istraživačkog rada i profesionalnog iskustva, zaključujemo da je kandidat Ranko Petrović kvalifikovan da samostalno radi na predloženoj temi doktorske disertacije i načini doprinose u toj oblasti.

Predložena tema disertacije je izmenjena radi usklađivanja sa problematikom u pristupnom radu koji je uspešno odbranjen. Modifikovani naziv je „**MODEL EDUKACIONE PLATFORME ZA ISPITIVANJE UTICAJA SATELITSKOG LINKA NA USPEŠNOST MISIJE BEZBEDNOSNO-KRITIČNIH IoT HCP SISTEMA**“. Tema disertacije odgovara istraživačkom radu koji je kandidat prikazao tokom doktorskih studija.

Konačno, kandidat ima ima eksplicitno iskustvo u oblasti lične prodaje i poznavanju procesa direktne prodaje, te stoga iz praktičnog iskustva može dodatno doprineti istraživačkom radu.

2.PROBLEM, PREDMET I CILJ ISTRAŽIVANJA

U dostupnoj literaturi ne postoji model edukacione platforme koji se bavi ispitivanjem uticaja mrežnih parametara satelitskog linka na uspešnost misije bezbednosno-kritičnih HCP sistema koji se oslanjaju na IoT senzorske mreže. Generalno, industrija je prijavila probleme sa dostupnim obrazovanjem za namenske sisteme, a nedostatak obrazovnih programa, edukacionih modela, platformi i laboratorija je naročito karakterističan za vojno-odbrambene i bezbednosno-kritične HCP sisteme koji se oslanjaju na IoT senzorske mreže. Takođe, simulacija ili emulacija satelitske mreže nije pokrivena drugim, dostupnim HCP i IoT laboratorijama i edukacionim platformama, s obzirom da one ciljaju standardne HCP i IoT projekte kao što su pametni gradovi, pametne kuće, pametni kampusi, pametno zdravstvo, pametna privreda, praćenje parametara sredine, upravljanje energijom, u kojima se satelitska veza jednostavno ne koristi. Kada se uzme u obzir da su eksperimentalne metode na realnom sistemu ovakvog tipa retko izvodljive, kako zbog skupih troškova iznajmljivanja satelitskog linka tako i zbog potencijalnog negativnog uticaja na korisnički saobraćaj u produkciji, onda je potreba za modelom edukacione platforme koja će biti podjednako korisna kako za arhitekte i dizajnere sistema i njegove korisnike, tako i za buduće inženjere, više nego očigledna.

Jedna od osnovnih misija bezbednosno-kritičnih IoT HCP sistema je nadzor kopnene i morske granice, kao i kontrola kritične infrastrukture. Ovakvi sistemi se često oslanjaju na prenos preko satelitskog linka. Komunikacija preko satelitskog linka ima svoje prednosti i nedostatke. Glavna prednost je mogućnost pokrivanja velikih geografskih površina zbog čega je satelitski link najčešće, a vrlo često i jedino dostupno, komunikaciono rešenje za povezivanje senzorskih mreža za kontrolu nepristupačnih graničnih područja sa komandno-kontrolnim centrom. Sa druge strane, glavna ograničenja kada je u pitanju prenos preko satelitskog linka su velika propagaciona kašnjenja, značajne varijacije u kašnjenju, gubitak paketa, nepredvidivi prekidi, zavisnost od meteoroloških faktora, kao i ograničeni propusni opseg koji, ne tako retko, treba deliti sa drugim korisnicima. Zbog svega navedenog planiranje, razvoj, projektovanje, unapređenje i rukovanje jednim takvim bezbednosno-kritičnim IoT HCP sistemom kao i uspešnost neke od njegovih misija poput tačne detekcije, identifikacije, a zatim i preciznog praćenja različitih objekata od interesa u velikoj meri zavise upravo od dostupnog satelitskog linka što može da bude krajnje problematično. Pre svega zbog deljivih, a ograničenih resursa, kako bi se izbegao negativan uticaj na korisnički saobraćaj u produkciji, ne preporučuje se upotreba realnog satelitskog linka u fazama razvoja i testiranja bezbednosno-kritičnih IoT HCP sistema ili nekih njihovih komponenti. Takođe, iznajmljivanje dodatnog satelitskog linka samo za potrebe testiranja nije ekonomski isplativo. A još manje se preporučuje korišćenje ovakvih produkcionih sistema za potrebe edukacije. Zbog toga se vrlo često, većina servisa, senzora, aktuatora i blokova za obradu koji se koriste u bezbednosno-kritičnim IoT HCP sistemima i čija se komunikacija zasniva na satelitskom linku razvija i testira gotovo isključivo u lokalnoj računarskoj mreži. Osim toga, obuka operatera koji rade na ovakvim sistemima, a čija je pravovremena, precizna i ispravna reakcija od ključnog značaja, se takođe često odvija u ograničenim okruženjima i kontrolisanim uslovima sa lokalnom računarskom mrežom. Rezultat toga su postignute znatno niže performanse u produkcijom nego u testnom okruženju. Razlog za to je što lokalna računarska mreža, za razliku od satelitskog linka, nema ograničenja u vidu propusnog opsega, velikog propagacionog kašnjenja, značajnih varijacija u kašnjenju, gubitka paketa kao i zavisnosti od meteoroloških uslova koji dovode do nepredvidivih prekida u komunikaciji. Kada se još uzme u obzir da ovakvi sistemi moraju da budu maksimalno zaštićeni, da podržavaju integritet i poverljivost podataka, zbog čega kompletna komunikacija mora da bude šifrovana, problem postaje i izraženiji, jer se uvođenjem šifrovanja i drugih vidova zaštite dodatno opterećuje i onako ograničen kapacitet satelitskog linka.

U ovakvim situacijama modelovanje, simulacija i emulacija se nameću kao objektivne i pouzdane metode koje bi pomogle u planiranju, projektovanju i ispitivanju ovakvih sistema, naročito jer su eksperimentalne metode na realnom sistemu retko izvodljive, kako zbog skupih troškova iznajmljivanja satelitskog linka tako i zbog potencijalnog negativnog uticaja na korisnički saobraćaj u produkciji. Sisteme za zaštitu bezbednosno-kritične infrastrukture po pravilu koriste obučeni, profesionalni korisnici, koji imaju za cilj ostvarenje jasno definisane misije. Pa ipak, uspešno obavljanje misije bezbednosno-kritičnih IoT HCP sistema umnogome zavisi upravo od čoveka kao verovatno najslabije karike sistema i njegovih karakteristika poput pouzdanosti, vremena odziva, prilagodljivosti promenama, sposobnosti suočavanja sa nepoznatim situacijama, kooperativnosti, stručnosti, odgovornosti i volje. U svakom slučaju, u dostupnoj literaturi ne postoji opisan model koji bi trebalo da dizajnerima i arhitektama bezbednosno-kritičnih IoT HCP sistema pruži jasan uvid u ograničenja koja sa sobom nosi satelitski link, a koja su i te kako važna za razvoj i unapređenje različitih komponenti sistema kao što su senzori, servisi, aplikacije, algoritmi i uređaji. Takođe, u dostupnoj literaturi ne postoji opisan model kojim bi trebalo da se omogući unapređenje funkcionalnosti i efikasnosti kao i optimizacija postojećeg, već implementiranog bezbednosno-kritičnog IoT HCP sistema, u odnosu na mnoga ograničenja koja pre svega sa sobom donosi satelitski link, i to kroz povećanje stepena obučenosti i iskustva korisnika sistema simulacijom i emulacijom u laboratorijskim uslovima. Osim toga, sama industrija prijavljuje probleme sa dostupnim obrazovanjem za namenske sisteme, a u dostupnoj literaturi gotovo i da nema radova koji se bave problemom edukacije u ovako specifičnim sistemima čija se komunikacija bazira na satelitskom linku. Ipak, u literaturi, pa čak i u većem broju komercijalnih rešenja postoje izdvojeni modeli, simulatori i emulatori satelitskog linka koji definišu

