VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

PRIMERJALNA ANALIZA MOBILNIH SISTEMOV ZA TAKTIČNO VODENJE: ATAK-CIV IN OSMAND Z VIDIKA FUNKCIONALNOSTI, MODULARNOSTI IN KIBERNETSKE ZAŠČITE

Kandidat: Fabian Moharić

Vrsta študija: študent izrednega študija

Študijski program: Računalništvo

Mentor predavatelj: mag. Ervin Schaff

Mentor v podjetju: Zoltan Sep, univ. dipl. inž. in rač.

Lektor: Andreja Golob, prof. slov. jez.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani/a Fabian Moharić, sem avtor/ica diplomskega dela z naslovom Primerjalna analiza mobilnih sistemov za taktično vodenje: ATAK-CIV in OsmAnd z vidika funkcionalnosti, modularnosti in kibernetske zaščite, ki sem ga napisal/a pod mentorstvom mag. Ervin Schaff.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel/a, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, september 2025 Podpis študenta:

ZAHVALA

Iskrena zahvala gre vsem, ki so me na moji študijski poti podpirali, spodbujali in mi omogočili, da sem uspešno zaključil to pomembno poglavje.

Zahvaljujem se mentorju predavatelju, mag. Ervinu Schaffu, za strokovno podporo, potrpežljivost ter jasna in konstruktivna usmerjanja v procesu priprave diplomske naloge. Njegova odzivnost in razumevanje sta mi omogočila, da sem kljub občasnim oviram ohranil jasno usmeritev in motivacijo.

Posebna zahvala gre mentorju iz podjetja, g. Zoltanu Sepu, univ. dipl. inž. rač., za pripravljenost prevzeti formalno mentorsko vlogo ter za podporo in razumevanje, ki mi veliko pomenita.

Zahvala gre tudi sodelavcem na mednarodni misiji, ki so me v času službene odsotnosti spodbujali pri študiju in mi pomagali ohraniti zagon za zaključek naloge, kljub zahtevnim delovnim okoliščinam.

Iskrena hvala gre tudi moji družini, ki mi je ves čas stala ob strani, me spodbujala in mi nudila moralno oporo pri pisanju diplomske naloge. Vaša prisotnost, potrpežljivost in zaupanje vame so mi dali moč, da sem vztrajal do konca.

Zahvaljujem se Ministrstvu za obrambo Republike Slovenije za podporo v okviru pogodbe o sofinanciranju študija ter za razumevanje in omogočanje usklajevanja službenih in študijskih obveznosti.

Nenazadnje pa se zahvaljujem tudi vsem predavateljem, strokovnim sodelavcem in tistim, ki so mi s svojim znanjem, spodbudami ali zgledom pomagali na tej poti.

POVZETEK

Diplomska naloga obravnava primerjalno študijo dveh odprtokodnih mobilnih aplikacij za situacijsko zavedanje: Android Team Awareness Kit – Civil (ATAK-CIV) in Open Source Map Automated Navigation Directions (OsmAnd). Gre za aplikaciji, ki služita orientaciji na terenu, prikazu prostorskih informacij ter podpori odločanju, pri čemer vsaka izhaja iz drugačnega razvojnega okolja in ciljne skupine uporabnikov. ATAK-CIV je prvotno razvit za vojaške potrebe in taktično rabo, medtem ko je OsmAnd zasnovan kot civilna navigacijska aplikacija, temelječa na odprtokodnem kartografskem projektu OpenStreetMap.

Cilj naloge je ugotoviti, katera izmed teh dveh platform je primernejša za uporabo v varnostnem oziroma taktičnem okolju, kjer so zanesljivost, razširljivost in zaščita informacij ključni dejavniki. V ta namen naloga temelji na štirih raziskovalnih hipotezah, ki se nanašajo na: enostavnost in modularnost razvoja vtičnikov, primernost sistema za premikanje in usklajevanje enot na terenu, stopnjo zaupanja med uporabniki, ter stopnjo kibernetske zaščite in varnosti aplikacij. V okviru raziskave sta bila razvita osnovna vtičnika za obe platformi – Time-in-Zone Monitor – ki merita čas, preživet znotraj določenega območja. To je omogočilo empirično primerjavo razvojnega procesa, uporabniškega vmesnika, dostopa do sistemskih komponent in kompleksnosti integracije. Uporabljene so bile kombinirane raziskovalne metode – kvalitativna analiza dokumentacije, lastna uporabniška izkušnja avtorja (v okviru šestmesečne uporabe ATAK-CIV na mednarodni misiji), ter kvantitativna ocena funkcionalnosti in varnostnih elementov.

Rezultati raziskave kažejo, da ATAK-CIV ponuja bolj robustno in modularno infrastrukturo, ki omogoča razvoj naprednih in varnostno zanesljivih vtičnikov, medtem ko je OsmAnd primernejši za osnovno civilno uporabo. ATAK-CIV se izkaže kot bolj primeren za delovanje v taktičnem okolju, saj podpira vojaške standarde označevanja, šifrirano komunikacijo, ter delovanje v izoliranih omrežjih brez dostopa do interneta. OsmAnd pa izstopa z uporabnostjo, enostavnostjo distribucije in delovanjem brez povezave, vendar ne nudi zadostne stopnje integracije in nadzora za operativno uporabo v kriznih razmerah.

Ključne besede: *situacijsko zavedanje, ATAK-CIV, OsmAnd, vtičniki, odprtokodna programska oprema, taktična komunikacija, kibernetska zaščita, krizno upravljanje, primerjalna analiza.*

ABSTRACT

Comparative analysis of mobile systems for tactical command and control: Atak-Civ and Osmand from the perspective of functionality, modularity, and cyber security

This thesis presents a comparative study of two open-source mobile applications for situational awareness: Android Team Awareness Kit – Civil (ATAK-CIV) and Open Source Map Automated Navigation Directions (OsmAnd). Both platforms are designed for field orientation, spatial data visualization, and real-time support for decision-making, yet they originate from vastly different environments. ATAK-CIV was developed for military and tactical use, while OsmAnd was created for civilian navigation based on the open-source OpenStreetMap project.

The main objective of the thesis is to determine which of the two platforms is more suitable for use in security or tactical environments, where reliability, scalability, and information security are of critical importance. The analysis is based on four research hypotheses, focusing on: ease and modularity of plugin development, operational usability in tactical movement and coordination, user trust in the system, and level of cybersecurity provided by the platforms.

As part of the research, a custom plugin called Time-in-Zone Monitor was developed for both platforms to measure the amount of time spent within a designated zone. This enabled an empirical comparison of the development process, access to system-level functions, and user interface design. A combination of qualitative methods (documentation analysis, user experience from a six-month deployment of ATAK-CIV during an international mission) and quantitative evaluation (functionality comparison, system structure, security mechanisms) was used.

The findings demonstrate that ATAK-CIV provides a more robust and modular infrastructure for the development of secure, advanced plugins. OsmAnd, in contrast, proves to be more suitable for basic civilian use, thanks to its ease of use, offline functionality, and wide community support. However, it lacks the necessary system integration and control required for specialized field operations.

Keywords: *situational awareness, ATAK-CIV, OsmAnd, plugin development, open-source software, tactical communication, cybersecurity, crisis management, comparative analysi*

KAZALO VSEBINE

1 UVOD 10

1.1 Opis področja in opredelitve problema 10
1.2 Namen, cilji in osnovne trditve 11
1.3 Predpostavke in omejitve 12
1.4 Uporabljene raziskovalne metode 13

2 TEORETIČNA OSNOVA: MOBILNI TAKTIČNI SISTEMI 15

2.1 Predstavitev: ATAK-CIV 15
2.1.1 Kaj je ATAK-CIV? 15
2.1.2 Glavne značilnosti ATAK-CIV 15
2.1.3 Varnostne značilnosti 16
2.1.4 Orodna vrstica 18
2.2 Predstavitev OsmAnd 27
2.2.1 Kaj je OsmAnd? 27
2.2.2 Glavne značilnosti OsmAnd 27
2.2.3 Varnostne značilnosti 28

3 PRIMERJALNA ANALIZA (FUNKCIONALNOST, MODULARNOST IN UPORABNOST) 41

3.1 Modularnost in razvoj vtičnikov 41
3.2 Uporabnost v taktičnem okolju 46
3.3 Zaupanje in varnostna ocena 47
3.3.1 Splošno 47
3.3.2 Primerjava 49
3.4 Kibernetska zaščita 50
3.4.1 Splošno 50
3.4.2 Primerjava 53

4 OPIS RAZVITEGA VTIČNIKA »TIME-IN-ZONE MONITOR« 55

4.1 Namen vtičnika 55
4.2 Ključne funkcije 55
4.3 Scenarij uporabe 55
4.4 Načrt razvoja vtičnika 56
4.4.1 ATAK-CIV (Java, Android) 56
4.4.2 OsmAnd (Java, OsmAndPlugin) 58
4.5 Rezultat izvorne kode 60

5 PREDLOGI IN MOŽNOSTI NADGRADNJE 61

5.1 PREDLOGI IN MOŽNOSTI NADGRADNJE 61

5.2 POVZETEK DOSEŽENIH CILJEV 61

5.3 POTRDITEV ALI OVRŽBA HIPOTEZ 62

5.3.1 H1: Razvoj vtičnika za sistem ATAK-CIV je enostavnejši in bolj modularen kot v sistemu OsmAnd. 62

5.3.2 H2: ATAK-CIV je v primerjavi z OsmAnd primernejši za taktično premikanje in terensko vodenje enot. 63

5.3.3 H3: Ocena varnosti in zaupanja je boljša pri ATAK-CIV kot pri OsmAnd. 63

5.3.4 H4: ATAK nudi višjo raven kibernetske zaščite kot OsmAnd. 63

5.4 KLJUČNE UGOTOVITVE RAZISKAVE 64

5.5 PREDLOGI ZA NADGRADNJO 64

6 SKLEP 65

7 VIRI IN LITERATURA 67

KAZALO SLIK

SLIKA 1 IZGLED ATAK-CIV-A 17

SLIKA 2 UPRAVLJANJE SKUPIN 18

SLIKA 3 UPRAVLJANJE SLOJEV 19

SLIKA 4 UPRAVLJANJE KARTOGRAFSKIH VIROV 20

SLIKA 5 MENJAVA KARTOGRAFSKEGA VIRA 20

SLIKA 6 OZNAČEVANJE TOČK 21

SLIKA 7 USMERJANJE LOKACIJE 22

SLIKA 8 ORODJA ZA UPRAVLJANJE 23

SLIKA 9 ORODJA ZA UPRAVLJANJE 2 24

SLIKA 10 ORODJA ZA UPRAVLJANJE 3 24

SLIKA 11 NASTAVITVE ATAK-CIV 25

SLIKA 12 NASTAVITVE ATAK-CIV 2 26

SLIKA 13 IZGLED OSMAND 29

SLIKA 14 UPRAVLJANJE APLIKACIJE 30

SLIKA 15 NASTAVITVE ZEMLJEVIDA 31

SLIKA 16 PRILJUBLJENE TOČKE IN SHRANJENE POTI 32

SLIKA 17 ZEMLJEVIDI IN DRUGI VIRI 33

SLIKA 18 OZNAKE ZEMLJEVIDA 34

SLIKA 19 NASVETI ZA POT 35

SLIKA 20 NAVIGACIJA 36

SLIKA 21 NAČRTUJ POT 37

SLIKA 22 NASTAVITVE ZASLONA 38
SLIKA 23 VTIČNIKI 39
SLIKA 24 NASTAVITVE 40
SLIKA 25 DIAGRAM POTEKA ATAK-CIV 56
SLIKA 26 VTIČNIK V ATAK-CIV 57
SLIKA 27 DIAGRAM POTEKA OSMAND 58
SLIKA 28 PRVI DEL KODE 59
SLIKA 29 DRUGI DEL KODE 59
SLIKA 30 REZULTAT IZVORNE KODE VTIČNIKOV 60

KAZALO TABEL

TABELA 1 TABELA PRIMERJALNE ANALIZE 54

Slovar strokovnih izrazov in kratic

ATAK-CIV – Android Team Awareness Kit-Civil

OsmAnd – Open source map and navigation app

Plugin - Vtičnik

UAV – Unnamed Aerial Vehicle

GPS – Global Positioning System

SDK – Software Development Kit

Repozitorji - prostor na strežniku za shranjevanje in dostopanje do dokumentov, datotek

Online – V omrežju

Offline – Brez omrežja, lokalno

Virtualizacija – Postopek ustvarjanja navideznih strežnikov

Avtentikacija – Postopek, kjer se računalnik prepriča o identifikaciji uporabnika

Geofence – Geografsko ograjevanje

OsmAnd source build in plugin framework – Ogrodje vtičnikov vgrajeno v izvorno kodo OsmAnd

Odprtokodnost – Tip izvorne kode programa, aplikacije ali podobno, ki je dostopna vsem

API – Application Programming Interface, je množica rutin, protokolov in orodij za izgradnjo programske opreme in aplikacij

Intents – Sistem Intent skrbi za komunikacijo med komponentami in programskimi modeli, ki temeljijo na njem in se osredotočajo na cilje uporabnikov ali sistemov višje ravni in ne natančne postopke

Mesh Omrežje – Sistem več povezanih vozlišč, ki skupaj prenašajo podatke in ustvarjajo enotno omrežje

VPN – Virtual Private Network, navidezno zasebno omrežje

UI – User Interface, uporabniški vmesnik

1 UVOD

1.1 Opis področja in opredelitve problema

V sodobnem svetu, kjer informacijska tehnologija hitro napreduje, mobilne rešitve za situacijsko zavedanje postajajo ključne pri odločanju v varnostnem, obrambnem in kriznem sektorju. Učinkovita orientacija, vizualizacija podatkov in koordinacija na terenu so temelj odzivnosti in varnosti.

