

Teme studentskih projekata 2025./2026.

1. Poboljšanje robusnosti lokalizacije za USV Karolina pomoću napredne fuzije senzora

Autonomno plovilo

PROBLEM: Postojeći sustav lokalizacije na [trkaćem plovilu Karolina](#) koristi PX4 EKF2 algoritam. U realnom okruženju sustav pokazuje značajne pogreške u odometriji i nagle skokove u mjerenjima (vidjeti [diplomski rad](#), poglavlje 5.2.2). Ove anomalije, vjerojatno uzrokovane magnetskim smetnjama, predstavljaju kritičnu točku kvara.

OPIS: PX4 EKF2 omogućuje estimaciju stanja spajanjem podataka s IMU-a, GPS-a i magnetometra. Postojeći ROS2 čvor *frame_publisher* (vidjeti diplomski rad, poglavlje 4.3.1) prenosi dobivene podatke o odometriji iz PX4 sustava u ROS i pritom ne provodi nekakvu značajnu obradu podataka. To sugerira da je izvor grešaka u samom PX4 EKF2 sustavu. Predlaže se istraživanje drugih rješenja za lokalizaciju koja nude veću kontrolu nad fuzijom senzora. Potrebno je:

- Usporediti PX4 EKF2 s naprednijim rješenjima za fuziju senzora u ROS2, npr. ROS2 paket *robot_localization* ili GTSAM;
- Postaviti Gazebo/VRX/SITL simulacijsko okruženje iz diplomskog rada;
- Analizirati postojeći čvor *frame_publisher*;
- Predložiti kako biste migrirali sustav lokalizacije na *robot_localization* EKF čvor. Novi čvor bi spajao podatke s IMU-a, GPS-a i, potencijalno, vizualnu odometriju sa ZED X kamere koja se trenutačno ne koristi u ovu svrhu.

CILJ: Cilj projekta je ostvariti glađu i robusniju lokalizaciju, smanjiti *drift* i osjetljivost na magnetske smetnje u operativnom okruženju trkaćeg plovila.

2. Sustav temeljen na Behavior Tree logici za integraciju COLREG pravila u ROS2 Nav2 sustav

Autonomno plovilo

PROBLEM: Postojeći sustav navigacije na [trkaćem plovilu Karolina](#) učinkovito izbjegava statične prepreke, ali ne poštuje COLREG međunarodna pravila za sprječavanje sudara na moru koja reguliraju dinamičke susrete plovila. Ovo

ograničenje smanjuje sigurnost i autonomnost plovila, pogotovo u situacijama poput direktnog susreta, križanja ili pretjecanja.

OPIS: Poštivanje COLREG međunarodnih pravila za sprječavanje sudara na moru je ključno za sigurnu autonomnu navigaciju, no njihova implementacija pomoću klasičnih *if-else* uvjeta je nepraktična zbog složenosti i dinamičnosti interakcija između plovila. Predlaže se korištenje Behavior Tree (BT) arhitekture za modeliranje sustava i donošenje odluka. Potrebno je:

- Istražiti kako modelirati i integrirati COLREG pravila u ROS2 Nav2 sustav;
- Upoznati se s osnovama Behavior Tree struktura koje koristi Nav2;
- Predložiti dizajn jednostavnog Behavior Tree *plugina* koji implementira jedno COLREG pravilo, npr. kada se dva plovila približavaju jedan drugom iz suprotnih kurseva, oba moraju promijeniti kurs udesno;
- Za potrebe testiranja razvijenog koncepta, u Gazebo simulacijskom okruženju potrebno je dodati drugo, skriptirano plovilo koje će omogućiti stvaranje i analizu navedenog scenarija.

CILJ: Cilj projekta je istražiti Behavior Tree (BT) arhitekturu kako bi se omogućilo fleksibilno i predvidivo upravljanje plovilom u složenim scenarijima u skladu s COLREG pravilima.