neke od njegovih parametara i posredno se mogu uključiti u istraživačko razvojno rešenje. Takođe, za veliki broj servisa postoji i neka vrsta metodologije koja kvantifikuje njihov kvalitet za prosečnog korisnika. Međutim, glavni nedostatak postojećih rešenja je nepostojanje sveobuhvatnog modela, koji bi za kvantifikaciju uspešnosti misije uzimao u obzir, ne samo parametre satelitskog linka koji je svakako u fokusu ove disertacije, već i parametre senzora, aktuatora, bloka za obradu podataka, kao i ulogu čoveka čiji se uticaj na sistem ogleda kroz stepen obučenosti i iskustvo. Svaka od pomenutih komponenti je predmet daljih unapređenja te je cilj formirati sveobuhvatni model koji bi mogao da kvantifikuje doprinos svakog od pomenutih parametara uspešnosti misije jednog bezbednosno-kritičnog IoT HCP sistema koji se oslanja na prenos preko satelitskog linka.

Predmet istraživanja ove doktorske disertacije je mogućnost realizacije modela edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka na uspešnost misije bezbednosno-kritičnih IoT HCP sistema. To su kiber fizički sistemi za kontrolu graničnih područja i nadzor kritične infrastrukture za koje je uobičajeno da pokrivaju ogromne geografske površine zbog čega su prinuđeni da se često oslanjaju na satelitski link kao jedini dostupan vid komunikacije. Iako ovakvi sistemi teže potpunoj automatizaciji, što je postalo naročito vidno pojavom veštačke inteligencije, čovek još uvek predstavlja centralnu, a najčešće i najkritičniju figuru u ovakvim sistemima. Zato je potrebno identifikovati njegovu ulogu kao i njegove karakteristike sa kojima on potencijalno može da utiče na uspešnost misije jednog ovakvog sistema, a koje bi mogle da se unaprede edukacijom kroz predloženi model edukacione platforme. Interaktivnost preko satelitskog linka kao najproblematičnije komponente sistema, između senzorske mreže, bloka za obradu podataka i ljudskog faktora, je nešto na šta treba obratiti posebnu pažnju i što u velikoj meri utiče na uspešnost misije nekog bezbednosno-kritičnog IoT HCP sistema, bilo da je u pitanju razvoj ili unapređenje jednog takvog sistema ili na primer tačna detekcija i identifikacija različitih objekata od interesa, a zatim i njihovo precizno praćenje. U skladu sa navedenim potrebno je ispitati da li jedan ovakav model edukacione platforme može da kroz povećanje stepena obučenosti i iskustva arhitekata ili korisnika sistema, simulacijom i emulacijom u laboratorijskim uslovima, omogući olakšan razvoj novog ili unapređenje i optimizaciju postojećeg, već implementiranog bezbednosno-kritičnog IoT HCP sistema, u odnosu na mnoga ograničenja koja pre svega sa sobom donosi satelitski link. U skladu sa navedenim predmet istraživanja u okviru ove disertacije biće i postojeći HCP i IoT edukacioni modeli, platforme i laboratorije, kao i modeli, simulatori i emulatori komunikacionog sistema.

Verifikacija primenljivosti predloženog modela biće moguća u laboratorijskom okruženju, njegovom parametrizacijom na osnovu eksperimentalnih rezultata dobijenih na realnom sistemu za nadzor obale u Gvinejskom zalivu, zbog čega će prenos različitih servisa preko realnog satelitskog linka u različitim meteorološkim uslovima u okviru pomenutog sistema biti takođe predmet istraživanja ove doktorske disertacije. Tom prilikom biće razmatrani servisi senzora sa različitim stepenom interaktivnosti: prikupljanje podataka sa radara za posmatranje iza linije horizonta, video striming sa elektro-optičkog sistema opremljenog kamerama u vidljivom i infra-crvenom delu spektra kao i merenje rastojanja do mete primenom laserskog daljinomera pomoću visoko-interaktivne aplikacije. Zbog bezbednosno-pravnih ograničenja, podaci o konkretnim lokacijama i tipovima senzora neće biti dostupni, ali će prikupljeni rezultati merenja na telekomunikacionom sistemu moći da se koriste za istraživanje.

Na kraju, predmet istraživanja će biti i mogućnost generalizacije edukacionog modela, na takav način da on ne bude ograničen samo na prenos preko satelitskog linka već da obuhvata i druge telekomunikacione tehnologije, a sve za potrebe dodatne edukacije inženjera i studenata završnih godina tehničkih fakulteta. U svakom slučaju to bi bio predmet nekih budućih istraživanja.

Cilj istraživanja ove doktorske disertacije je razvoj novog modela edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka na uspešnost misije bezbednosno-kritičnih HCP sistema koji se oslanjaju na IoT senzorske mreže. Ideja je da se predloženim modelom edukacione platforme obezbedi

moгуćnost kvantifikacije uspešnosti misije jednog takvog sistema, uzimajući u obzir ne samo parametre satelitskog linka, koji je svakako u fokusu ove disertacije, već i parametre senzora, aktuatora, bloka za obradu podataka, kao i ulogu čoveka čiji se uticaj na sistem ogleda kroz stepen obučenosti i iskustvo, čime bi se postigla njegova sveobuhvatnost u odnosu na druge dostupne modele. Tom prilikom biće razmatrane tri različite pozicije čoveka u ovakvim sistemima. U pitanju su dizajner ili arhitekta sistema, korisnik, odnosno operater sistema i student ili bilo koji inženjer kojem će predloženi model omogućiti stručno usavršavanje kroz podizanje nivoa praktičnog znanja.

U svakom slučaju novim modelom edukacione platforme bi trebalo da je moguće evidentirati potencijalne slabe tačke sistema i potvrditi da je određeni bezbednosno-kritični IoT HCP sistem sa datim skupom operatera spreman za efikasnu upotrebu. Budući model bi takođe trebalo da kroz povećanje stepena obučenosti i iskustva korisnika sistema, simulacijom i emulacijom u laboratorijskim uslovima, omogući unapređenje funkcionalnosti i efikasnosti kao i optimizaciju postojećeg, već implementiranog bezbednosno-kritičnog IoT HCP sistema, u odnosu na mnoga ograničenja koja pre svega sa sobom donosi satelitski link. Na taj način, primenjeni model edukacione platforme bi potvrdio i kvantifikovao da se uspešnost misije može ostvariti i dobrom edukacijom i obukom koja bi kompenzovala tehničke nedostatke sistema.