Pričujoča diplomska naloga primerja dve rešitvi – **ATAK-CIV** (Android Team Awareness Kit – Civil) in **OsmAnd** (OpenStreetMap Automated Navigation Directions). ATAK-CIV, razvit za ameriške obrambne sile, danes kot odprtokodna aplikacija omogoča kartografijo, deljenje lokacij v realnem času, šifrirano komunikacijo in razvoj vtičnikov, prilagojenih taktičnim okoljem. OsmAnd pa izhaja iz civilne sfere, s poudarkom na navigaciji, odprtih kartah, turistični uporabi in delovanju brez internetne povezave. Čeprav izhajata iz različnih kontekstov, sta uporabni tudi pri odzivanju na naravne nesreče, civilni zaščiti in logistični podpori.

Namen naloge je primerjalna analiza obeh platform z vidika funkcionalnosti, razvoja vtičnikov, kibernetske zaščite in zaupanja uporabnikov. V okviru raziskave bo izdelan tudi osnovni vtičnik za vsako aplikacijo, kar omogoča neposredno oceno fleksibilnosti in zahtevnosti razvoja. Potreba po tovrstni analizi izhaja iz prakse, kjer so razpoložljivost, varnost in zanesljivost digitalnih orodij pogosto ključni.

Odprtokodne rešitve, kot sta ATAK-CIV in OsmAnd, prinašajo prednosti prilagodljivosti in neodvisnosti od licenc, a tudi vprašanja o stabilnosti in varnosti. Primerjava med njima je zato pomembna tako z vidika razvoja programske opreme kot tudi informacijske varnosti.

Naloga združuje kvalitativni in kvantitativni pristop ter povezuje teorijo s prakso, saj avtor črpa iz izkušenj v varnostnem sektorju. Tako ne gre zgolj za tehnično primerjavo, temveč za širši pogled na to, kako odprtokodne platforme lahko podpirajo odločanje, varnost in koordinacijo na operativni ravni ter predstavljajo alternativo komercialnim rešitvam.

1.2 Namen, cilji in osnovne trditve

Namen je primerjati mobilna sistem ATAK-CIV in OsmAnd glede na taktično uporabo, varnost in razširljivost. Oceniti primernost za uporabo v obrambnem in civilno-zaščitnem okolju. Analizirati možnosti razvoja lastnega vtičnika za posamezno platformo ter predlagati izboljšave ali priporočila za uporabo odprtokodnih rešitev v kriznem odzivanju.

Hipoteze predstavljajo temeljno usmeritev raziskovalnega dela in izhajajo neposredno iz raziskovalnih vprašanj, zastavljenih v uvodnem delu naloge. Z njihovo pomočjo želim preveriti ključne razlike med mobilnima platformama ATAK-CIV in OsmAnd, zlasti z vidika njihove funkcionalne ustreznosti, razširljivosti in varnostnih značilnosti v taktičnih okoljih. Vsaka hipoteza se nanaša na specifičen vidik sistema, ki bo v nadaljevanju predmet primerjalne analize.

H1: Razvoj vtičnika za sistem ATAK-CIV je enostavnejši in bolj modularen kot v sistemu OsmAnd

Namen te hipoteze je nanašanje na razvojno okolje ter razpoložljivost orodij, ki jih ponuja omenjen sistem. ATAK-CIV je zasnovan kot taktična platforma z uradnim SDK-jem, s čimer ponuja podporo razvijalcem ter bolj strukturirano integracijo dodatkov. Kljub temu, da je OsmAnd odprtokoden, ne vsebuje enako obsežnih orodij ali dokumentacije za razvoj razširitev, kar lahko vpliva na kompleksnost implementacije.

H2: Sistem ATAK-CIV je v primerjavi z OsmAnd primernejši za taktično premikanje in terensko vodenje enot

Izhaja iz namenskega razvoja ATAK-CIV, ki je bil od začetka načrtovan za podporo premikanju in vodenju enot v realnem času, z naprednimi možnostmi sledenja, sodelovanja in koordiniranja. OsmAnd se osredotoča predvsem na navigacijo z možnostjo nadgradnje za prikaz vremena, parkiranja, topografije vendar je v taktičnem smislu omejen.

H3: Ocena varnosti in zaupanja je boljša pri ATAK-CIV kot pri OsmAnd

Pod oceno varnosti in zaupanja razumemo kombinacijo percepcije uporabnikov, zgodovinskih podatkov o uporabi v varnostnem sektorju ter implementiranih zaščitnih mehanizmov. ATAK-CIV je bil razvit z mislijo na vojaško uporabo, zato je njegova zasnova bolj povezana z zanesljivostjo, robustnostjo in skladnostjo z varnostnimi politikami. OsmAnd kot civilna rešitev ter aspektov praviloma ne pokriva v enaki meri.

H4: ATAK nudi višjo raven kibernetske zaščite kot OsmAnd

Kibernetska zaščita vključuje protokole šifriranja, možnosti delovanja v zaprtih omrežjih, preverjanje pristnosti in nadzor nad komunikacijskimi kanali. ATAK-CIV za šifriranje uporablja TLS (Transport Layer Security- Prenosni sloj zaščite), ki omogoča povezovanje preko taktičnih omrežij ter integracijo s sistemi z višjo stopnjo varnostnih zahtev.

OsmAnd teh možnosti v osnovni različici ne ponuja, kar bo predmet empirične in tehnične analize.

1.3 Predpostavke in omejitve

Raziskava temelji na primerjavi dveh odprtokodnih sistemov za situacijsko zavedanje, ATAK-CIV in OsmAnd, s poudarkom na razvoju in delovanju osnovnega vtičnika Time-in-Zone Monitor za merjenje časa znotraj definiranega območja.

Predpostavke raziskave:

- Oba sistema sta bila testirana v najnovejših javno dostopnih različicah, z uradnimi ali preverjenimi repozitoriji.
- Vtičnika sta bila razvita v Android Studiu in testirana na isti napravi.
- Območja za testiranje so bila definirana ročno (poligon, GPX) in z gibanjem uporabnika.
- Analiza uporabnosti se je omejila na osnovne funkcije, brez zunanjih senzorjev ali infrastrukture.

Omejitve raziskave:

• ATAK-CIV ne omogoča dostopa do vseh vojaških funkcij.

• OsmAnd ne podpira neposredne integracije vtičnikov, zato je bil uporabljen zunanji pristop.

• Realno taktično testiranje je bilo omejeno; del izkušenj temelji na simulacijah in praksi avtorja.

• Merjenje časa ne vključuje okoliščin, kot so izguba GPS signala ali večuporabniška koordinacija.

• Kibernetska varnost je bila ocenjena na podlagi dokumentacije, brez neodvisnega testiranja.

1.4 Uporabljene raziskovalne metode

Za raziskavo je bil uporabljen kombiniran metodološki pristop, ki združuje kvalitativne in kvantitativne metode. Tak okvir omogoča celostno oceno sistemov ATAK-CIV in OsmAnd z vidika uporabnosti, zmogljivosti, razširljivosti in varnosti.

Kvalitativni pristop zajema analizo uporabniške izkušnje, zasnove vmesnika, odzivnosti ter dokumentacije in razvojne podpore. Kvantitativni pristop pa omogoča številčno primerjavo funkcij, varnostnih mehanizmov in odzivnosti v realnih pogojih.

V nadaljevanju sta zato predstavljeni obe komponenti: kvalitativna, ki temelji na praktičnem testiranju in dokumentaciji, ter kvantitativna, usmerjena v sistematično merjenje ključnih parametrov.

Kvalitativna metodologija

V kvalitativnem delu raziskave so bile uporabljene metode za poglobljeno razumevanje delovanja, uporabnosti in razširljivosti sistemov ATAK-CIV in OsmAnd. Namen ni bil le opis funkcij, temveč tudi presoja njihove praktične vrednosti v taktičnih in civilnih scenarijih.

Pomemben prispevek k raziskavi predstavlja avtorjeva lastna uporabniška izkušnja z ATAK-CIV, pridobljena med šestmesečno mednarodno misijo. Ta je dopolnila analizo dokumentacije in simulacij ter omogočila vpogled v dejanske prednosti in izzive sistema.

Analiza dokumentacije

Najprej je bila izvedena analiza dokumentacije obeh platform, ki je zajemala uradne vire (navodila, SDK, GitHub repozitorije) ter neodvisne prispevke (strokovni članki, forumi, vodiči skupnosti). Pri ATAK-CIV je bil poudarek na SDK dokumentaciji, arhitekturi vtičnikov in varnostnih mehanizmih, pri OsmAnd pa na priročnikih za konfiguracijo, dodajanje slojev in razvojnih smernicah. Namen analize je bil oceniti raven tehnične dokumentiranosti ter enostavnost vključevanja uporabnikov in razvijalcev v uporabo ter prilagoditev sistema.

Presoja uporabniške izkušnje

Kvalitativna analiza je vključevala praktični preizkus obeh aplikacij v realnem in simuliranem taktičnem okolju. Testiranje je potekalo na enakih napravah z identično konfiguracijo, kar je omogočilo primerljivo presojo. Spremljani so bili ključni vidiki uporabniške izkušnje: odzivnost, preglednost vmesnika, logičnost menijev, intuitivnost navigacije ter zanesljivost pri nalogah, kot so označevanje točk, sledenje poti in prikaz zemljevidov. Posebna pozornost je bila namenjena tudi učni krivulji – hitrosti razumevanja delovanja brez dodatnega usposabljanja – ter dostopnosti pomoči in prilagodljivosti vmesnika.

Testiranje aplikacij

Dodatno je bilo izvedeno ciljno testiranje s poudarkom na različnih tipih zemljevidov (online, offline, topografski sloji) ter preverjanju stabilnosti v različnih geografskih okoljih. Preizkušene so bile možnosti konfiguracije komunikacijskih poti, deljenje lokacije, izvoz/uvoz podatkov (GPX, KML), uporaba dodatkov ter delovanje v načinu brez povezave.

Kvantitativna metodologija

Kvantitativni del raziskave se je osredotočil na merljivo primerjavo značilnosti obeh sistemov, da bi bila presoja čim bolj objektivna.

Primerjava funkcionalnosti:

Deljenje lokacije v realnem času, podpora slojem (karte, POI, GPX), razširljivost z dodatki, konfiguracija taktičnih podatkov ter orodja za označevanje, risanje in načrtovanje poti.

Ocena varnostnih parametrov: šifriranje podatkov (npr. TLS v ATAK-CIV), preverjanje identitete, delovanje offline, nadzor dostopa in vloge ter integracija s strežniki (TAKServer, LAN). Vsak vidik je bil ocenjen po prisotnosti, zanesljivosti in stopnji integracije.

Analiza odzivnosti in modulov: merjen je bil čas odziva na vnos podatkov (koordinate, območja), hitrost nalaganja modulov in vtičnikov, stabilnost pri dolgotrajni rabi ter zmogljivost pri intenzivni uporabi.

Takšen kombiniran pristop je omogočil celostno oceno ATAK-CIV in OsmAnd z vidika uporabnosti, varnosti in tehnične zmogljivosti**.**

2 TEORETIČNA OSNOVA: MOBILNI TAKTIČNI SISTEMI

2.1 Predstavitev: ATAK-CIV

2.1.1 Kaj je ATAK-CIV?

ATAK-CIV (Android Team Awareness Kit – Civilian Use) je odprtokodna verzija mobilne aplikacije ATAK, prvotno razvite za ameriške oborožene sile, danes pa dostopne tudi širšemu obsegu civilnih in varnostnih uporabnikov. Gre za kompleksno geografsko-informacijsko platformo, zasnovano za prikaz okolja, navigacijo, sodelovanje ekip ter deljenje podatkov v realnem času (ATAK, 2019)