3. Robusna detekcija prepreka u pomorskom okruženju

Autonomno plovilo

PROBLEM: Postojeći sustav percepcije na [trkaćem plovilu Karolina](#) često lažno detektira prepreke (vidjeti [diplomski rad](#), poglavlje 5.2.2), najvjerojatnije zbog šuma senzora ili pogrešnih klasifikacija modela WaSR-T koji se koristi za segmentaciju i detekciju prepreka u pomorskom okruženju. Lažne detekcije smanjuju pouzdanost sustava, otežavaju planiranje putanje i mogu uzrokovati nepotrebne manevre izbjegavanja, što direktno utječe na sigurnost i učinkovitost navigacije.

OPIS: Postojeći sustav obrađuje svaki kadar dobiven sa ZED X kamere zasebno, pa se kratkotrajne pogrešne detekcije nastale zbog šuma zapisuju u karte cijena prijelaza (eng. *costmap*) kao stvarne prepreke. Kako bi se to spriječilo, predlaže se uvođenje vremenskog ili probabilističkog filtriranja (npr. Bayesove karte zauzeća), koji uzima u obzir konzistenciju detekcija kroz više uzastopnih kadrova. Potrebno je:

- Analizirati suvremene metode vremenskog ili probabilističkog filtriranja 3D oblaka točaka;
- Analizirati postojeću percepcijsku arhitekturu (vidjeti [diplomski rad](#), poglavlje 4.3.2);

- Predložiti novi ROS2 čvor *perception_filter_node* koji bi pratio pojavljivanje prepreka kroz vrijeme i objavljivao prepreke u *costmap* samo ako su dosljedno detektirane u više uzastopnih kadrova (npr. 3 od zadnjih 5).

CILJ: Cilj projekta je povećati pouzdanost percepcije i smanjiti broj lažnih detekcija kako bi se dobila stabilnija karta cijena prijelaza za sigurno i učinkovito planiranje putanje trkaćeg plovila.

4. Sigurna autentifikacija identiteta i naredbi za udaljene USV operacije pomoću Distributed Ledger Testneta

Autonomno plovilo

Blockchain

PROBLEM: Tradicionalni komunikacijski sustavi između autonomnih plovila i kopnenih postaja oslanjaju se na centralne poslužitelje i povjerenje u mrežnu infrastrukturu. Međutim, komunikacija često nije kriptografski zaštićena, što otvara mogućnost zlonamjernog presretanja ili manipulacije naredbama. Time se direktno ugrožava sigurnost plovila i pouzdanost misije.

OPIS: Osiguranje autentičnosti naredbi i nepromjenjivosti podataka koje plovilo šalje prema kopnenom kontrolnom sustavu ključno je za pouzdano daljinsko upravljanje USV-om. Predlaže se primjena Distributed Ledger Testneta poput *blockchaina* za autentifikaciju naredbi i zaštitu podataka autonomnog plovila. Potrebno je:

- Istražiti postojeću literaturu o primjeni *blockchain* tehnologije u robotici i IoT sustavima, s naglaskom na sigurno potpisivanje i provjeru poruka te nepromjenjivo zapisivanje podataka;
- Postaviti lokalni *blockchain testnet*;
- Implementirati dvije jednostavne skripte ([Python](#), Rust...):
 - *gcs_simulator.py* koji generira i potpisuje poruku (npr. koordinate {x:10, y:20}) pomoću privatnog ključa;
 - *usv_simulator.py* koji prima poruku i provjerava digitalni potpis tako što rekonstruira javni ključ i uspoređuje ga s postojećim popisom odobrenih pošiljatelja (eng. *whitelist*).
- Predložiti kako biste integrirali ovaj sustav autentifikacije unutar postojećeg ROS2 i QGroundControl sustava (vidjeti [diplomski rad](#), poglavlje 4.2.2).

CILJ: Cilj projekta je povećati razinu pouzdanosti i sigurnosti u komunikaciji između USV-a i kontrolnog sustava korištenjem *blockchain* infrastrukture. Tako plovilo može dokazati da svaka naredba dolazi od ovlaštenog izvora i da su podaci koje ono šalje kriptografski zaštićeni i nepromjenjivi.

5. Grafičko sučelje za analizu mehanizama konsenzusa na lokalnoj testnoj mreži

Blockchain

PROBLEM: Praćenje događaja u *blockchain* mreži u stvarnom vremenu, poput dolaska novih blokova ili transakcija, često je teško zbog nedostatka intuitivnih i preglednih vizualnih alata. Bez prikaza dinamike konsenzusa i aktivnosti pojedinih čvorova, teško je analizirati kako mreža reagira na promjene, što otežava razumijevanje, istraživanje i dijagnostiku performansi *blockchain* sustava.