Osim toga, jedan od ciljeva je i da se praktičnom realizacijom predloženog modela u laboratorijskim uslovima dizajnerima i arhitektama sistema pruži jasan uvid u ograničenja koja sa sobom nosi satelitski link, a koja su i te kako važna za razvoj i unapređenje različitih senzora, servisa, aplikacija, algoritama i uređaja. Laboratorijsko okruženje u kojem je moguće verifikovati primenljivost budućeg modela oslanjaće se na simulirani satelitski link realizovan parametrizacijom na osnovu eksperimentalnih rezultata dobijenih na realnom sistemu za nadzor obale u Gvinejskom zalivu.

Poseban cilj će biti prilagođenje budućeg modela za potrebe edukacije inženjera i studenata završnih godina tehničkih fakulteta u okviru stručne prakse koju organizuje Institut Vlatacom, kako bi se kroz simulaciju različitih telekomunikacionih servisa, u različitim uslovima podigao nivo i kvalitet njihovog praktičnog znanja. Time bi se ukazalo na potrebe i mogućnost generalizacije predloženog modela jer on ne bi bio više ograničen samo na satelitski link već bi obuhvatao i druge telekomunikacione tehnologije, što će svakako biti predmet nekih budućih istraživanja.

4. POČETNA LISTA BIBLIOGRAFSKIH IZVORA KOJA ĆE BITI KORIŠĆENA U IZRADI DOKTORSKE DISERTACIJE

1. Abdelsalam, A., Roseti, C., & Zampognaro, F. (2018). Satellite telecommunication networks Simulation and Emulation requirements. *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–7. <https://doi.org/10.1109/ISNCC.2018.8531074>
2. Abraham, S., & Miguel, A. (2017). Creation of an internet of things (IoT)-based innovation lab. *Proceedings of the ASEE Annual Conference and Exposition, 2017*. <https://doi.org/10.18260/1-2--28087>
3. Afzaal, H., & Zafar, N. A. (2018). Modeling of IoT-based border protection system. *Proceedings of the 1st International Conference on Latest Trends in Electrical Engineering and Computing Technologies, INTELLECT 2017*, 1–6. <https://doi.org/10.1109/INTELLECT.2017.8277639>
4. Agrawal, J. P., Farook, O., Anderson, Z. J., & Walker, D. G. (2019). Internet of Things (IoT) laboratory. *Proceedings of the ASEE Annual Conference and Exposition 2019*. <https://doi.org/10.18260/1-2--33008>
5. Al-Emran, M., Malik, S. I., & Al-Kabi, M. N. (2020). A survey of Internet of Things (IoT) in

- education: Opportunities and challenges. In A. E. Hassanien, R. Bhatnagar, N. E. M. Khalifa, & M. H. N. Taha (Eds.), *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* (Vol. 846, pp. 197–209). Springer International Publishing. https://doi.org/10.1007/978-3-030-24513-9_12
6. Alkhathami, M., Alazzawi, L., & Elkateeb, A. (2015). Border surveillance and intrusion detection using wireless sensor networks. *International Journal of Advances in Engineering & Technology*, 8(2), 17–29.
7. Althoubi, A., Alshahrani, R., & Peyravi, H. (2021). Delay Analysis in IoT Sensor Networks. *Sensors*, 21(11). <https://doi.org/10.3390/s21113876>
8. Amruta N. Banagar, & Rajshankar Khattar. (2020). IoT based Smart Laboratory System. *International Journal of Engineering Research And*, 9(01), 315–318. <https://doi.org/10.17577/ijertv9is010178>
9. Anwar, N., Xiong, G., Lu, W., Ye, P., Zhao, H., & Wei, Q. (2021). Cyber-Physical -Social Systems for Smart Cities: An Overview. *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*, 348–353. <https://doi.org/10.1109/DTPI52967.2021.9540102>
10. Aukua Systems. (n.d.). *MGA2510 Network Impairment Emulator*. Retrieved May 10, 2021, from https://www.aukua.com/MGA2510/networkemulator.html?gclid=CjwKCAjw1uiEBhBzEiwAO9B_HSjq37X95ECwI8tHh3WSuYej0wTqRHtze57YLNagSC9fTR6y7iERxoCnCEQAvD_BwE
11. Barnes, P. (2022). Challenges in Simulating Communication Systems: State of the art and open challenges in simulating network and communications systems. *Proceedings of the 2022 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation*, 118–125. <https://doi.org/10.1145/3518997.3534120>
12. Barrere, M., & Hankin, C. (2021). Analysing mission-critical cyber-physical systems with AND/OR graphs and MaxSAT. *ACM Transactions on Cyber-Physical Systems*, 5(3), 1–29. <https://doi.org/10.1145/3451169>
13. Bayani, M. (2020). The Influence of IoT Simulation in the Learning Process: A Case Study. *Proceedings of the 2020 8th International Conference on Information and Education Technology*, 104–109. <https://doi.org/10.1145/3395245.3396427>
14. Bellouch, A., Boujnoui, A., Zaaloul, A., & Haqiq, A. (2021). Modelling and Performance Evaluation of IoT Network During the COVID-19 Pandemic. In A. Abraham, H. Sasaki, R. Rios, N. Gandhi, U. Singh, & K. Ma (Eds.), *Innovations in Bio-Inspired Computing and Applications* (pp. 131–140). Springer International Publishing.
15. Boulila, N. (2019). *Cyber-Physical Systems and Industry 4.0: Properties, structure, communication, and behavior*. <https://doi.org/10.13140/RG.2.2.27890.76485>
16. Burd, B., Barker, L., Divitini, M., Perez, F. A. F., Russell, I., Siever, B., & Tudor, L. (2018). Courses, Content, and Tools for Internet of Things in Computer Science Education. *Proceedings of the 2017 ITiCSE Conference on Working Group Reports*, 125–139. <https://doi.org/10.1145/3174781.3174788>
17. Calinescu, R., Cámara, J., & Paterson, C. (2019). Socio-Cyber-Physical Systems: Models, Opportunities, Open Challenges. *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 2–6. <https://doi.org/10.1109/SEsCPS.2019.00008>
18. Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer Network Simulation with ns-3: A Systematic Literature Review. *Electronics*, 9(2). <https://doi.org/10.3390/electronics9020272>
19. Chen, M., Miao, Y., & Humar, I. (2019). Introduction to OPNET Network Simulation. In *OPNET IoT Simulation* (pp. 77–153). Springer Singapore. https://doi.org/10.1007/978-981-32-9170-6_2
20. Chou, T.-S., Baker, S. K., & Vega-Herrera, M. (2016). A comparison of network simulation and emulation virtualization tools. *Proceedings of the 2016 ASEE Annual Conference & Exposition*. <https://doi.org/10.18260/p.26285>
21. Crespo, R., Lopez-Caudana, E., Romo, K., & Mantilla, A. (2022). Scenarios for student-centered