2.1.2 Glavne značilnosti ATAK-CIV

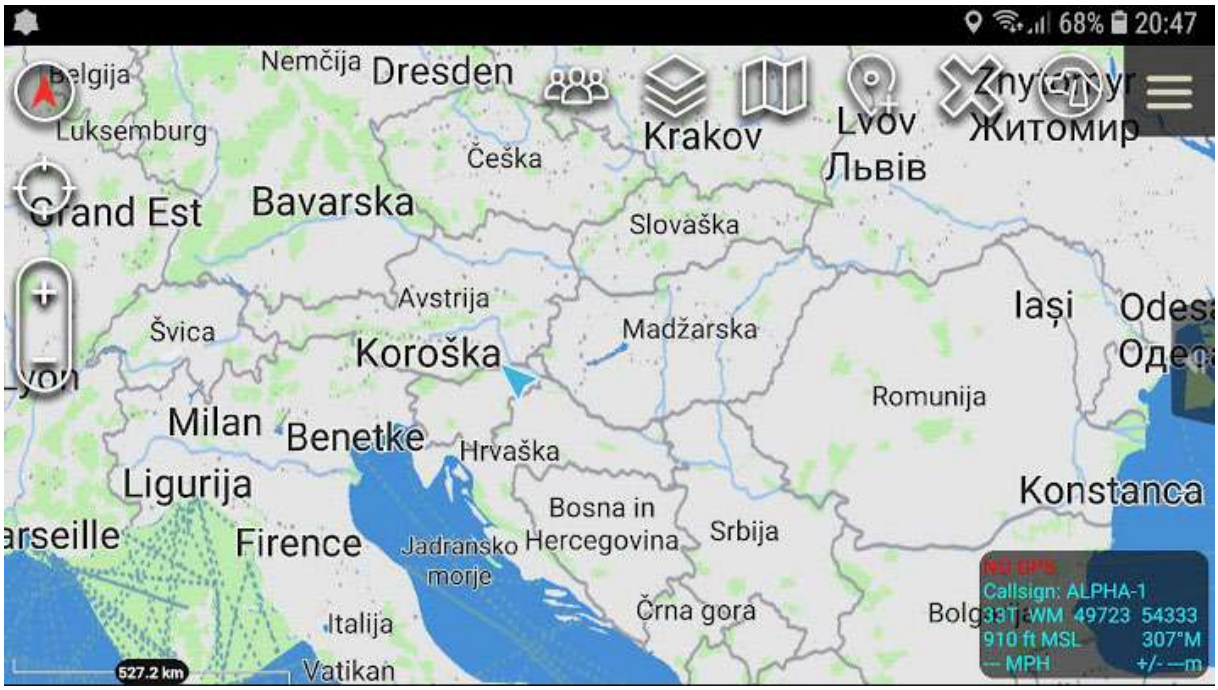
- **Navigacija in prostorska predstavitev:** podpira spletne in lokalne karte prav tako tudi karte z visokimi ločljivostmi (<1cm), hitro vizualizacijo in različne formate (GPX, KML, KMZ…)
- **Sodelovanje ekip:** omogoča delitev lokacije, označbe točk, skupno risanje po zemljevidu ter klepet in izmenjavo datotek (zvočne ali slikovne)
- **Modularnost preko vtičnikov:** omogoča razvoj dodatkov- vtičnikov; ki razširijo funkcionalnost glede na specifične operativne potrebe
- **Merilna orodja in taktika:** vključuje orodje za merjenje razdalj, geografskih izmerkov, predelitev območij z aktivacijskimi sprožilci, analiza terena, načrtovanje poti ter nadzor nad višinskimi profili
- **Varnostna in komunikacijska integracija:** vključuje funkcije za šifriranje (TLS), timske opozorilne signale in integracijo z radijskimi sistemi preko vtičnikov

2.1.3 Varnostne značilnosti

ATAK-CIV, kot civilna različica vojaško razvitega sistema ATAK, ohranja pomembne varnostne komponente, ki so zasnovane za delovanje v potencialno nevarnih in občutljivih operativnih okoljih. Čeprav različica CIV ne vključuje vseh zaupnih ali vojaško specifičnih funkcij (zaradi omejitev izvoza in zaupnosti), vseeno ponuja več kibernetskih varnostnih mehanizmov, ki presegajo običajne civilne navigacijske aplikacije.

2.1.3.1 Glavne varnostne značilnosti

- **TLS (*Transport Layer Security- Plast prenosa in zaščite*):** uporablja šifriranje TLS za zaščito omrežne komunikacije med napravami, s čimer zagotavlja zaupnost prenosa podatkov (npr. lokacij, sporočil ali koordinat)
- **Podpora za zaprta omrežja:** sistem lahko deluje popolnoma brez omrežja z uporabo lokalnih strežnikov (npr. TAK Server) ali neposredne naprava-na-napravo povezave (Wi-Fi Direct ali Bluetooth), kar je ključno za operacije v varovanih območjih ali brez infrastrukture
- **Omejena komunikacija in nadzor dostopa:** sistem omogoča nadzor nad tem, kdo dostopa do omrežja in katere informacije prejema, s čimer se zmanjšuje tveganje za podatkovne vdore ali zlonamerne vstopne točke
- **Integracija z varnostno certificiranimi strežniki:** Organizacije lahko ATAK-Civ povežejo z varnostno upravljalnim TAK strežnikom, ki omogoča centralizirano upravljanje uporabnikov, nadzor nad pretočnostjo informacij in dodatne varnostne protokole
- **Kriptografska podpora prek vmesnikov:** Naprednejše funkcije šifriranja in identifikacije se lahko vgradijo s pomočjo namenskih vtičnikov, razvitih s pomočjo ATAK SDK
- **Zaznavanje in nadzor lokacijskih podatkov:** omogoča nadzor nad lokacijo, kdo vidi uporabnikovo lokacijo in možnost onemogočanja deljenja v občutljivih situacijah



Slika 1 Izgled ATAK-CIV-a

Vir: Lastni vir

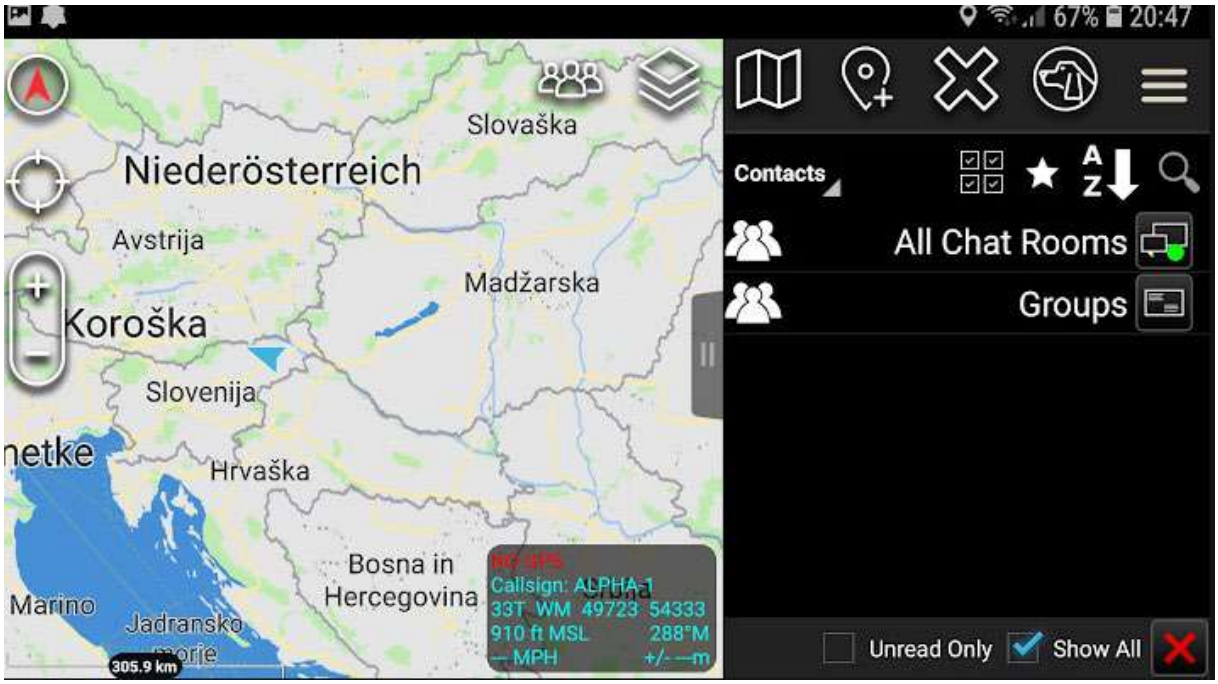
Na tej sliki je prikazan uporabniški vmesnik aplikacije ATAK-CIV, natančneje glavni pogled na zemljevid, kot ga vidi uporabnik na Android napravi. Slika vključuje več ključnih elementov, ki so značilni za ATAK.

V nadaljevanju je predstavljena orodna vrstica, ki je prikazana zgoraj in sicer kompas (levo), desno pa upravljanje skupin, upravljanje slojev, upravljanje lokacije, nastavitve orodij ter vtičnikov in glavni meni.

Na levi strani pod kompas ikono se nahaja tudi možnost zaklepa lokacije in povečanje ali zmanjšanje pogleda. Spodaj v levem kotu pa je razvidno merilo zemljevida oz. obseg prikazane regije v tem primeru 527,2 km.

V spodnjem desnem kotu aplikacije so zraven klicnega znaka prikazani ostali ključni navigacijski podatki, kot so smer gibanja uporabnika (npr. 307° M, kar pomeni 307 stopinj glede na magnetni sever), trenutna višina nad morsko gladino, geografske koordinate in natančnost GPS signala (izražena kot odstopanje v metrih).

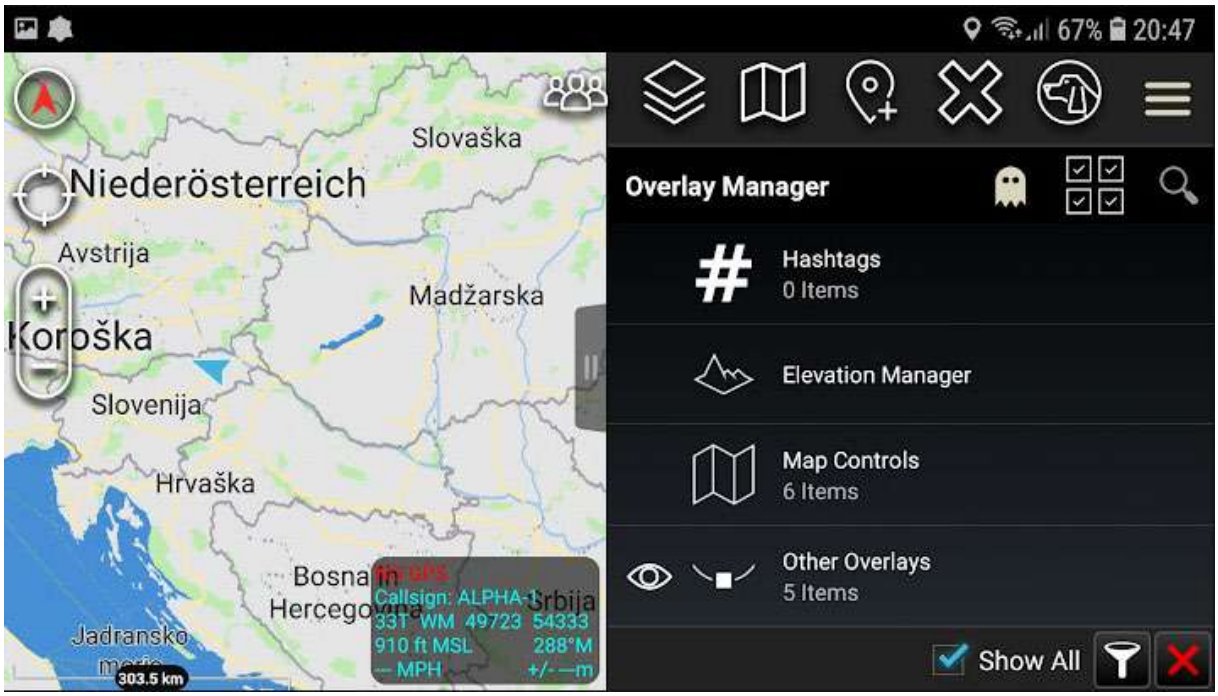
2.1.4 Orodna vrstica



Slika 2 Upravljanje skupin

Vir: Lastni vir

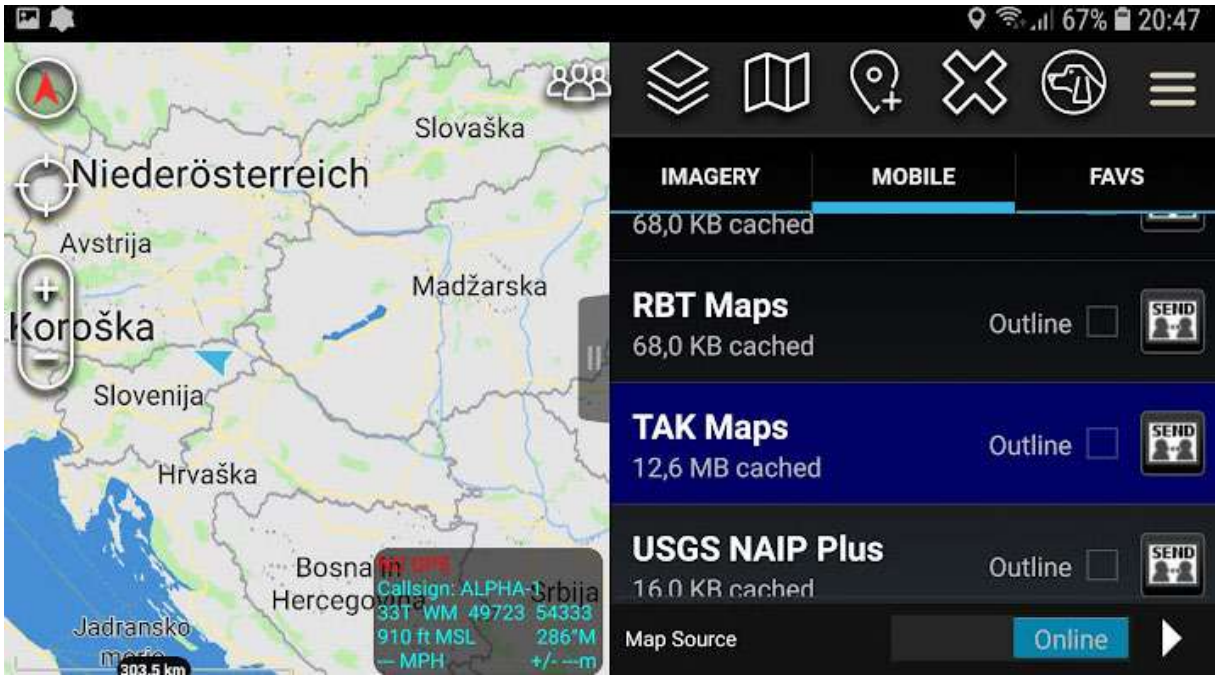
Tukaj je prikazano upravljanje skupin in klepetalnic, kar omogoča koordinacijo enot in timsko komunikacijo v realnem času. Možnost je razvrščanja ali označevanja najljubših skupin po abecedi. Prav tako lahko izberemo prikaz vseh sporočil ali pa samo tiste, ki še niso bile prebrane.