OPIS: Projekt se fokusira na razvoj vizualnog alata za analizu mehanizama konsenzusa u lokalnoj *blockchain* testnoj mreži. Potrebno je:

- Proučiti postojeće alate za vizualizaciju *blockchaina* (npr. tx2viz) i procijeniti njihovu sposobnost intuitivnog prikaza konsenzusnih događaja;
- Na lokalnoj APASLab testnoj mreži postaviti jednostavan web poslužitelj i program na svakom čvoru koji će pretplatničkim modelom pratiti dolazak novih blokova ili transakcija;
- Razviti jednostavnu *single-page* web aplikaciju koja vizualizira rast *blockchaina* u stvarnom vremenu. Svaki novi blok potrebno je prikazati kao novu kutiju povezanu s prethodnom, s osnovnim informacijama poput rudara i broja transakcija.

CILJ: Cilj projekta je razviti intuitivni vizualni alat koji omogućuje praćenje i analizu događaja u *blockchain* mreži u stvarnom vremenu. Ovaj alat omogućit će bolje razumijevanje kako konsenzus funkcionira, kako se blokovi šire kroz mrežu te kako pojedini čvorovi sudjeluju u procesu.

6. Analiza i simulacija novog održivog Proof-of-Work konsenzusnog mehanizma

Blockchain

PROBLEM: Klasični Proof-of-Work (PoW) mehanizam konzumira velike količine energije, generira visoke troškove i ograničava skalabilnost *blockchain* mreža. Kako *blockchain* tehnologija sve više pronalazi primjenu u decentraliziranim aplikacijama, javlja se potreba za razvojem održivih alternativa koje zadržavaju sigurnost PoW-a, ali smanjuju energetske i ekološke otiske.

OPIS: Projekt se fokusira na analizu energetske, troškovne i komunikacijske zahtjeva alternativnih konsenzusnih mehanizama. Potrebno je:

- Istražiti održive PoW alternative, kao što su Proof-of-Useful-Work (PoUW), Proof-of-Space (PoS) ili hibridni modeli;

- Izraditi jednostavnu simulaciju u Pythonu ili Rustu koja uključuje diskretne događaje (ne cijeli *blockchain*) između 4-5 čvorova i modelira rudarenje kako biste usporedili dvije verzije konsenzusa:
 - A)** Klasični PoW: pronalazak *nonce* n gdje $\text{hash}(\text{podaci} + n)$ ima k vodećih nula;
 - B)** Predloženi PoUW: pronalazak rješenja za jednostavan „koristan” problem (npr. mali optimizacijski problem).
- Stvoriti grafički prikaz koji uspoređuje „potrošene” (A) i „korisne” (B) izračune.

CILJ: Cilj projekta je analizirati i kvantitativno usporediti održivost različitih PoW alternativa, s naglaskom na omjer između sigurnosti, energetske učinkovitosti i skalabilnosti.

7. Sustav evidencije pristupa zaštićen lancem blokova

Biometrija

Blockchain

PROBLEM: Tradicionalni sustavi evidencije pristupa (temeljeni na biometriji ili karticama) često nemaju nepromjenjivu i provjerljivu evidenciju događaja. Takvi sustavi mogu biti podložni manipulaciji, brisanju ili izmjeni zapisa o pristupu, što ugrožava sigurnost i integritet sustava.

OPIS: Projekt istražuje primjenu *permissioned blockchain* sustava za sigurno vođenje i provjeru biometrijskih zapisa o pristupu. Sustav bi bilježio svaku autentifikaciju kao transakciju na *blockchainu*, čime se postiže nepromjenjivost, transparentnost i mogućnost revizije. Potrebno je:

- Razviti pametni ugovor (eng. *smart contract*) za pohranu biometrijskih zapisa;
- Izraditi nadzornu ploču (eng. *dashboard*) koja prikazuje povijest pristupa u stvarnom vremenu.

CILJ: Cilj projekta je osigurati trajnu provjerljivost i nepromjenjivost biometrijskih zapisa, čime se povećava sigurnost sustava pristupa i omogućuje transparentna revizija svih događaja u sigurnim objektima.