- learning: RFID Pocket Lab and IoT Platform as teaching tools. *Proceedings of the IEEE Global Engineering Education Conference, EDUCON 2022*, 108–116.
<https://doi.org/10.1109/EDUCON52537.2022.9766547>
22. Daun, M., & Tenbergen, B. (2022). Context modeling for cyber-physical systems. *Journal of Software: Evolution and Process*, n/a(n/a), e2451. <https://doi.org/https://doi.org/10.1002/smr.2451>
 23. De Sanctis, M., Cianca, E., Araniti, G., Bisio, I., & Prasad, R. (2016). Satellite communications supporting internet of remote things. *IEEE Internet of Things Journal*, 3(1), 113–123.
<https://doi.org/10.1109/JIOT.2015.2487046>
 24. Delaney, D. T., & O'Hare, G. M. P. (2016). A framework to implement IoT network performance modelling techniques for network solution selection. In *Sensors (Switzerland)* (Vol. 16, Issue 12).
<https://doi.org/10.3390/s16122038>
 25. Dobrilovic, D., & Stojanov, Z. (2016). Design of open-source platform for introducing Internet of Things in university curricula. *Proceedings of the 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, SACI 2016*, 273–276.
<https://doi.org/10.1109/SACI.2016.7507384>
 26. Duan, T., & Dinavahi, V. (2021). Starlink Space Network-Enhanced Cyber-Physical Power System. *IEEE Transactions on Smart Grid*, 12(4), 3673–3675.
<https://doi.org/10.1109/TSG.2021.3068046>
 27. Ehlers, B. (n.d.). *NETem - Network Link Emulator*. Retrieved May 10, 2021, from <https://www.b-ehlers.de/projects/netem/index.html>
 28. Eisenberg, D. A., Alderson, D. L., Kitsak, M., Ganin, A., & Linkov, I. (2018). Network foundation for command and control (C2) systems: Literature review. *IEEE Access*, 6, 68782–68794. <https://doi.org/10.1109/ACCESS.2018.2873328>
 29. Elsaadany, A., & Khalil, K. (2020). Assessment of coverage quality of sensor networks for IoT applications. *Peer-to-Peer Networking and Applications*, 13(1), 320–332.
<https://doi.org/10.1007/s12083-019-00796-2>
 30. Erickson, V. L., Varshney, P., & Ertaul, L. (2021). A Project-Based Approach to Teaching IoT. In H. R. Arabnia, L. Deligiannidis, F. G. Tinetti, & Q.-N. Tran (Eds.), *Advances in Software Engineering, Education, and e-Learning* (pp. 195–216). Springer International Publishing.
 31. Eriksson, K. M., Alsaleh, A., Behzad Far, S., & Stjern, D. (2022). Applying Digital Twin Technology in Higher Education : An Automation Line Case Study. *Advances in Transdisciplinary Engineering*, 21, 461–472. <https://doi.org/10.3233/atde220165>
 32. Fabrizio, G. A. (2013). *High Frequency Over-the-Horizon Radar: Fundamental Principles, Signal Processing, and Practical Applications*. McGraw Hill Professional.
 33. Flores, E., Xu, X., & Lu, Y. (2020). Human Cyber-Physical Systems: A skill-based correlation between humans and machines. *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, 1313–1318. <https://doi.org/10.1109/CASE48305.2020.9216843>
 34. Galaxy Technologies, L. (2021). *Graphical Network Simulator-3, GNS3*. <https://www.gns3.com/>
 35. Gameiro, A., Castanheira, D., Sanson, J., & Monteiro, P. P. (2018). Research Challenges, Trends and Applications for Future Joint Radar Communications Systems. *Wireless Personal Communications*, 100(1), 81–96. <https://doi.org/10.1007/s11277-018-5614-8>
 36. GL Communications Inc. (n.d.). *IP WAN Emulator*. Retrieved May 10, 2021, from <https://www.gl.com/wan-link-emulation-ipnetsim.html>
 37. Gonzalez-Nalda, P., Calvo, I., Etxeberria-Agiriano, I., García-Ruiz, A., Martínez-Lesta, S., & Caballero-Martín, D. (2014). Building a CPS as an Educational Challenge. *International Journal of Online and Biomedical Engineering (IJOE)*, 10(4), 52–58.
<https://doi.org/10.3991/ijoe.v10i4.3765>
 38. Guan, Y., Vasquez, J. C., Guerrero, J. M., Samovich, N., Vanya, S., Oravec, V., Garcia-Castro, R., Serena, F., Poveda-Villalon, M., Radojicic, C., Heinz, C., Grimm, C., Tryferidis, A., Tzovaras, D., Dickerson, K., Paralic, M., Skokan, M., & Sabol, T. (2017). An open virtual neighbourhood network to connect IoT infrastructures and smart objects - VICINITY. *Global Internet of Things Summit, Giots 2017*, 134–139.

39. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
40. Guillén, E., Sánchez, J., & Ramos, C. O. (2017). A model to evaluate the performance of IoT applications. *Proceedings of the International MultiConference of Engineers and Computer Scientists, IMECS 2017*, 2227, 147–150.
41. Handa, A., & Reka, S. S. (2022). Developing a Cyber-Physical Laboratory Using Internet of Things. In R. R. Raje, F. Hussain, & R. J. Kannan (Eds.), *Artificial Intelligence and Technologies* (pp. 287–294). Springer Singapore.
42. Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). *IoT Fundamentals: Networking Technologies, Protocols and Use Cases for the Internet of Things*. Cisco Press.
43. Hemminger, S. (2005). Network Emulation with NetEm. *Proceedings of the 6th Australian National Linux Conference (LCA 2005)*, 1–9.
44. Hudaib, A. A. Z. (2016). Satellite network hacking & security analysis. *International Journal of Computer Science and Security (IJCSS)*, 1(10), 2016–2024.
45. IBM. (n.d.). *What is a digital twin?* Retrieved May 23, 2022, from <https://www.ibm.com/topics/what-is-a-digital-twin>
46. Ilčev, S. D. (2017). *Global Mobile Satellite Communications Theory For Maritime, Land and Aeronautical Applications* (2nd ed.). Springer International Publishing Switzerland. <https://doi.org/10.1007/978-3-319-39171-7>
47. Isakovic, H., Ratasich, D., Hirsch, C., Platzer, M., Wally, B., Rausch, T., Nickovic, D., Krenn, W., Kappel, G., Dustdar, S., & Grosu, R. (2019). CPS/IoT Ecosystem: A Platform for Research and Education. In R. Chamberlain, W. Taha, & M. Törngren (Eds.), *Cyber Physical Systems. Model-Based Design* (pp. 206–213). Springer International Publishing.
48. iTrinegy. (n.d.). *NE-ONE Network Emulator*. Retrieved May 10, 2021, from <https://itrinegy.com/ne-one-professional-range/>
49. Jahandideh, I., Ghassemi, F., & Sirjani, M. (2019). Hybrid Rebeca: Modeling and Analyzing of Cyber-Physical Systems. In R. Chamberlain, W. Taha, & M. Törngren (Eds.), *Cyber Physical Systems. Model-Based Design* (pp. 3–27). Springer International Publishing.
50. Jun, S., Przystupa, K., Beshley, M., Kochan, O., Beshley, H., Klymash, M., Wang, J., & Pieniak, D. (2020). A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network. *Electronics*, 9(1). <https://doi.org/10.3390/electronics9010040>
51. Kalita, H. K., & Nambiar, M. K. (2011). Designing WANem : A wide area network emulator tool. *Proceedings of the 3rd International Conference on Communication Systems and Networks, COMSNETS 2011*, 4–7. <https://doi.org/10.1109/COMSNETS.2011.5716495>
52. Kang, B. G., Seo, K.-M., & Kim, T. G. (2019). Model-Based Design of Defense Cyber-Physical Systems to Analyze Mission Effectiveness and Network Performance. *IEEE Access*, 7, 42063–42080. <https://doi.org/10.1109/ACCESS.2019.2907566>
53. Karthick, R., Prabakaran, A. M., & ... (2019). Internet of things based high security border surveillance strategy. *Asian Journal of Applied Science and Technology (AJAST)*, 3(2), 94–100. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3394082
54. Karvinen, K., & Karvinen, T. (2018). IoT rapid prototyping laboratory setup. *International Journal of Engineering Education*, 34(1), 263–272.
55. Keysight Technologies. (n.d.). *Network Emulator II*. Retrieved May 10, 2021, from <https://www.keysight.com/zz/en/products/network-test/network-test-hardware/network-emulator-ii.html>
56. Kirichek, R., & Koucheryavy, A. (2016). Internet of things laboratory test bed. *Lecture Notes in Electrical Engineering*, 348, 485–494. https://doi.org/10.1007/978-81-322-2580-5_44
57. Kleinschmidt, J. H. (2021). Teaching internet of things for engineering courses: A project-based cooperative approach. *The International Journal of Electrical Engineering & Education*, 58(4), 858–873. <https://doi.org/10.1177/0020720919867437>
58. Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., Montoya, J. F. M., Duncan, J.