Slika 3 Upravljanje slojev

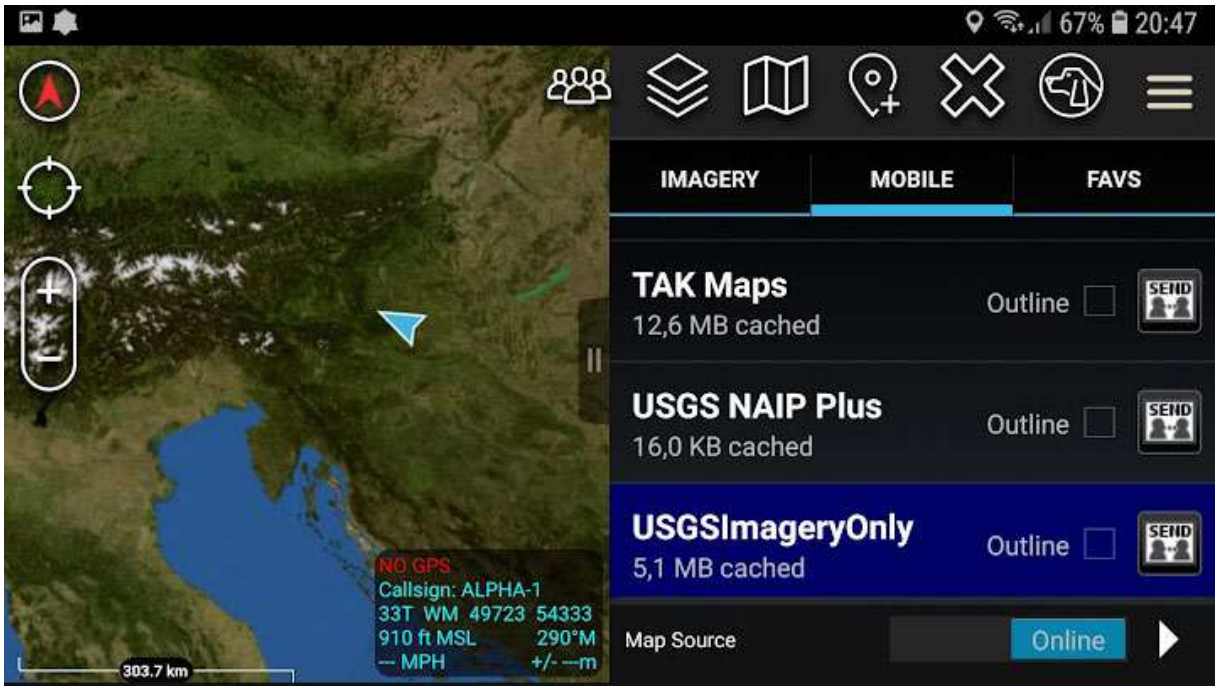
Vir: Lastni vir

Na tej sliki je prikazan ključni element aplikacije in sicer upravljanje slojev. Omogoča virtualizacijo, dodajanje in nadzor podatkovnih slojev na zemljevidu, kar je ena izmed osrednjih funkcij taktično-situacijskega vodenja.



Slika 4 Upravljanje kartografskih virov

Vir: Lastni vir



Slika 5 Menjava kartografskega vira

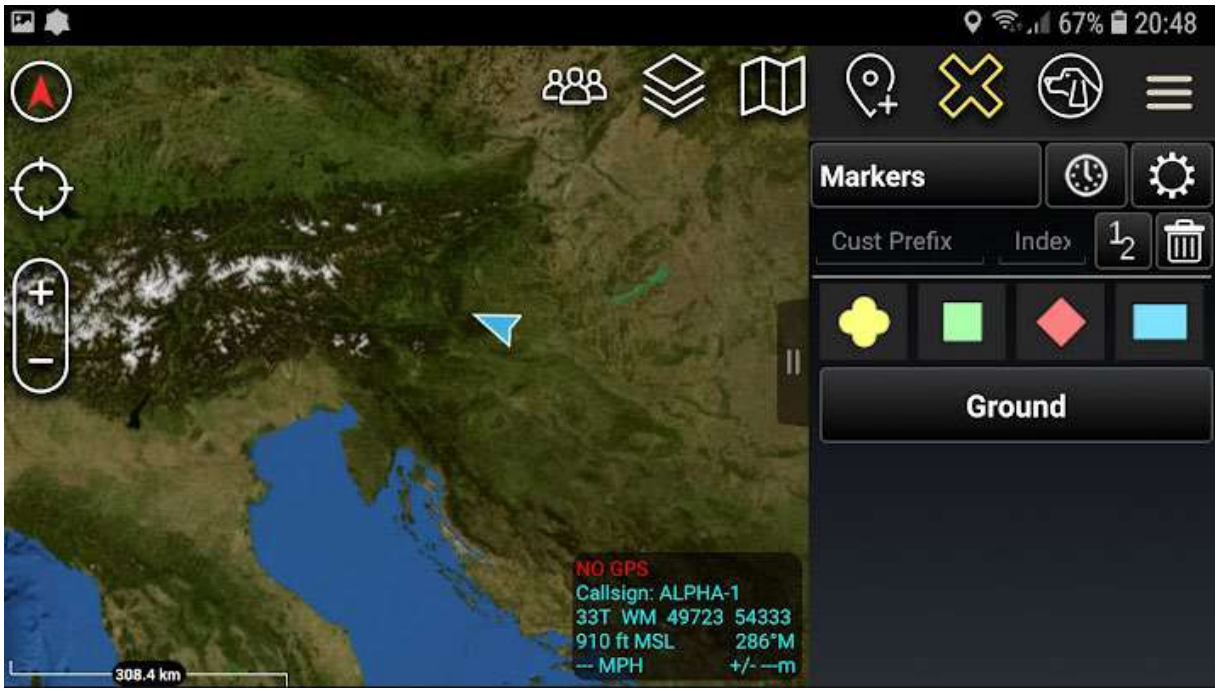
Vir: Lastni vir

Na prejšnjih slikah je prikazana menjava kartografskega vira v aplikaciji.

Splošno upravljanje kartografije je pomembno saj uporabniku omogoča izbiro, prenos in aktivacijo različnih slojev kart in pogleda bodisi prek spleta ali lokalno.

Izbiramo lahko med satelitskimi ali zračnimi posnetki (Imagery), zemljevidi, ki so optimizirani za mobilne naprave (Mobile) in shranjeni ali priljubljeni sloji (Favs).

Opcija pošlji (Send) v ikoni zraven določene karte pa predstavlja možnost pošiljanja zemljevida ostalim uporabnikom v omrežju.

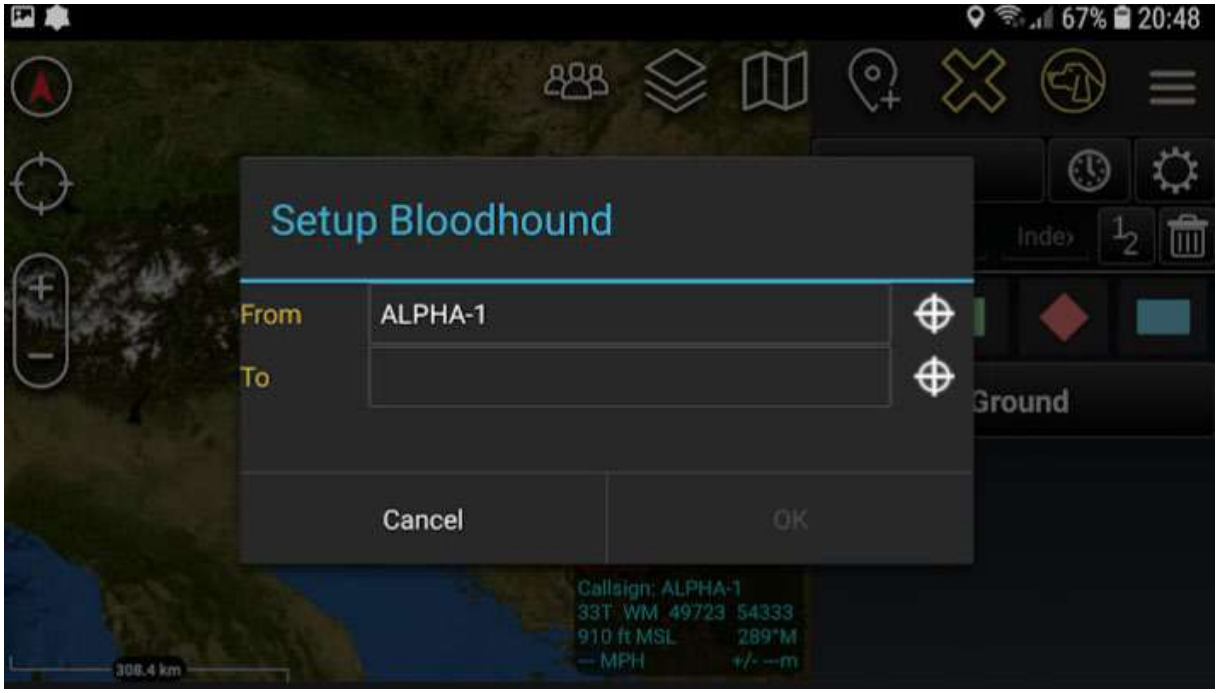


Slika 6 Označevanje točk

Vir: Lastni vir

Na tej siki je prikazan modul za označevanje točk (marker), ki omogoča uporabnikom dodajanje različnih vrst markerjev na zemljevid, Ta funkcionalnost je ključna za taktično usmerjanje, vizualno komunikacijo in označevanje pomembnih elementov na terenu.

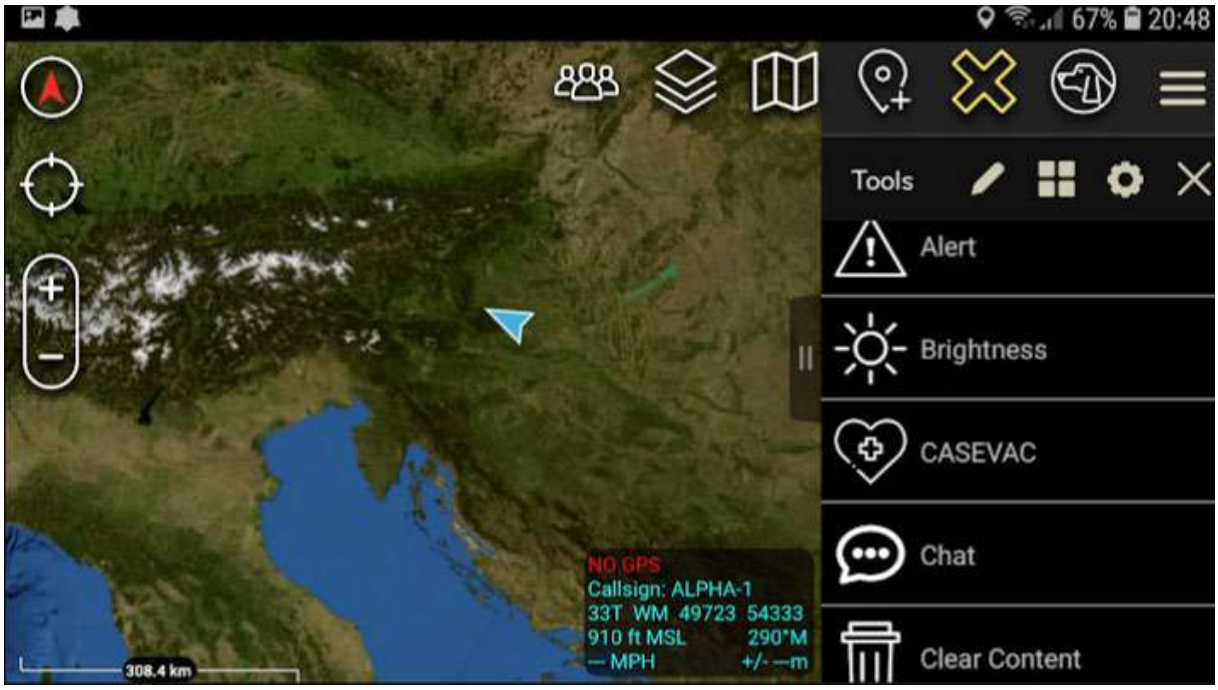
Funkcija »Markers« omogoča označevanje ciljev, točk, nevarnosti, opazovalnice. Zraven je zgodovina označevanja in nastavitve označevanja. Možnosti prilagoditve so dodajanje predpone (Crust Prefix), številčenje markerjev (Index), izbira oblike ali barve. Markerji se lahko kasneje urejajo, premikajo, izbrišejo ali izvozijo.



Slika 7 Usmerjanje lokacije

Vir: Lastni vir

Bloodhound je ena izmed naprednih funkcionalnosti ATAK-CIV, ki omogoča določitev sledenja med izbranim začetnim položajem in ciljno lokacijo. Funkcija je uporabna za koordinacijo enot, usmerjanje patrulj in taktično vodenje, saj omogoča sprotno prikazovanje razdalje in smeri gibanja. Uporabnik lahko izbira točke ročno, preko zemljevida ali izmed aktivnih članov v omrežju. V primerjavi z OsmAnd takšna funkcionalnost ni prisotna v enaki obliki, saj OsmAnd nima neposrednega vmesnika za taktično sledenje drugim uporabnikom.