8. Multimodalna autentifikacija koristeći sliku i zvuk

Biometrija

PROBLEM: Sustavi koji se oslanjaju samo na jedan biometrijski modalitet (npr. lice ili glas) podložni su *spoofing* napadima i pogreškama u uvjetima smanjene vidljivosti ili buke.

OPIS: Projekt se fokusira na razvoj sustava koji kombinira prepoznavanje lica i autentifikaciju glasa pomoću dubokih neuronskih mreža implementiranih u TensorFlowu ili PyTorchu. Sustav treba koristiti multimodalnu fuziju odluka (eng. *decision-level fusion*) kako bi se objedinili rezultati oba modela i postigla veća otpornost na pokušaje lažiranja (*spoofing*) te pouzdanija identifikacija korisnika u stvarnim uvjetima. Potrebno je:

- Implementirati pojedinačne modele za prepoznavanje lica i prepoznavanje glasa;
- Integrirati ih u zajednički autentifikacijski sustav;
- Razviti jednostavno *demo* sučelje koje omogućuje prijavu korisnika pomoću slike i zvuka;
- Provesti evaluaciju usporedbom točnosti, brzine i otpornosti između jednostrukog (unimodalnog) i multimodalnog pristupa, uz analizu kompromisa između performansi i složenosti sustava.

CILJ: Cilj projekta je razviti multimodalni biometrijski sustav autentifikacije koji kombinira lice i glas kako bi se postigla viša razina sigurnosti i robusnosti.

9. Istraživanje state-of-the-art tehnika prepoznavanja lica

Biometrija

PROBLEM: Trenutne *state-of-the-art* metode za prepoznavanja lica razlikuju se po točnosti, robusnosti i efikasnosti u stvarnim uvjetima. Potrebno je sustavno istražiti i usporediti moderne pristupe kako bi se procijenila njihova primjenjivost u praktičnim biometrijskim sustavima, posebno pri varijacijama osvjetljenja, poze i zaklanjanja lica.

OPIS: Projekt se fokusira na istraživanje suvremenih algoritama za prepoznavanje lica i njihovu eksperimentalnu evaluaciju. Potrebno je:

- Istražiti i analizirati nekoliko aktualnih arhitektura, primjerice LVFace 2025, ArcFace, FaceNet ili slične modele, s ciljem razumijevanja njihovih prednosti i ograničenja;
- Implementirati i testirati jedan ili više modela na dostupnim skupovima podataka te evaluirati točnost, robusnost i brzinu izvođenja.

CILJ: Cilj projekta je istražiti, implementirati i evaluirati moderne metode za prepoznavanje lica te usporediti njihove performanse u stvarnim uvjetima. Time se želi postići dublje razumijevanje trenutnog stanja tehnologije (*state-of-the-art*) i pružiti smjernice za budući razvoj učinkovitijih i robusnijih biometrijskih sustava.

10. Optimizacija modela dubokog učenja Vision Transformer za rubne uređaje

Biometrija

PROBLEM: Modeli dubokog učenja, posebno Vision Transformer (ViT) arhitekture, postižu izvrsne rezultate, ali zahtijevaju značajne računalne resurse. To ih čini nepraktičnima za rubne uređaje (eng. *edge devices*) poput Raspberry Pi ili Jetson Nano, gdje su procesorska snaga, memorija i energetska učinkovitost ograničeni.

OPIS: Projekt se fokusira na istraživanje i eksperimentalnu evaluaciju postojećih metoda optimizacije Vision Transformer modela za primjenu na rubnim uređajima. Potrebno je:

- Istražiti tehnike poput *model quantizationa*, *model pruninga*, *model distillationa* te kompaktnih ViT arhitektura (npr. MobileViT, TinyViT);
- Implementirati jednostavnu aplikaciju za prepoznavanje lica u stvarnom vremenu koja koristi optimizirani ViT model i radi na uređaju s ograničenim resursima;
- Provesti testiranje performansi i analizu kompromisa između brzine i točnosti.

CILJ: Cilj projekta je pokazati kako se moderni ViT modeli mogu prilagoditi za biometrijsku autentifikaciju u stvarnom vremenu uz minimalne resurse.