- C. M., Spano, D., Chatzinotas, S., Kisseleff, S., Querol, J., Lei, L., Vu, T. X., & Goussetis, G. (2021). Satellite communications in the new space era: A survey and future challenges. *IEEE Communications Surveys and Tutorials*, 23(1), 70–109. <https://doi.org/10.1109/COMST.2020.3028247>
59. Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.
 60. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
 61. Liu, Q. (2019). Applying simulators in computer networks education to encourage personalised learning. *Global Journal of Engineering Education*, 21(2), 109–114.
 62. Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, 4(1), 27–40. <https://doi.org/10.1109/JAS.2017.7510349>
 63. Liu, Zhiming, & Wang, J. (2020). Human-cyber-physical systems: concepts, challenges, and research opportunities. *Frontiers of Information Technology & Electronic Engineering*, 21(11), 1535–1553. <https://doi.org/10.1631/FITEE.2000537>
 64. Liu, Zhong, Yang, D., Wen, D., Zhang, W., & Mao, W. (2011). Cyber-Physical-Social Systems for Command and Control. *IEEE Intelligent Systems*, 26(4), 92–96. <https://doi.org/10.1109/MIS.2011.69>
 65. Loukatos, D., Androulidakis, N., Arvanitis, K. G., Peppas, K. P., & Chondrogiannis, E. (2022). Using Open Tools to Transform Retired Equipment into Powerful Engineering Education Instruments: A Smart Agri-IoT Control Example. *Electronics*, 11(6). <https://doi.org/10.3390/electronics11060855>
 66. Lshukri, D. A., Vidhya Lavanya, L., Sumesh, E. P., & Krishnan, P. (2019). Intelligent border security intrusion detection using IoT and embedded systems. *Proceedings of the 4th MEC International Conference on Big Data and Smart City, ICBDS C 2019*, 1–3. <https://doi.org/10.1109/ICBDSC.2019.8645587>
 67. Maral, G., Bousquet, M., & Sun, Z. (2020). *Satellite communications systems: systems, techniques and technology* (6th ed.). John Wiley & Sons Ltd.
 68. Marquardson, J., & Gomillion, D. L. (2019). Simulation for network education: Transferring networking skills between simulated to physical environments. *Information Systems Education Journal*, 17(1).
 69. Marwedel, P., Mitra, T., Grimheden, M. E., & Andrade, H. A. (2020). Survey on Education for Cyber-Physical Systems. *IEEE Design Test*, 37(6), 56–70. <https://doi.org/10.1109/MDAT.2020.3009613>
 70. Metzger, F., Hoßfeld, T., Bauer, A., Kounev, S., & Heegaard, P. E. (2019). Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud. *Proceedings of the IEEE*, 107(4), 679–694. <https://doi.org/10.1109/JPROC.2019.2901578>
 71. Microsoft. (n.d.). *Network Emulator Toolkit*. Retrieved May 10, 2021, from <https://blog.mrpnl.nl/2010/01/14/network-emulator-toolkit/>
 72. Murdoch, O., O’Grady, M., & O’Hare, G. (2021). A cyber sensor model for cyber-physical-social systems. *International Journal of Agricultural and Environmental Information Systems (IJAEIS)*, 12(1). <https://doi.org/10.4018/IJAEIS.20210101.0a6>
 73. Musk, E. (2002). *SpaceX*. <https://www.spacex.com/>
 74. Mylonas, G., Amaxilatis, D., Pocero, L., Markelis, I., Hofstaetter, J., & Koulouris, P. (2019). An educational IoT lab kit and tools for energy awareness in European schools. *International Journal of Child-Computer Interaction*, 20, 43–53. <https://doi.org/https://doi.org/10.1016/j.ijcci.2019.03.003>
 75. Nambiar, M., Kalita, H. K., Mishra, D., & Rane, S. (2007). WANem: The wide area network emulator. *Performance Engineering Research Centre, Mumbai*.
 76. Nawrat, A., Simek, K., & Świerniak, A. (Eds.). (2013). *Advanced technologies for intelligent systems of national border security* (1st ed., Vol. 440). Springer-Verlag Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-31665-4>