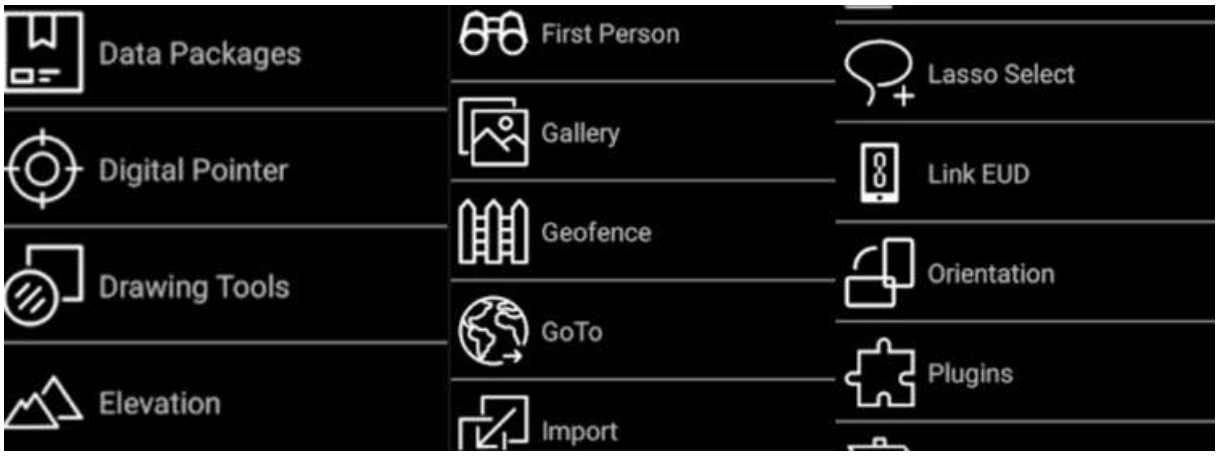


Slika 8 Orodja za upravljanje

Vir: Lastni vir

ATAK-CIV vsebuje obsežen nabor orodij, ki so dostopna preko menija »Tools«. Ta orodja omogočajo uporabniku upravljanje z zemljevidom, komunikacijo, označevanje, nastavitev opozoril, nadzor osvetlitve zaslona, določanje geografsko pogojenih opozoril (geofence) in še mnogo več. Orodja so posebej prilagojena za uporabo v taktičnih okoljih, kjer je hitrost reakcije ključna, hkrati pa se preko njih dostopa tudi do naprednih možnosti – kot so uvoz podatkov, risanje linij na zemljevid ali upravljanje z dodatnimi vtičniki (plugins). V nadaljevanju so opisana posamezna orodja.

Meni »**Tools**« je dostopen prek ikone v zgornjem desnem delu vmesnika (ikona orodnega ključa in kladiva). Ob kliku se odpre seznam funkcij, razdeljenih v več stolpcev. Te funkcije so **ključne za terensko delo**, saj omogočajo hitro izvajanje nalog brez potrebe po dodatnih aplikacijah.



Slika 9 Orodja za upravljanje 2

Vir: Lastni vir

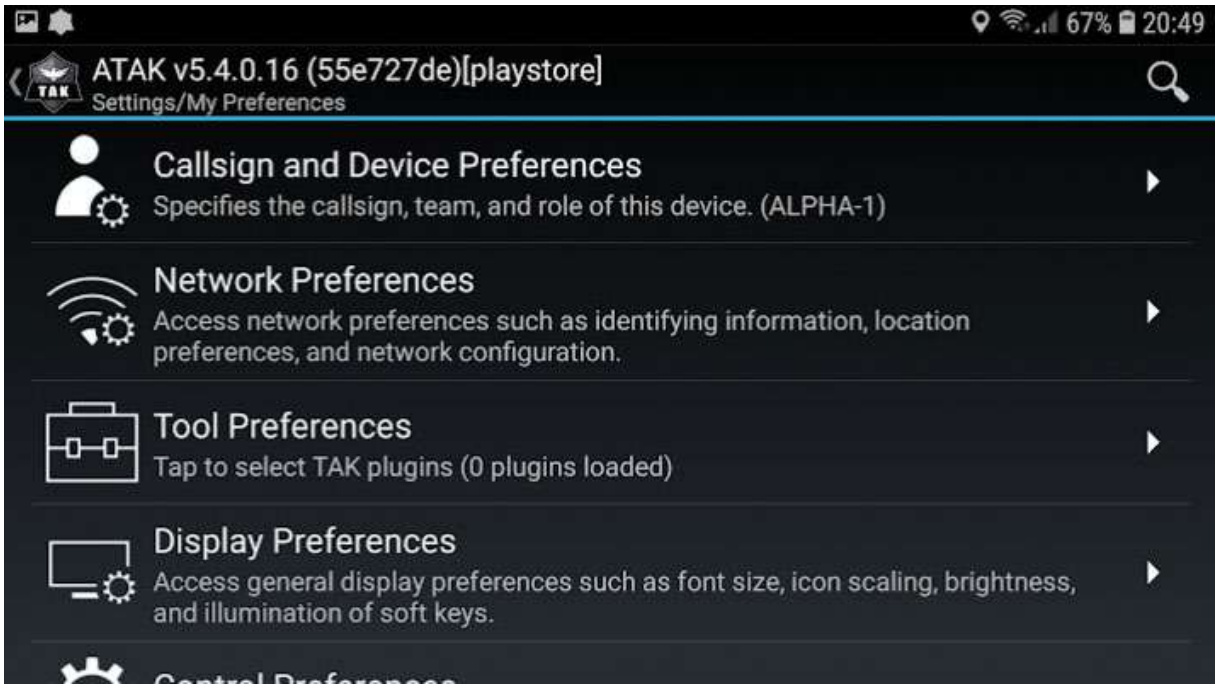
Nadaljevanje orodnega menija (Tools) v ATAK-CIV. Prikazane funkcije vključujejo risanje, geofencing, kazalce, povezovanje z napravami, uvoz podatkov ter napredno selekcijo. Meni orodij je sestavljen tako, da omogoča hitro taktično odzivanje, obveščanje ter popoln nadzor nad prikazom in analizo okolja.



Slika 10 Orodja za upravljanje 3

Vir: Lastni vir

Zadnji del orodnega menija (Tools) v aplikaciji ATAK-CIV. Vključuje napredne funkcije za sledenje, načrtovanje poti, merjenje razdalj, ponoven izračun pozicije, upravljanje multimedijskih vsebin ter nastavitev povezljivosti in sistema. Te funkcije omogočajo širok spekter uporabe v taktičnih in civilno-zaščitnih operacijah.

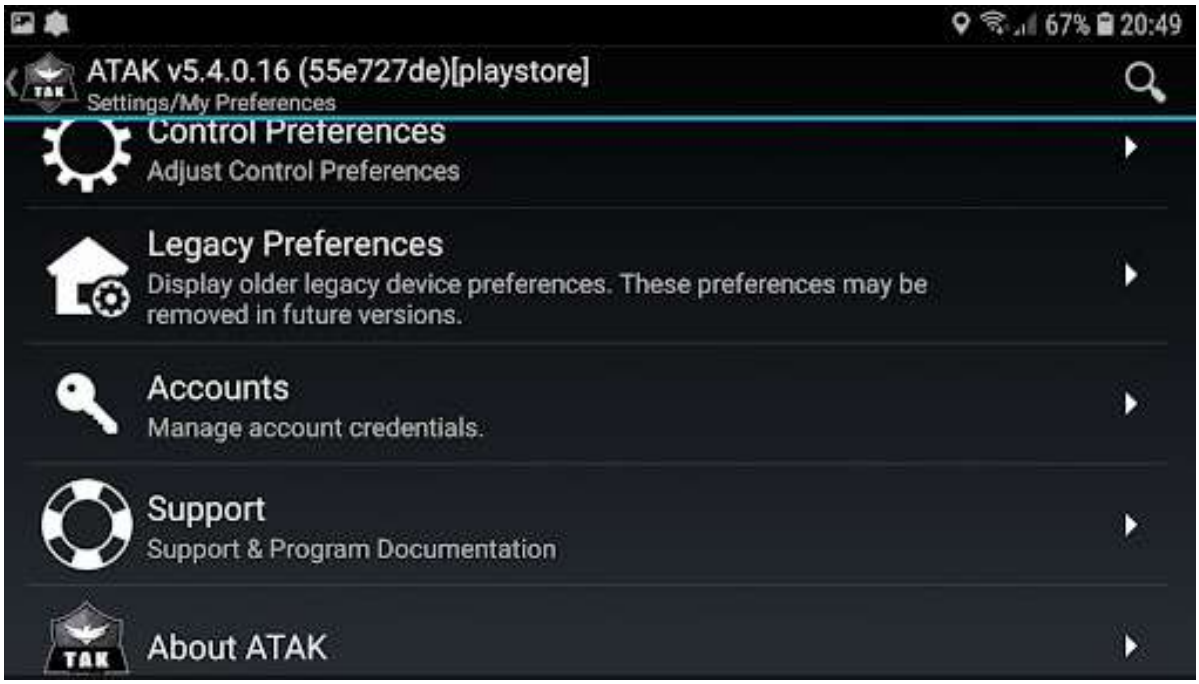


Slika 11 Nastavitve ATAK-CIV

Vir: Lastni vir

Na tej sliki vidimo zaslon z **nastavitvami (Settings)** v aplikaciji **ATAK-CIV v5.4.0.16**, ki omogoča uporabniku celostno prilagoditev aplikacije glede na njegovo vlogo, omrežje, prikaz ter vtičnike. To je pomemben modul v sistemu ATAK, saj zagotavlja operativno fleksibilnost in optimizacijo za posamezne scenarije uporabe.

Prikaz osnovnih uporabniških nastavitev (My Preferences) v aplikaciji ATAK-CIV. Uporabnik lahko nastavi identifikacijske podatke, konfigurira omrežno povezljivost, aktivira ali izključi vtičnike ter prilagodi prikaz aplikacije glede na operativne potrebe.



Slika 12 Nastavitve ATAK-CIV 2

Vir: Lastni vir

Nadaljevanje menija “My Preferences” v ATAK-CIV. Tu se nahajajo napredne nastavitve, kot so kontrolne sheme, podpora, uporabniški računi ter tehnični podatki o aplikaciji. Sistem omogoča popolno prilagoditev glede na potrebe uporabnika in okolje.

2.2 Predstavitev OsmAnd

2.2.1 Kaj je OsmAnd?

OsmAnd (OpenStreetMap Automated Navigation Directions) je odprtokodni sistem za kartorafijo in navigacijo, na voljo za Android in iOS. Zasnovan je kot mobilna aplikacija, ki omogoča uporabo brez internetne povezave, saj si uporabnik sam prenese zemljevide iz OpenStreetMap in jih shrani lokalno na napravo.

Deluje kot celovita navigacijska rešitev: vključuje glasovno vodenje, načrtovanje poti za različne profile uporabnikov (avtomobil, kolo, hoja, peš), pa tudi prikaz in klikanje točk zanimanja (POI), brez dodatnih stroškov ali naročnin. (OsmAnd)

2.2.2 Glavne značilnosti OsmAnd

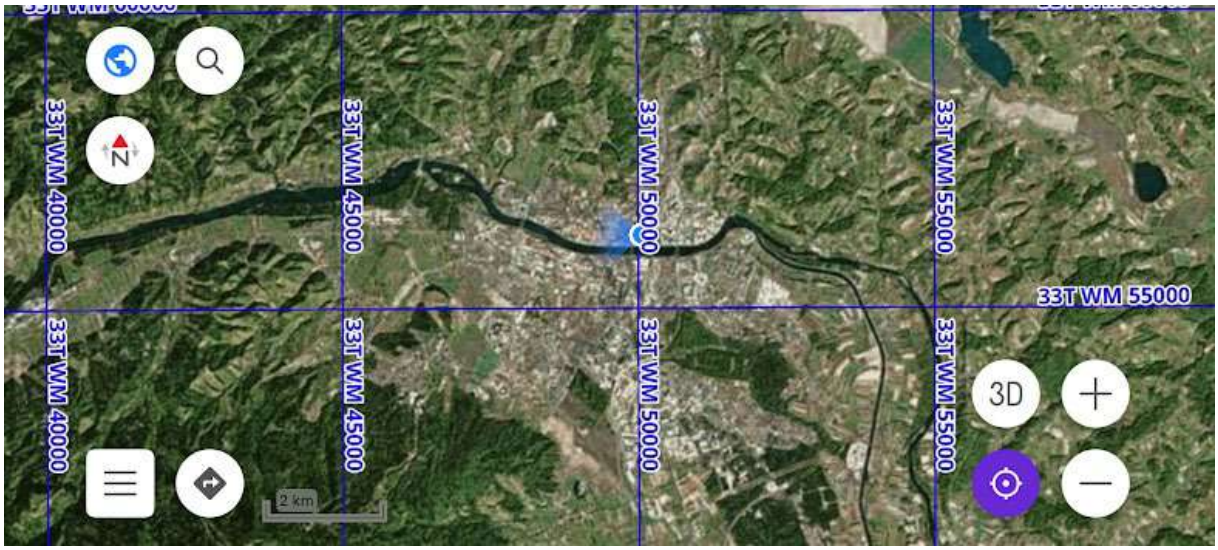
- **Navigacija in poti:** omogoča glasovno navigacijo za različne prevozne profile (vozilo, kolo, peš) s podporo vmesne točke, izračun časa prihoda in samodejno prerazporejanje poti, če uporabnik zapusti prvotno pot. Za delovanje ne potrebuje povezave, saj se izračuni izvajajo lokalno na napravi.
- **Karte in vizualizacija:** omogoča mesečno posodabljanje zemljevidov, možnost naročniškega servisa *OsmAnd Live.* Oblikovno prilagajanje zemljevida, prikaz plastnic terena, senčenje, višinski profili ali dodatni sloji
- **Prilagodljivost in razširljivost:** aplikacija omogoča urejanje konfiguracije preko datotek tipa XML ali vmesnika ter dodajanje vtičnikov, integracija Wikipedije v zemljevid, prikaz terena. Ima možnosti konfiguracije izogibanja določenim cestam, samodejno prikazovanje omejitev hitrosti, opozoril in drugih funkcij.