11. Dizajn i treniranje modela multimodalnog biometrijskog prepoznavanja pomoću značajki lica, hoda i izgleda tijela

Biometrija

PROBLEM: Unimodalni sustavi biometrijske identifikacije (npr. samo lice) često ne pružaju dovoljnu točnost u uvjetima promjena izgleda, pokreta ili zaklanjanja.

OPIS: Projekt se fokusira na razvoj naprednog multimodalnog biometrijskog sustava koji integrira tri različite vrste biometrijskih značajki (lice, hod i izgled tijela) u jedinstveni model temeljen na dubokom učenju. Ovakav pristup omogućuje međusobno nadopunjavanje informacija iz različitih izvora, čime se povećava robusnost prepoznavanja u situacijama kada jedan modalitet nije pouzdan (npr. djelomično zaklonjeno lice). Projekt uključuje dizajn modela dubokog učenja koji spaja više biometrijskih obilježja u jedinstvenu fuzijsku mrežu. Treniranje je potrebno provesti na multimodalnim skupovima podataka, uz usporedbu performansi s modelima koji koriste samo jedan modalitet.

CILJ: Cilj projekta je razviti robustan multimodalni biometrijski model koji kombinira više izvora informacija radi postizanja veće točnosti i otpornosti u identifikaciji osoba u stvarnim uvjetima.

12. Procjena sigurnosti multimodalnih biometrijskih sustava pristupa

Biometrija

PROBLEM: Multimodalni biometrijski sustavi, iako sigurniji od jednostrukih, i dalje mogu biti ranjivi na *spoofing* napade (npr. ispisane fotografije, videosnimke, audio reprodukcije) i adversarijalne manipulacije.

OPIS: Potrebno je:

- Dizajnirati i provesti testove sigurnosti (*red-team* evaluacija) za multimodalne biometrijske sustave;
- Analizirati učinke različitih napada, poput reprodukcije slike/glasa i fizičkog prikrivanja, kako bi se procijenila otpornost sustava na pokušaje kompromitiranja;
- Kvantificirati rezultate kroz mjerenje stope lažnog prihvatanja (False Acceptance Rate) pod različitim scenarijima napada;
- Izraditi preporuke za poboljšanje sigurnosti i ojačavanje modela protiv stvarnih prijetnji na temelju dobivenih rezultata.

CILJ: Cilj projekta je procijeniti i kvantitativno mjeriti otpornost multimodalnih biometrijskih sustava na različite vrste napada te razviti preporuke za povećanje sigurnosti i robusnosti sustava.

13. 3D prepoznavanje lica i anti-spoofing

Biometrija

PROBLEM: Klasični 2D sustavi prepoznavanja lica lako se mogu prevariti printanim slikama ili videosnimkama, jer ne prepoznaju dubinsku strukturu lica.

OPIS: Potrebno je:

- Proširiti 2D prepoznavanje lica implementacijom 3D analize pomoću stereo kamere ili dubinskih senzora. Sustav treba rekonstruirati dubinsku mapu lica i omogućiti razlikovanje stvarnih trodimenzionalnih objekata od lažnih prikaza;
- Usporediti točnost i robusnost između 2D i 3D pristupa;

- Provesti testiranje anti-spoofing algoritama u različitim scenarijima kako bi se procijenila učinkovitost 3D komponente u povećanju sigurnosti sustava.

CILJ: Cilj projekta je razviti 3D biometrijski sustav prepoznavanja lica sposoban za detekciju *spoofing* napada i povećati sigurnost sustava autentifikacije u realističnim uvjetima.

14. Prilagodljiva politika pristupa korištenjem strojnog učenja

Biometrija

PROBLEM: Tradicionalne politike pristupa često su statične i ne uzimaju u obzir promjene u obrascima ponašanja korisnika, što može dovesti do kompromitacije sigurnosti ili lažnih alarma.

OPIS: Potrebno je razviti model strojnog učenja koji analizira dnevnik pristupa (vrijeme, učestalost, lokacija, identitet) radi detekcije anomalija u ponašanju korisnika. U slučaju otkrivanja sumnjivog obrasca, sustav treba automatski aktivirati restriktivne mjere (npr. privremeno zaključavanje pristupa) ili slati sigurnosne obavijesti nadležnim korisnicima ili administratorima.