77. Negri, E., Fumagalli, L., & Macchi, M. (2017). A Review of the Roles of Digital Twin in CPS-based Production Systems. *Procedia Manufacturing*, 11, 939–948. <https://doi.org/https://doi.org/10.1016/j.promfg.2017.07.198>
78. Nikolaev, S., Gusev, M., Padalitsa, D., Mozhenkov, E., Mishin, S., & Uzhinsky, I. (2018). Implementation of “Digital Twin” Concept for Modern Project-Based Engineering Education. In P. Chiabert, A. Bouras, F. Noël, & J. Rios (Eds.), *Product Lifecycle Management to Support Industry 4.0* (pp. 193–203). Springer International Publishing.
79. Nvidia Developer. (n.d.). *Jetson TX2 Module*. Retrieved May 10, 2021, from <https://developer.nvidia.com/embedded/jetson-tx2>
80. Park, E., del Pobil, A. P., & Kwon, S. J. (2018). The role of Internet of Things (IoT) in smart cities: Technology roadmap-oriented approaches. *Sustainability*, 10(5), 1–13. <https://doi.org/10.3390/su10051388>
81. Park, H., Easwaran, A., & Andalam, S. (2019). Challenges in Digital Twin Development for Cyber-Physical Production Systems. In R. Chamberlain, W. Taha, & M. Törngren (Eds.), *Cyber Physical Systems. Model-Based Design* (pp. 28–48). Springer International Publishing.
82. Parmar, R., Leiponen, A., & Thomas, L. D. W. (2020). Building an organizational digital twin. *Business Horizons*, 63(6), 725–736. <https://doi.org/https://doi.org/10.1016/j.bushor.2020.08.001>
83. Peng, S.-L., Pal, S., & Huang, L. (Eds.). (2020). *Principles of Internet of Things (IoT) ecosystem: Insight paradigm* (1st ed., Vol. 174). Springer International Publishing. <https://doi.org/10.1007/978-3-030-33596-0>
84. Perkel, J. (2017). The Internet of Things comes to the lab. *Nature*, 542(7639), 125–126. <https://doi.org/10.1038/542125a>
85. Petrovic, R., Simic, D., Drajić, D., Cica, Z., Nikolic, D., & Peric, M. (2020). Designing laboratory for IoT communication infrastructure environment for remote maritime surveillance in equatorial areas based on the Gulf of Guinea field experiences. *Sensors*, 20(5). <https://doi.org/10.3390/s20051349>
86. Petrovic, R., Simic, D., & Peric, M. (2020). IoT laboratory for supporting different types of secure communications with sensors, with the special emphasis on satellite link. *17th International Symposium on Business and Artificial Intelligence, Symorg 2020*, 183–192.
87. Petrovic, S. (2012). Dilema: Kiber ili sajber. *Strani Pravni Život*, 56(2), 368–377.
88. Ponsford, A. M., Sevgi, L., & Chan, H. C. (2001). An integrated maritime surveillance system based on high-frequency surface-wave radars, Part 2: Operational status and system performance. *IEEE Antennas and Propagation Magazine*, 43(5), 52–63. <https://doi.org/10.1109/74.979367>
89. Poongothai, M., L., A., & Priyadharshini, R. (2018). Implementation of IoT based Smart Laboratory. *International Journal of Computer Applications*, 182(15), 31–34. <https://doi.org/10.5120/ijca2018917853>
90. Popereshnyak, S., Suprun, O., Suprun, O., & Wieckowski, T. (2018). IoT application testing features based on the modelling network. *2018 XIV-Th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, 127–131. <https://doi.org/10.1109/MEMSTECH.2018.8365717>
91. Prakash, K. R., Narake, P., & Ramya, M. V. (2022). Implementation of Industrial IoT Laboratory for Sensors. In S. K. Natarajan, R. Prakash, & K. Sankaranarayanan (Eds.), *Recent Advances in Manufacturing, Automation, Design and Energy Technologies* (pp. 435–443). Springer Singapore. https://doi.org/10.1007/978-981-16-4222-7_50
92. Rath, G., & Payr, M. (2022). A Remote Laboratory for Teaching Internet of Things in Online Education. *Proceedings of the 11th Mediterranean Conference on Embedded Computing (MECO)*, 2022, 1–4. <https://doi.org/10.1109/MECO55406.2022.9797153>
93. Rout, K. K., Mishra, S., & Routray, A. (2018). Development of an Internet of Things (IoT) based introductory laboratory for under graduate engineering students. *Proceedings of the International Conference on Information Technology, ICIT 2017*, 113–118. <https://doi.org/10.1109/ICIT.2017.22>
94. Routray, S. K., Javali, A., Sharma, L., Tengshe, R., Sarkar, S., & Ghosh, A. D. (2019). Satellite

- based IoT for mission critical applications. *Proceedings of the International Conference on Data Science and Communication, IconDSC 2019*, 1–6.
<https://doi.org/10.1109/IconDSC.2019.8817030>
95. Sahinel, D., Akpolat, C., Görür, O. C., & Sivrikaya, F. (2019). Integration of Human Actors in IoT and CPS Landscape. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 485–490.
<https://doi.org/10.1109/WF-IoT.2019.8767276>
 96. Seshia, S. A. (2022). Explorations in CPS education and related research projects over the past two decades unveil where CPS learning is headed. *Communications of the ACM*, 65(5), 60–69.
<https://doi.org/10.1145/3490442>
 97. Sevgi, L., Ponsford, A. M., & Chan, H. C. (2001). An integrated maritime surveillance system based on high-frequency surface-wave radars. 1. Theoretical background and numerical simulations. *IEEE Antennas and Propagation Magazine*, 43(4), 28–43.
<https://doi.org/10.1109/74.951557>
 98. Singh, M., Srivastava, R., Fuenmayor, E., Kuts, V., Qiao, Y., Murray, N., & Devine, D. (2022). Applications of Digital Twin across Industries: A Review. *Applied Sciences*, 12(11).
<https://doi.org/10.3390/app12115727>
 99. Song, Z., Shah, N., Guo, J., & Zhu, Q. (2022). Applying Project-based Learning to Improve Computer Networks Courses: An Experience Report. *Proceedings of the IEEE Global Engineering Education Conference, EDUCON 2022*, 148–156.
<https://doi.org/10.1109/EDUCON52537.2022.9766750>
 100. SpaceX. (2015). *Starlink*. <https://www.starlink.com/>
 101. Stellios, I., Kotzanikolaou, P., Psarakis, M., & Alcaraz, C. (2021). Risk Assessment for IoT-Enabled Cyber-Physical Systems. In G. A. Tsihrintzis & M. Virvou (Eds.), *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris* (pp. 157–173). Springer International Publishing. https://doi.org/10.1007/978-3-030-41196-1_8
 102. Sun, W., Ji, M., Huang, W., Ji, Y., & Dai, Y. (2020). Vessel tracking using bistatic compact HFSWR. *Remote Sensing*, 12(8), 3–8. <https://doi.org/10.3390/RS12081266>
 103. Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. *Journal of Network and Computer Applications*, 154, 102538.
<https://doi.org/10.1016/j.jnca.2020.102538>
 104. Tan, Y., Yang, W., Yoshida, K., & Takakuwa, S. (2019). Application of IoT-aided simulation to manufacturing systems in cyber-physical system. *Machines*, 7(1).
<https://doi.org/10.3390/machines7010002>
 105. Tao, J., Xia, Q., Liu, Q., & She, X. (2022). Design and Research of a Virtual Computer Network Experimental Teaching System. *Proceedings of the 11th International Conference on Educational and Information Technology, ICEIT 2022*, 16–20.
<https://doi.org/10.1109/ICEIT54416.2022.9690752>
 106. TATA Consultancy Services. (n.d.). *WANem Network Emulator*. Retrieved May 10, 2021, from <http://wanem.sourceforge.net/>
 107. Tian, J., Li, X., Wan, D., Li, N., & Wang, Y. (2017). Design of intelligent laboratory based on IOT. *Advances in Intelligent Systems and Computing*, 454, 687–692. https://doi.org/10.1007/978-3-319-38789-5_75
 108. Vodrážka, J., Kocur, Z., & Hrad, J. (2019). Experimental setup for testing of communication systems and services in engineering education. *Proceedings of the 29th Annual Conference of the European Association for Education in Electrical and Information Engineering, EAEEIE 2019*.
<https://doi.org/10.1109/EAEEIE46886.2019.9000470>
 109. Von Sperling, T. L., De Caldas Filho, F. L., De Sousa, R. T., Martins Lucas, M. C. E., & Rocha, R. L. (2017). Tracking intruders in IoT networks by means of DNS traffic analysis. *Proceedings of the 2nd Workshop on Communication Networks and Power Systems, WCNPS 2017, 2018-Janua*, 1–4. <https://doi.org/10.1109/WCNPS.2017.8252938>
 110. Wang, B., Zhou, H., Yang, G., Li, X., & Yang, H. (2022). Human Digital Twin (HDT) Driven Human-Cyber-Physical Systems: Key Technologies and Applications. *Chinese Journal of*