2.2.3 Varnostne značilnosti

OsmAnd je odprtokodna mobilna aplikacija za navigacijo in kartografijo, ki deluje na platformah Android in iOS. Čeprav ni bila primarno zasnovana za delovanje v varnostno občutljivih ali taktičnih okoljih, ponuja nekaj osnovnih varnostnih mehanizmov, predvsem na področju zasebnosti in delovanja brez povezave.

2.2.3.1 Glavne varnostne značilnosti

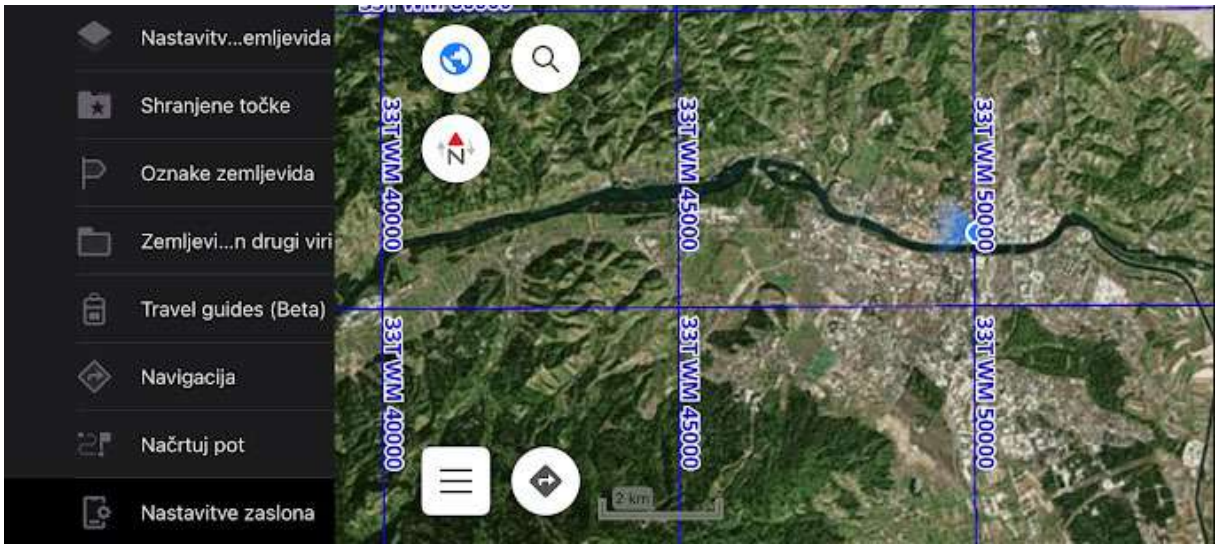
- **Delovanje brez internetne povezave:** sistem ima možnost popolnega delovanja brez dostopa do interneta. Uporabniki lahko prenesejo zemljevide in jih uporabljajo lokalno, kar pomeni, da aplikacija ne potrebuje vzpostavitve povezave z zunanjimi strežniki med uporabo, kar zmanjšuje izpostavljenost omrežnim napadom in vdiranju
- **Zasebnost uporabnika:** ne pošilja uporabniških podatkov na zunanje strežnike in ne zbira osebnih informacij brez izrecnega dovoljenja. Vsi podatki, vključno z lokacijo se shranjujejo lokalno na napravi, kar pomeni, da uporabnik ohranja popoln nadzor nad svojo digitalno sledjo
- **Odprtokodna zasnova:** zaradi odprto kodnega tipa sistema je koda sistema javno dostopna in pregledna. Vsakdo lahko preveri varnostne implementacije, identificira morebitne ranljivosti ali razvije prilagoditve za specifične varnostne potrebe. S tem je zagotovljena višja stopnja transparentnosti, čeprav ne nujno enaka stopnja zaščite kot pri specializiranih varnostnih rešitvah



Slika 13 Izgled OsmAnd

Vir: Lastni vir

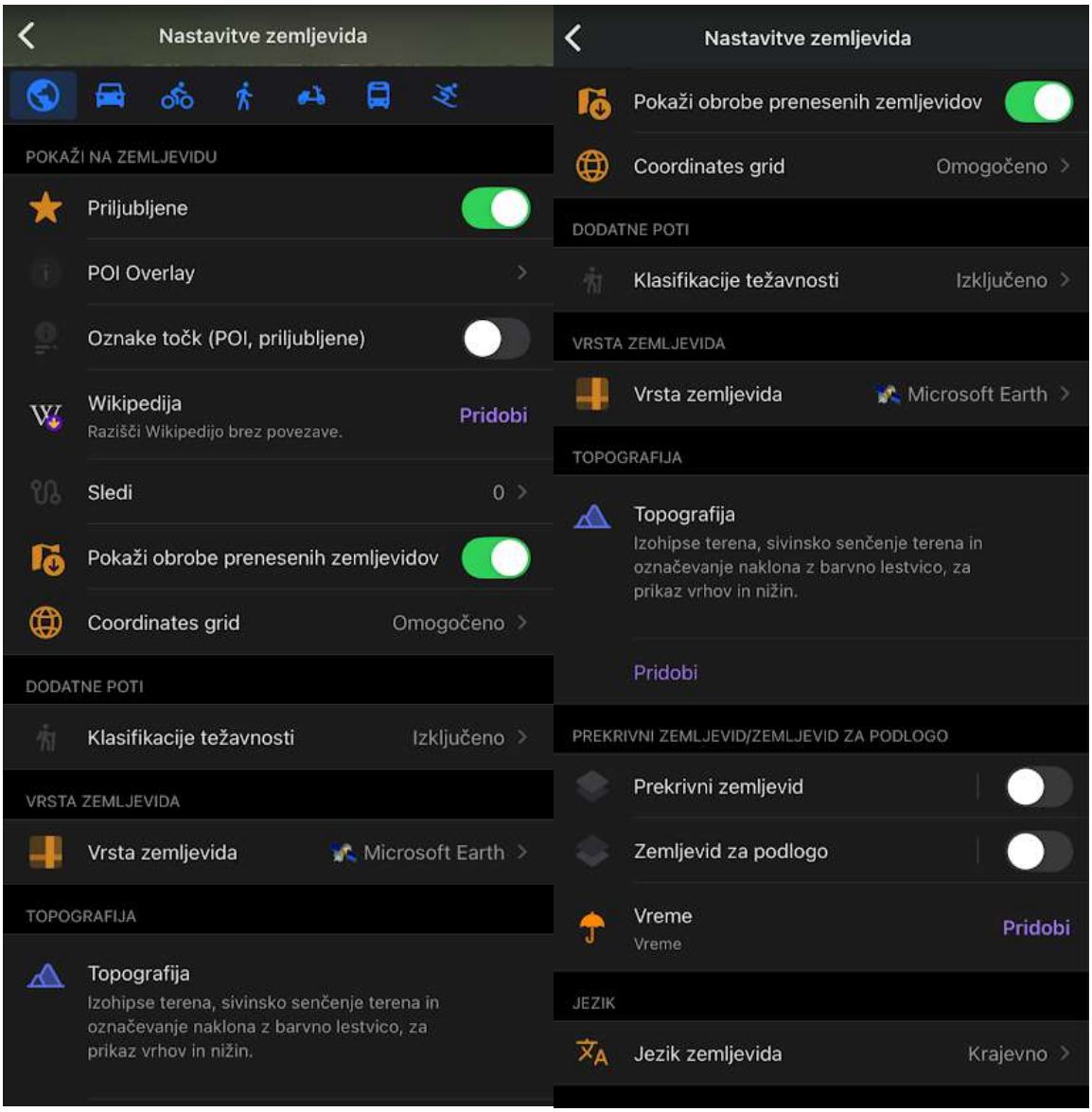
Prikaz satelitskega zemljevida v aplikaciji OsmAnd z aktiviranim UTM mrežnim sistemom (Universal Transverse Mercator). Mrežne črte prikazujejo koordinatna območja v coni 33T (npr. 33T WWM 50000), kar omogoča natančno orientacijo in postavitev na terenu. Takšna mreža je uporabna pri civilni zaščiti, geodetskih nalogah ter osnovni taktični orientaciji brez povezave.



Slika 14 Upravljanje aplikacije

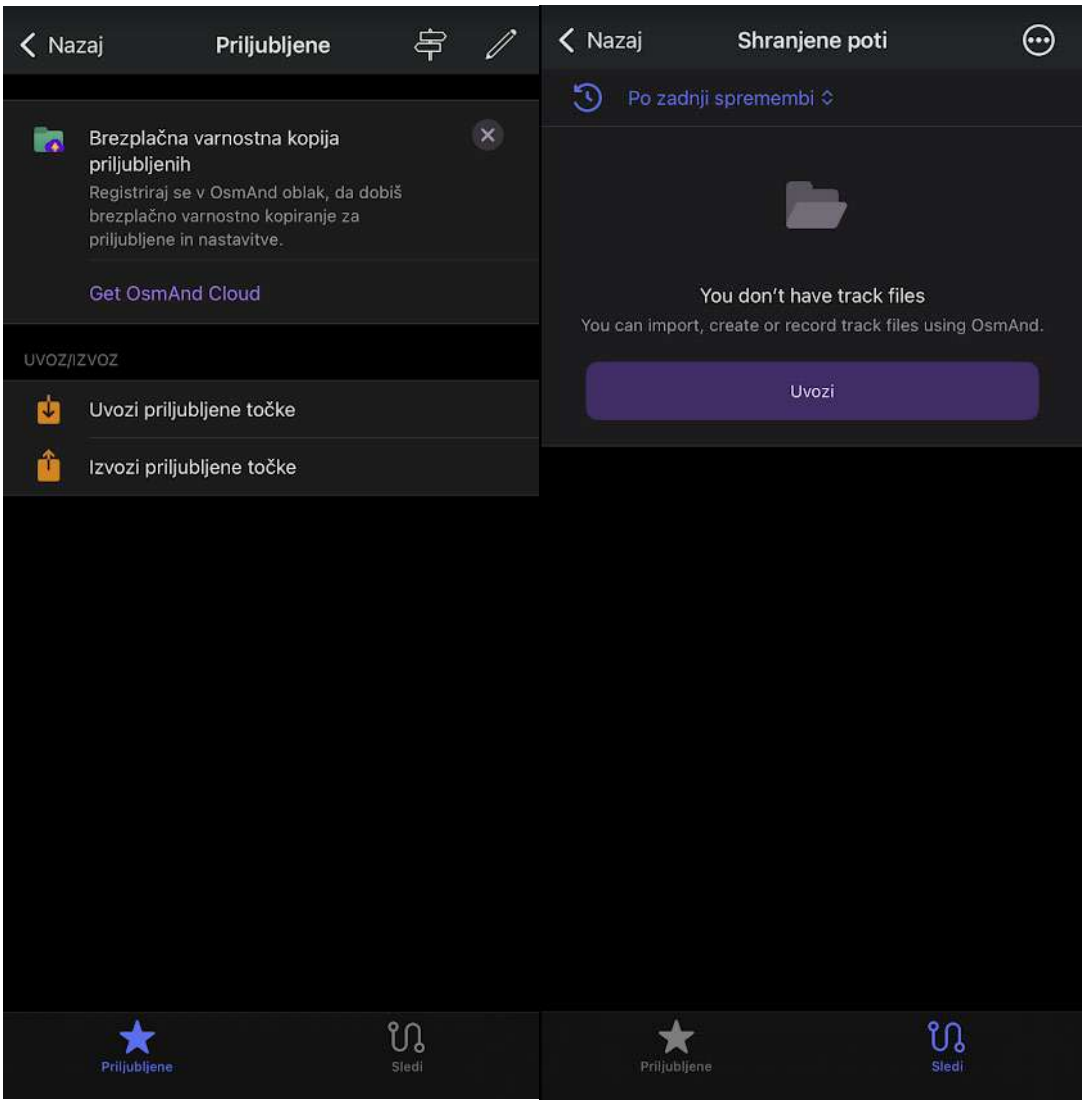
Vir: Lastni vir

Prikaz stranskega menija aplikacije OsmAnd med uporabo satelitskega pogleda z aktivirano UTM mrežo. Meni omogoča hiter dostop do ključnih funkcij, kot so shranjevanje točk, upravljanje slojev, navigacija, načrtovanje poti in nastavitve prikaza. Takšen vmesnik je namenjen prilagodljivemu terenskemu delu in omogoča hitro konfiguracijo brez izhoda iz glavnega pogleda. Mreža 33T WWM dodatno pripomore k orientaciji na podlagi geografske lege.