CILJ: Cilj projekta je razviti adaptivni sigurnosni sustav pristupa temeljen na strojnom učenju koji prepoznaje anomalije u ponašanju korisnika i dinamički prilagođava sigurnosne politike, povećavajući time ukupnu otpornost sustava na kompromitaciju.

15. Primjena homomorfne enkripcije za izvođenje aritmetičkih operacija nad šifriranim vektorima

Kriptografija

PROBLEM: Kod klasične enkripcije, podaci se moraju dešifrirati prije nego što se nad njima mogu raditi izračuni, što otvara mogućnost curenja ili zloupotrebe podataka. Homomorfna enkripcija omogućuje izvođenje određenih matematičkih operacija nad šifriranim vrijednostima, bez potrebe za dešifriranjem. Iako je ideja vrlo moćna, u praksi je još uvijek izazovno provoditi složenije operacije zbog velikih računalnih zahtjeva. Također, postoje ograničenja u vrsti operacija koje su moguće u šifriranoj domeni.

OPIS: Projekt se fokusira na istraživanje i eksperimentalnu primjenu homomorfne enkripcije, s naglaskom na TFHE (Fast Fully Homomorphic Encryption over the

Torus) shemu i njezine mogućnosti izvođenja osnovnih i naprednih aritmetičkih operacija nad šifriranim vektorima. Potrebno je:

- Upoznati se s [osnovama](#) homomorfne enkripcije i istražiti moderne potpuno homomorfne pristupe (eng. Fully Homomorphic Encryption, FHE);
- Istražiti suvremene *open-source* TFHE knjižnice poput [Concrete](#) i [TFHE](#) te usporediti njihove mogućnosti i ograničenja.
- Implementirati jednostavne proračune poput zbrajanja i množenja vektora (nad šifriranim vektorima veličine najmanje 128 elemenata), množenja vektora s konstantom, dijeljenja, potenciranja, usporedbe dvaju brojeva (veće/manje), izračuna Euklidske udaljenosti, trigonometrijskih funkcija i sortiranja;
- Analizirati koje su operacije izvedive i s kojim ograničenjima u pogledu točnosti, performansi i vremena izvođenja.

CILJ: Cilj projekta je istražiti i eksperimentalno demonstrirati mogućnosti izvođenja osnovnih i naprednih matematičkih operacija nad šifriranim podacima korištenjem TFHE.

16. Rješavanje CTF izazova i izrada vodiča

Računalna sigurnost

PROBLEM: CTF izazovi su odličan način za uvježbavanje vještina iz računalne sigurnosti, ali mnogi studenti se osjećaju preplavljeno velikom količinom zadataka i nemaju dovoljno vremena da ih sve istraže. Osim toga, iako postoji mnogo *online* materijala, često su nestrukturirani i zbunjujući, što otežava učenje i razumijevanje ključnih tehnika.

OPIS: Ako vas zanima računalna sigurnost i CTF natjecanja, ali do sada niste imali vremena tome se posvetiti, ovo je prilika da se fokusirate na rješavanje izazova iz računalne sigurnosti i izradite vodič za kolege. Potrebno je:

- Odabrati CTF platformu (npr. [pwn.college](#), [platforma.hackultet.hr](#)) i područje unutar računalne sigurnosti koje vas najviše zanima;
- Samostalno riješiti skup problema različitih težina u odabranom području;
- Izraditi izvješće koje dokumentira kako ste riješili zadatke i što ste naučili. Oblikujte ga kao edukativni materijal koji jasno vodi druge studente kroz iste koncepte i izazove. Za svaki je zadatak potrebno opisati ranjivost, *step-by-step write-up*, korištene alate i savjete ili trikove za početnike;
- Kao konačni korak u ovom projektu možete odabrati jednu od dviju opcija:
 - Zamoliti 2-3 kolege da koriste vaš materijal za rješavanje sličnih zadataka kako biste testirali i analizirali njegovu kvalitetu, zabilježili poteškoće i predložili poboljšanja;

- Osmisliti vlastiti CTF zadatak iz odabranog područja.