- Mechanical Engineering*, 35(1), 11. <https://doi.org/10.1186/s10033-022-00680-w>
111. Zhou, J., Zhou, Y., Wang, B., & Zang, J. (2019). Human–Cyber–Physical Systems (HCPs) in the Context of New-Generation Intelligent Manufacturing. *Engineering*, 5(4), 624–636. <https://doi.org/10.1016/j.eng.2019.07.015>

5. HIPOTEZE I ZADACI U ISTRAŽIVANJU

Opšta hipoteza: Moguće je razviti novi model edukacione platforme za ispitivanje uticaja satelitskog linka na uspešnost misije bezbednosno-kritičnih HCP sistema koji se oslanjaju na IoT senzorske mreže čija bi glavna prednost u odnosu na postojeće modele bila njegova sveobuhvatnost jer obezbeđuje mogućnost kvantifikacije uspešnosti misije koju jedan bezbednosno-kritični IoT HCP sistem obavlja, uzimajući u obzir ne samo parametre satelitskog linka, koji je svakako u fokusu ove disertacije, već i parametre senzora, aktuatora, bloka za obradu podataka, kao i ulogu čoveka čiji se uticaj na sistem ogleda kroz stepen obučenosti i iskustvo.

Pomoćne hipoteze:

H1 - Novim modelom edukacione platforme moguće je u laboratorijskim uslovima evidentirati potencijalne slabe tačke sistema.

H2 - Budući model edukacione platforme omogućava unapređenje funkcionalnosti i efikasnosti kao i optimizaciju postojećeg, već implementiranog bezbednosno-kritičnog IoT HCP sistema, i to kroz povećanje stepena obučenosti i iskustva korisnika sistema, simulacijom i emulacijom u laboratorijskim uslovima, a u odnosu na mnoga ograničenja koja pre svega sa sobom donosi satelitski link.

H3 - Praktičnom realizacijom predloženog modela edukacione platforme u laboratorijskim uslovima dizajnerima i arhitektama sistema je moguće pružiti jasan uvid u ograničenja koja sa sobom nosi satelitski link na konkretnom sistemu koji se ispituje, a koja su i te kako važna za razvoj i unapređenje različitih senzora, servisa, aplikacija, algoritama i uređaja.

H4 - Predloženi model edukacione platforme, odnosno njegova praktična realizacija, podiže nivo praktičnog znanja kod studenata tehničkih fakulteta tokom obavljanja obavezne studentske prakse.

6. NAUČNE METODE ISTRAŽIVANJA

Opšte naučne metode istraživanja koje će biti upotrebljene jesu analitičko-sintetička, deduktivno logička, sistemski pristup i komparativni pristup.

Posebne metode koje će se koristiti za realizaciju istraživanja i evaluaciju postavljenih hipoteza su:

- Pregled i analiza raspoložive literature koja pripada naučnim oblastima relevantnim za predmet istraživanja
- Kritička analiza trenutnog stanja HCP i IoT edukacionih modela, platformi, i laboratorija kao i modela, simulatora i emulatora komunikacionog sistema i predlog novog rešenja

- Statistička analiza kvaliteta servisa sistema za nadzor mora baziranog na radarskim sistemima izvan linije horizonta i elektro-optičkim sistemima u Gvinejskom zalivu za potrebe parametrizacije predloženog modela u laboratorijskim uslovima
- Eksperimentalna provera da se uspešnost misije nekog sistema može ostvariti i dobrom edukacijom i obukom kroz predloženi model kako bi se kompenzovali tehnički nedostaci sistema
- Eksperimentalna provera primenljivosti predloženog modela na različitim slučajevima primene

7. OČEKIVANI DOPRINOSI ISTRAŽIVAČKOG RADA

Očekivani naučni doprinosi u okviru ovog istraživanja su:

- Kritički pregled i sistematizacija postojećih HCP i IoT laboratorija, edukacionih platformi i modela kao i modela, simulatora i emulatora komunikacionog bloka.
- Identifikovanje izazova i ograničenja u komunikaciji koja se zasniva na satelitskom linku u bezbednosno-kritičnim IoT HCP sistemima.
- Razvoj novog modela edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka na bezbednosno-kritične HCP sisteme koji se oslanjaju na IoT senzorske mreže. Sveobuhvatnost modela će se ogledati kroz mogućnost kvantifikacije uspešnosti misije bezbednosno-kritičnih IoT HCP sistema, uzimajući u obzir ne samo parametre satelitskog linka, koji je svakako u fokusu ove disertacije, već i parametre senzora, aktuatora, bloka za obradu podataka, kao i ulogu čoveka i to kroz tri različite pozicije čiji se uticaj na sistem ogleda kroz stepen obučenosti i iskustvo.
- Verifikacija predloženog modela edukacione platforme kroz praktičnu realizaciju u laboratorijskom okruženju na osnovu parametrizacije realnog satelitskog linka i eksperimenata u okviru jednog velikog bezbednosno-kritičnog sistema za nadzor morske obale u Gvinejskom zalivu baziranog na radarskim sistemima i satelitskoj komunikaciji, kao jedne njegove instance. Kroz povećanje stepena obučenosti i iskustva dizajnera i korisnika sistema, simulacijom i emulacijom u laboratorijskim uslovima, predloženim modelom omogućiti će se:
 1. unapređenje funkcionalnosti i efikasnosti kao i optimizacija postojećeg, već implementiranog bezbednosno-kritičnog IoT HCP sistema,
 2. olakšan razvoj različitih senzora, servisa, aplikacija, algoritama i uređaja, a sve u odnosu na mnoga ograničenja koja pre svega sa sobom donosi satelitski link.

Očekivani **društveni doprinosi** su u vidu prilagođenja predloženog modela za potrebe edukacije inženjera i studenata završnih godina tehničkih fakulteta, kako bi se kroz simulaciju različitih telekomunikacionih servisa, u različitim uslovima podigao nivo i kvalitet njihovog praktičnog znanja.