Slika 15 Nastavitve zemljevida

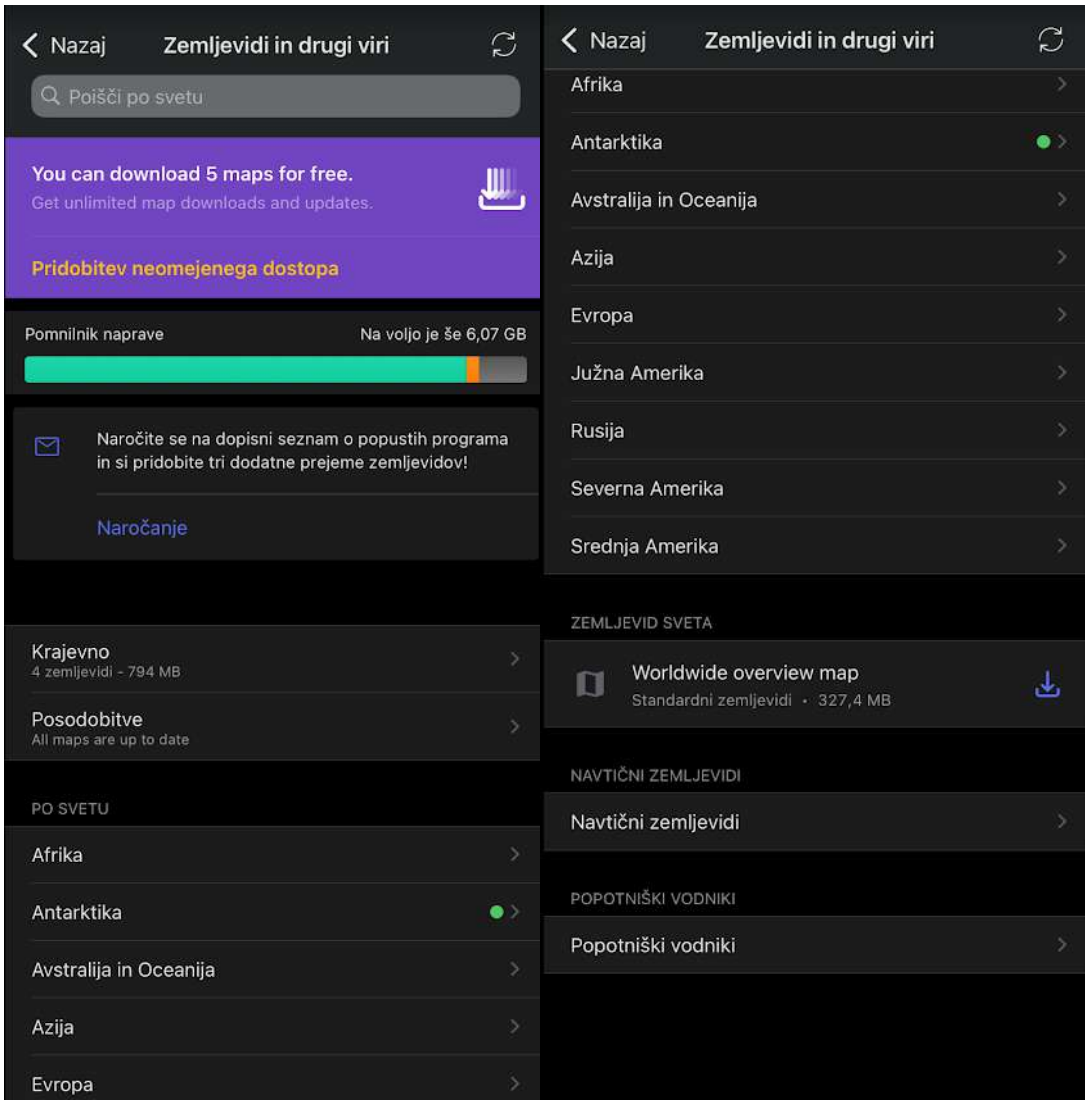
Vir: Lastni vir



Slika 16 Priljubljene točke in shranjene poti

Vir: Lastni vir

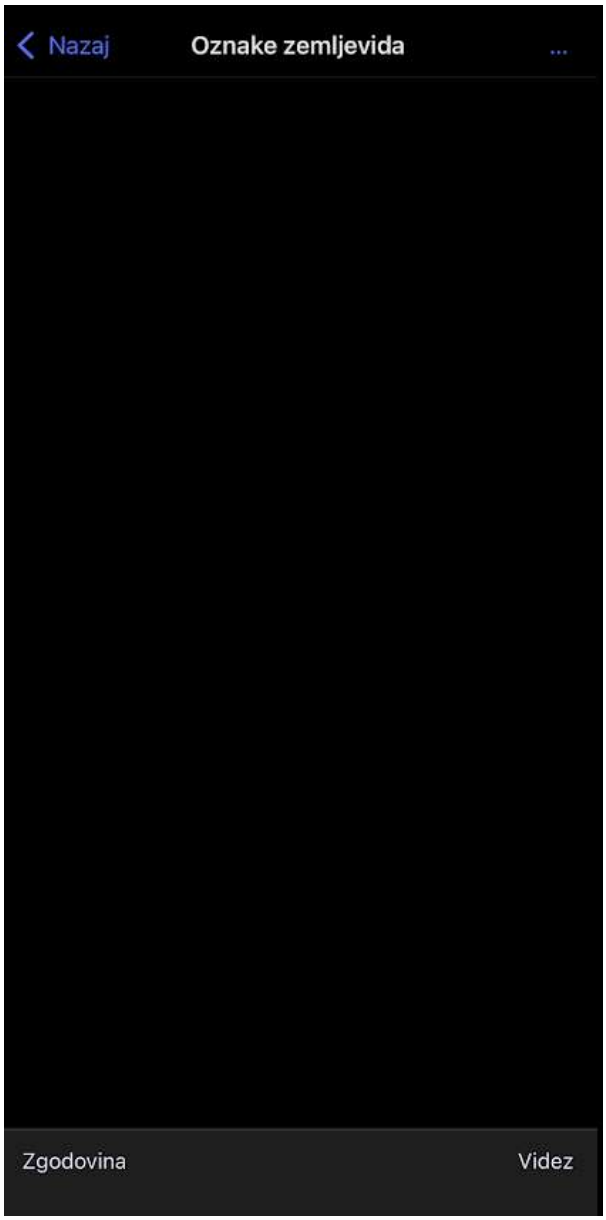
Prikaz nastavitev zemljevida v aplikaciji OsmAnd, kjer uporabnik lahko aktivira mreže koordinat (npr. UTM/MGRS), določi vrsto zemljevida (npr. Microsoft Earth), omogoči sloje, kot so izohipse in senčenje terena, in vključuje vremenske podatke. Poleg tega omogoča uvoz/izvoz točk in poti, kar je uporabno za sledenje, arhiviranje in pripravo nalog vnaprej. Takšne možnosti so ključne za delovanje vtičnikov, kot je Time-in-Zone Monitor, saj omogočajo precizno orientacijo in beleženje gibanja.



Slika 17 Zemljevidi in drugi viri

Vir: Lastni vir

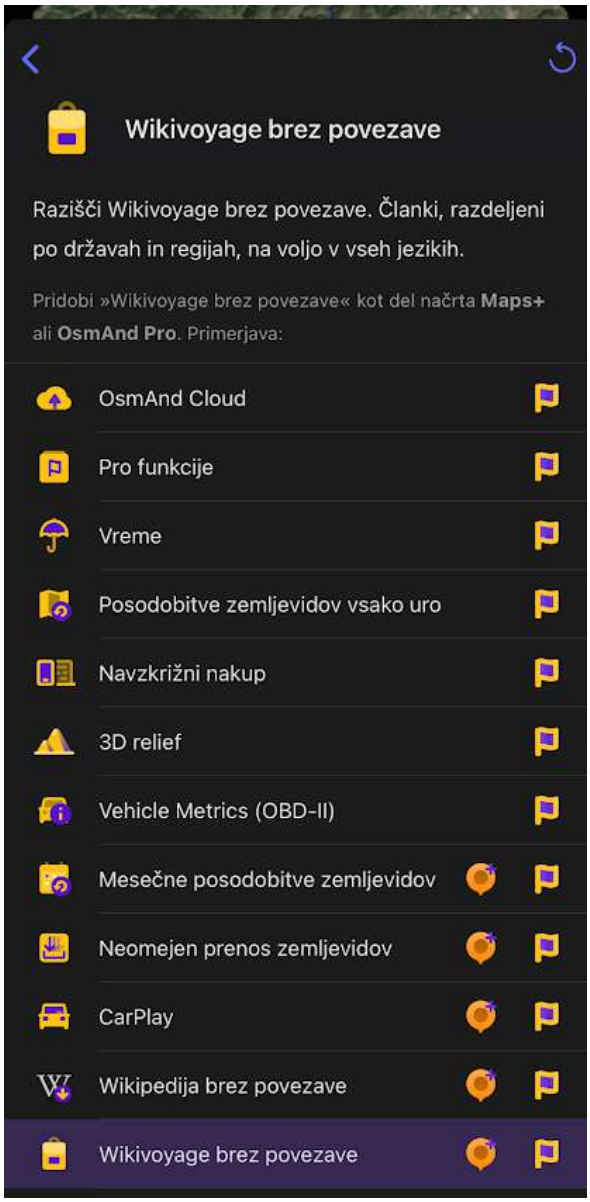
Uporabniški vmesnik menija »Zemljevidi in drugi viri« v aplikaciji OsmAnd. Uporabnik lahko izbere zemljevide glede na regijo (Afrika, Azija, Evropa itd.) in prenese do pet kart brezplačno, z možnostjo nadgradnje za neomejen dostop. Prikazana je tudi razpoložljivost pomnilnika naprave ter dodatni viri, kot so navtični zemljevidi, svetovni pregledni zemljevid (World Overview Map) in popotniški vodniki. Takšna modularna struktura omogoča pripravo lokacijskih podatkov za uporabo tudi v okolju brez internetne povezave.



Slika 18 Oznake zemljevida

Vir: Lastni vir

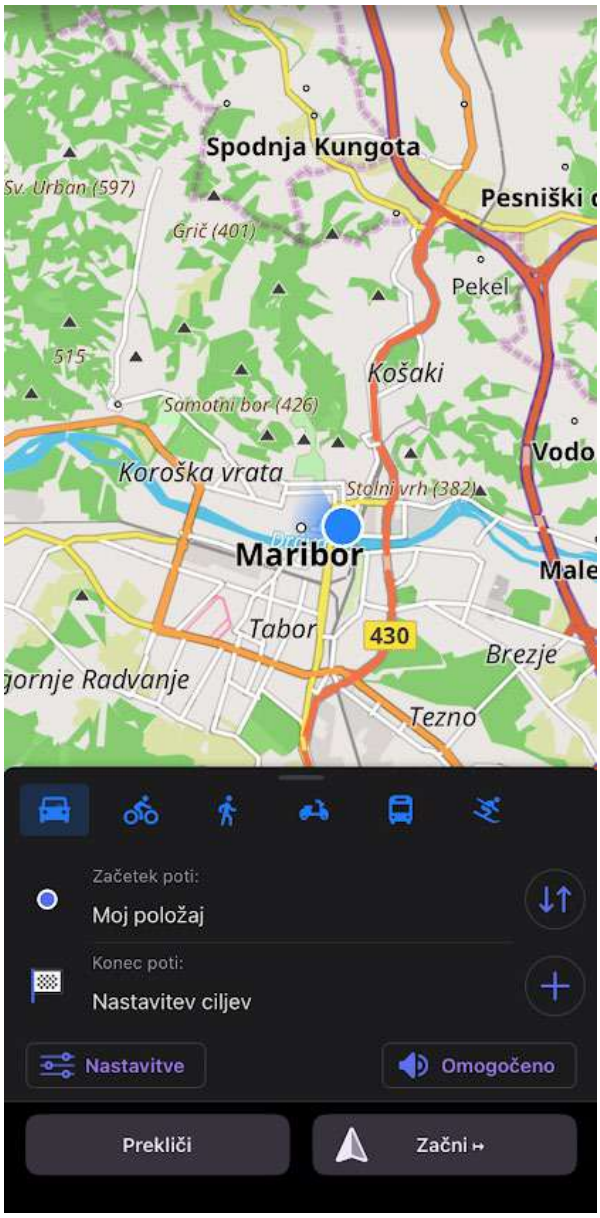
Prikaz razdelka »Oznake zemljevida« v aplikaciji OsmAnd. Čeprav na prikazu ni aktivnih oznak, ta vmesnik omogoča upravljanje s priljubljenimi točkami, označenimi lokacijami, zgodovino uporabe in vizualnim slogom zemljevida. Funkcionalnost je pomembna pri terenskem delu, saj omogoča hitro označevanje in kategorizacijo ključnih točk, kar je koristno tudi za nadgradnjo sistema z dodatnimi funkcijami



Slika 19 Nasveti za pot

Vir: Lastni vir

Prikaz dodatnih funkcionalnosti aplikacije OsmAnd znotraj razdelka »Wikivoyage brez povezave«. Uporabniku so na voljo številne razširitve, kot so vremenski sloji, 3D relief, neomejen prenos zemljevidov, posodobitve kart na uro, uporaba podatkov OBD-II, CarPlay integracija in dostop do člankov brez povezave. Takšne funkcije pomembno prispevajo k razširljivosti aplikacije in omogočajo uporabo v zahtevnih terenih ali v odsotnosti mobilnega omrežja, kar je še posebej pomembno za varnostne in taktične scenarije.