CILJ: Cilj projekta je analizirati ranjivosti u računalnom sustavu i razviti vlastite strategije rješavanja CTF zadataka. Kao rezultat projekta očekuje se izrada izvješća koje jasno dokumentira vaš pristup rješavanju problema i koje se može koristiti kao edukativni materijal za druge studente.

17. Izrada zadatka za samostalnu vježbu iz robotike

Robotika

PROBLEM: Studenti često uče ROS2 kroz gotove tutorijale, ali takvi primjeri često ne potiču dublje razumijevanje o tome kako sustav zapravo funkcionira.

OPIS: U ovom projektu student osmišljava vlastiti zadatak iz robotike koji drugi studenti mogu koristiti za samostalnu vježbu rada s ROS2 i TurtleBot3 u Gazebo simulaciji ili u stvarnom okruženju. Takav materijal mora poticati druge studente da razmišljaju o tome kako su čvorovi, senzori i algoritmi međusobno povezani i kako ROS2 radi u cjelini. Potrebno je:

- Odabrati hoće li se zadatak rješavati u simuliranom okruženju ili u stvarnom svijetu;
- Osmisliti scenarij zadatka koji se fokusira na percepciju, planiranje, kontrolu ili navigaciju, npr. praćenje linije, izbjegavanje prepreka, detekcija objekata pomoću kamere, prepoznavanje QR kodova, pronalazak cilja;
- Implementirati prototip zadatka u Gazebo ROS2 okruženju, što podrazumijeva barem jedan *world* model i lansirnu datoteku za pokretanje zadatka. Pripremiti barem jedan ROS2 čvor koji predstavlja osnovni *benchmark* primjer rješenja, npr. jednostavan navigacijski algoritam;
- Zamoliti 2-3 kolege da riješe vaš zadatak kako biste testirali i analizirali njegovu kvalitetu, zabilježili poteškoće i predložili poboljšanja;
- Pripremiti dokumentaciju koja jasno definira cilj zadatka i što predstavlja uspješno rješenje. Dokumentacija treba sadržavati opis zadatka, *step-by-step* upute za rješavanje zadatka (koji čvorovi se koriste, koje pakete treba instalirati, kako pokrenuti simulaciju) i očekivani ishod. Predložiti i detaljno opisati kako biste svoj zadatak prilagodili za tri razine težine: lagani, srednji i teški.

CILJ: Cilj projekta je osmisliti i testirati vlastiti zadatak koji se može koristiti kao edukativni materijal za druge studente. Student time uči planirati, strukturirati i dokumentirati edukativni zadatak.

18. Izrada zadatka za timsko natjecanje iz robotike

Robotika

PROBLEM: Natjecanja iz robotike su odličan način da studenti primijene i unaprijede svoje znanje, a pritom se i zabave. No, iza svakog natjecanja stoji kvalitetno osmišljen zadatak koji mora biti izazovan, jasan i izvediv, što nije trivijalno za pripremiti.

OPIS: Zadatak projekta je osmisliti i prototipirati izazov koji bi se mogao koristiti na budućem studentskom natjecanju iz robotike s TurtleBot3 robotima. Potrebno je:

- Odabrati hoće li se natjecanje izvoditi u simuliranom okruženju ili u stvarnom svijetu;
- Osmisliti scenarij zadatka koji kombinira elemente percepcije, planiranja, kontrole i navigacije, npr. dostava paketa, pronalazak cilja, izbjegavanje prepreka, prepoznavanje objekata, timsko natjecanje više robota;
- Implementirati prototip zadatka u Gazebo ROS2 okruženju, što podrazumijeva barem jedan *world* model i lansirnu datoteku za pokretanje zadatka. Pripremiti barem jedan ROS2 čvor koji predstavlja osnovni *benchmark* primjer rješenja, npr. jednostavan navigacijski algoritam;
- Testirati zadatak i osigurati da se može reproducirati na drugom računalu;
- Pripremiti dokumentaciju koja opisuje svrhu natjecanja, pravila, tijek zadatka, način bodovanja i rezultate testiranja te opisati što bi se moglo unaprijediti s natjecateljskog aspekta.

CILJ: Cilj projekta je razviti sposobnost strukturiranja natjecanja i dizajniranja kompleksnog zadatka iz robotike te razumjeti što čini zadatak zanimljivim i izvedivim.