Rezultati istraživanja koji nastanu u toku izrade doktorske disertacije biće saopšteni na naučnim i stručnim skupovima u zemlji i inostranstvu i objavljeni u časopisima međunarodnog značaja.

8. PLAN ISTRAŽIVANJA I STRUKTURA RADA

Plan istraživanja

Okvirni plan istraživanja po fazama je:

Faza 1 - Prikupljanje relevantnih bibliografskih referenci.

Faza 2 - Analiza prikupljene literature i pregled trenutnog stanja u oblasti.

Faza 3 - Prikupljanje i analiza podataka (vremena i brzine prenosa detekcijskih fajlova, veličine detekcijskih fajlova, broj uspešno prenetih fajlova, propusni opseg, latencija, gubici, džiter) sa realnog sistema u različitim meteorološkim uslovima. Treba imati u vidu da je velika količina podataka već prikupljena u toku prethodnih istraživanja i stoji na raspolaganju, tako da će eventualno biti prikupljeni samo dodatni podaci za dodatne provere hipoteza ove disertacije.

Faza 4 - Razvoj novog modela edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka na uspešnost misije bezbednosno-kritičnih HCP sistema koji se oslanjaju na IoT senzorske mreže.

Faza 5 - Praktična realizacija modela u laboratorijskim uslovima i potvrda da se uspešnost misije nekog sistema može ostvariti i dobrom obukom i edukacijom kroz predloženi model, koja bi kompenzovala tehničke nedostatke sistema.

Faza 6 - Eksperimentalna provera primenljivosti predloženog modela na različitim slučajevima primene.

Faza 7 - Izrada doktorske disertacije.

Faza 8 - Publikacija dela rezultata istraživanja koji će se naknadno pojaviti.

Faza	Mesec											
	1	2	3	4	5	6	7	8	9	10	11	12
1												
2												
3												
4												
5												
6												
7												
8												

Struktura istraživanja

Okvirni sadržaj doktorske disertacije je:

1. Uvod

- 1.1. Predmet i cilj istraživanja
- 1.2. Polazne hipoteze
- 1.3. Struktura disertacije
2. Uloga čoveka u CPS i IoT sistemima
3. Značaj modelovanja, simulacije i emulacije u edukaciji
 - 3.1. Modelovanje HCP sistema
 - 3.2. Primer modelovanja jednog bezbednosno-kritičnog CPS-a
 - 3.3. Koncept digitalnog blizanca
 - 3.4. Modelovanje komunikacionog bloka
 - 3.5. Simulacija i emulacija komunikacionog bloka
 - 3.6. Pregled postojećih HCP i IoT edukacionih platformi, modela i laboratorija
 - 3.7. Kritički osvrt na postojeća rešenja i mogućnost unapređenja
4. Komunikaciona infrastruktura u nepristupačnim graničnim područjima
 - 4.1. IoT komunikacione tehnologije
 - 4.1.1. Klasifikacija IoT komunikacionih tehnologija
 - 4.1.2. IoT komunikacione tehnologije velikog dometa
 - 4.2. Specifičnosti IoT komunikacije preko satelitskog linka
 - 4.2.1. Orbite satelitskih sistema i frekvencijski opsezi
 - 4.2.2. Uticaj meteoroloških uslova na satelitsku vezu
 - 4.3. Komunikaciona infrastruktura u zemljama Afrike
 - 4.3.1. Fiksna telefonija
 - 4.3.2. Fiksne širokopojasne tehnologije
 - 4.3.3. Mobilna telefonija
 - 4.3.4. Mikrotalasni linkovi
 - 4.3.5. Satelitski link
 - 4.4. IoT senzorske mreže za kontrolu nepristupačnih područja
5. Novi model edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka
 - 5.1. Uspešnost misije i stepen zadovoljstva korisnika kao osnova za razvoj modela edukacione platforme
 - 5.2. Realizacija modela edukacione platforme za ispitivanje uticaja mrežnih parametara satelitskog linka
 - 5.3. Doprinos predloženog modela
 - 5.4. Parametrizacija modela na osnovu praktičnog iskustva i eksperimentalnih rezultata dobijenih na realnom sistemu za nadzor obale u Gvinejskom zalivu
 - 5.4.1. Senzorska mreža za nadzor morske obale u Gvinejskom zalivu
 - 5.4.2. Parametri satelitskog linka na osnovu iskustva u Gvinejskom zalivu
 - 5.4.3. Analiza servisa za OTH radare, EO i senzore malog protoka
 - 5.5. Primena modela na formiranje traga mete i detekcija njene devijacije sa zadatog koridora
 - 5.6. Primena modela na ispitivanje uticaja ukupnog vremena prenosa na algoritam za fuziju
 - 5.7. Primena modela na identifikaciju mete na osnovu slike ili video strima i merenje rastojanja do mete
6. Praktična realizacija predloženog modela edukacione platforme
 - 6.1. Implementacija hardverske platforme za ispitivanje uticaja mrežnih parametara satelitskog linka
 - 6.2. Aplikacija za simulaciju komunikacionog linka

- 6.3. Primeri praktične primene modela edukacione platforme za ispitivanje u laboratorijskim uslovima
- 7. Pravci daljeg istraživanja
- 8. Zaključak
- 9. Literatura

9. ZAKLJUČAK I PREDLOG

Uvidom u profesionalne, akademske i istraživačke kvalifikacije i kompetencije kandidata Ranka Petrovića, potpisani članovi Komisije su saglasni da ovaj kandidat ispunjava sve preduslove za rad na predloženoj temi doktorske disertacije. Članovi Komisije su takođe mišljenja da su predloženi ciljevi, hipoteze, metode, plan i struktura dokorskog istraživanja konzistentni s prethodno definisanim predmetom i problemom dokorskog istraživanja, kao i da logično slede rezultate pristupnog rada koji je kandidat Ranko Petrović odbranio pred ovom Komisijom 30. septembra 2022. godine.

Članovi Komisije su saglasni i predlažu da se kandidatu Ranku Petroviću odobri izrada doktorske disertacije pod modifikovanim nazivom „**MODEL EDUKACIONE PLATFORME ZA ISPITIVANJE UTICAJA SATELITSKOG LINKA NA USPEŠNOST MISIJE BEZBEDNOSNO-KRITIČNIH IoT HCP SISTEMA**“.

Uža naučna oblast teme je: Informacione tehnologije.

Za mentora se predlaže: prof. dr Dejan Simić

Prof. dr Dejan Simić ispunjava sve uslove akreditacionih pravila visokoškolskih ustanova i dopunske kriterijume. Radovi koje je mentor objavio u poslednjih deset godina, a koji su u vezi s naučnom oblašću disertacije, priloženi su uz ovaj referat.

U Beogradu, 03.10.2022.

MENTOR

.....
Prof. dr Dejan Simić,

redovni profesor, Fakultet organizacionih nauka, Univerzitet u Beogradu

ČLANOVI KOMISIJE

.....
Prof. dr Miroslav Minović, redovni profesor, Fakultet organizacionih nauka, Univerzitet u Beogradu

.....
dr Dragana Perić, viši naučni saradnik, Vlatacom institut visokih tehnologija, Beograd