Slika 20 Navigacija

Vir: Lastni vir

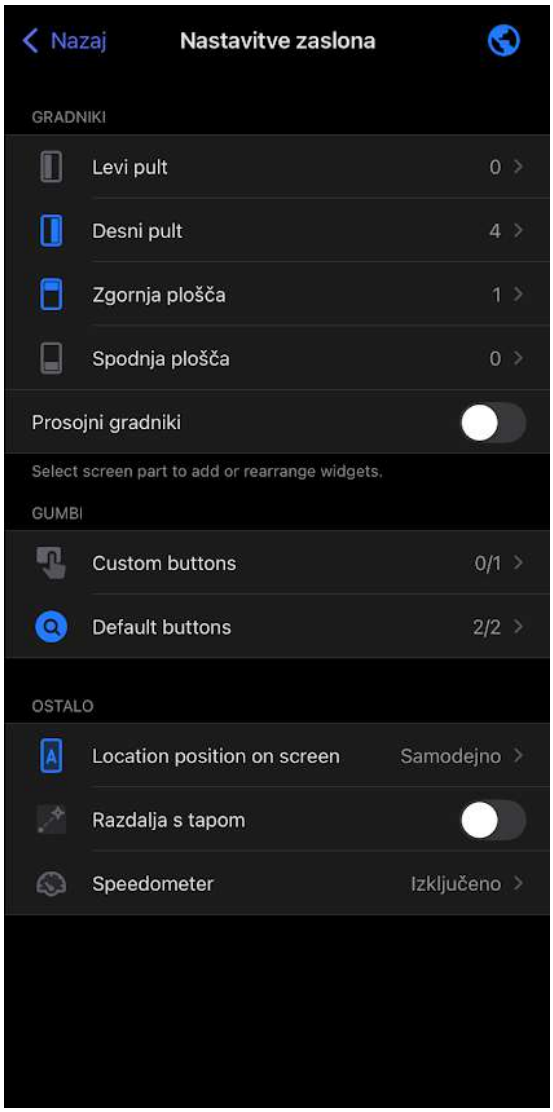
Prikaz načrtovanja poti v aplikaciji OsmAnd na območju Maribora. Uporabnik lahko izbere začetek poti (npr. trenutna lokacija), ciljno točko in način prevoza (avto, kolo, peš, javni prevoz, zrakoplov). Vmesnik omogoča tudi dostop do naprednih nastavitev poti in omogoča sledenje. Takšna funkcionalnost je ključna pri orientaciji in načrtovanju premikov enot na terenu



Slika 21 Načrtuj pot

Vir: Lastni vir

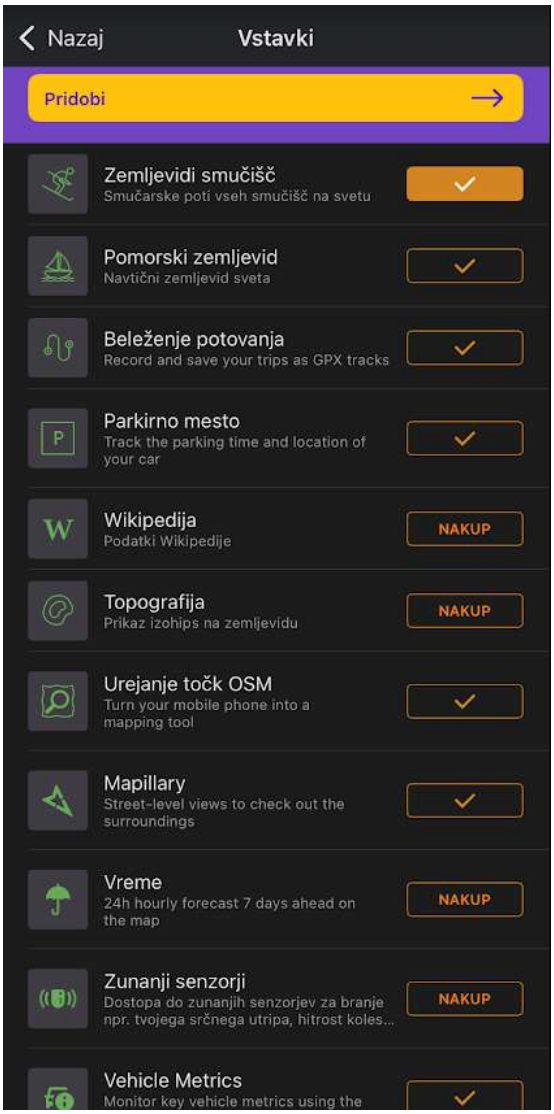
Prikaz načrtovanja poti v satelitskem načinu z vklopljeno UTM mrežo (npr. 33T WM 55000, 60000) v aplikaciji OsmAnd. Uporabnik ima možnost ustvariti novo pot ali naložiti obstoječo sled (npr. GPX datoteko). Takšna funkcionalnost je bistvena za vnaprejšnje planiranje gibanja, orientacijo ter povezovanje z različnimi vtičniki.



Slika 22 Nastavitve zaslona

Vir: Lastni vir

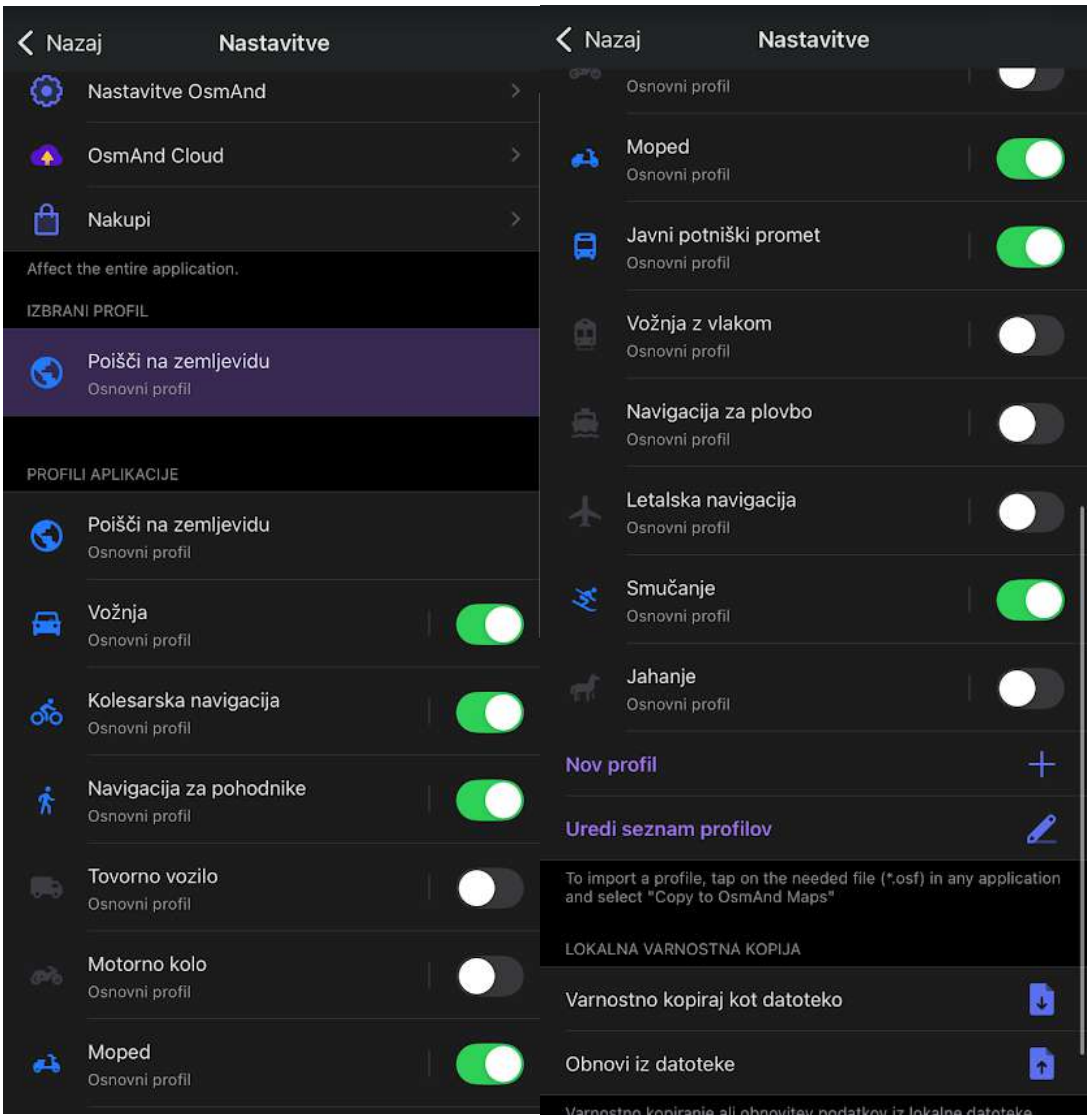
Prikaz razdelka »Nastavitve zaslona« v aplikaciji OsmAnd. Uporabnik lahko prilagodi prikazane elemente v posameznih delih zaslona (levo, desno, zgoraj, spodaj) ter doda ali odstrani gradnike in gumbe. Omogočeno je tudi določanje lokacije prikaza uporabnika, izračun razdalje s dotikom na zaslon in prikaz merilnika hitrosti. Takšna stopnja prilagodljivosti uporabniškega vmesnika je pomembna pri taktični rabi aplikacije, saj omogoča optimizacijo informacij glede na potrebe na terenu.



Slika 23 Vtičniki

Vir: Lastni vir

Prikaz seznama vstavkov (vtičnikov) v aplikaciji OsmAnd. Uporabnik lahko aktivira ali kupi razširitve, kot so zemljevide smučišč, pomorske zemljevide, beleženje potovanj (GPX sledi), topografske prikaze, vremenske podatke, OSM urejanje točk in podporo za zunanje senzorje. Takšen sistem dodatkov omogoča modularnost aplikacije in s tem večjo prilagodljivost za različne scenarije rabe, vključno s taktičnimi nalogami. V kontekstu diplomskega dela je razdelek pomemben tudi zaradi vključitve funkcionalnosti, ki podpirajo testiranje in delovanje vtičnika Time-in-Zone Monitor (npr. beleženje poti, topografija, vremenski sloji).



Slika 24 Nastavitve

Vir: Lastni vir

Prikaz nastavitev profilov v aplikaciji OsmAnd. Uporabnik lahko aktivira različne navigacijske profile, kot so vožnja z avtomobilom, kolesarjenje, hoja, moped, javni promet, smučanje in drugi. Vsak profil vsebuje prilagojene nastavitve, ki vplivajo na izris poti, navigacijska navodila, omejitve in prikaz podatkov. Ta funkcionalnost omogoča visoko stopnjo prilagodljivosti aplikacije specifičnim potrebam uporabnika ter zagotavlja boljšo podporo pri testiranju različnih scenarijev gibanja.

3 PRIMERJALNA ANALIZA (FUNKCIONALNOST, MODULARNOST IN UPORABNOST)

3.1 Modularnost in razvoj vtičnikov

Razširljivost sistema preko vtičnikov predstavlja pomembno lastnost sodobnih mobilnih aplikacij za situacijsko zavedanje, še posebej kadar gre za rabo v specializiranih okoljih, kot so vojaško-taktične operacije ali krizno odzivanje. Modularna zasnova omogoča prilagajanje sistema konkretnim potrebam uporabnikov, integracijo dodatnih funkcij ter boljšo stabilnost aplikacije.

ATAK-CIV temelji na modularnem sistemu, ki omogoča izdelavo in vključevanje namenskih vtičnikov preko uradno podprtega SDK (Software Development Kit). Razvijalci imajo dostop do primerjalno dobro dokumentiranega ogrodja za izdelavo vtičnikov, ki jih je mogoče distribuirati kot samostojne .atak-plugin datoteke. Vsak vtičnik ima svojo strukturo, uporabniški vmesnik in logiko, kar omogoča visoko stopnjo prilagodljivosti. Pri tem sistem omogoča dostop do internih komponent, kot so zemljevid, markerji, podatki o lokaciji, taktične funkcije ipd.

Izvedba osnovnega vtičnika je možna z uporabo predloge iz javno dostopnega repozitorija (npr. GitHub: tak-plugins/plugin-template). Kljub temu je za uspešen razvoj potrebno razumevanje gradbenega sistema, upravljanja dovoljenj in osnov programiranja v Javi za Android okolje.

OsmAnd uporablja drugačen pristop, saj ne omogoča neposredne izdelave internih vtičnikov na ravni same aplikacije. Namesto tega ponuja API in sistem Android Intentov, preko katerih lahko druge aplikacije sprožijo funkcije znotraj OsmAnd. Tako je mogoče zgraditi samostojno Android aplikacijo, ki npr. pošlje marker ali pot do OsmAnd, vendar brez integracije v sam uporabniški vmesnik ali osnovni meni aplikacije.

Čeprav je ta pristop enostavnejši za začetnike (ni potrebe po lastnem SDK-ju), hkrati omejuje modularnost sistema in globino nadzora. Uporabnik ne more v celoti posegati v notranje funkcionalnosti OsmAnd, saj večina sistemskih komponent ni dostopna za zunanje razvijalce brez sprememb izvorne kode.

Primerjalna analiza: ATAK-CIV in OsmAnd z vidika razvoja vtičnikov

Razširljivost sistema preko vtičnikov predstavlja ključno značilnost sodobnih mobilnih aplikacij za situacijsko zavedanje, še posebej v kontekstu specializirane uporabe – denimo v vojaško-taktičnih operacijah, gasilsko-reševalnih enotah ali drugih kriznih scenarijih. Modularna zasnova sistemov omogoča ne le prilagajanje potrebam konkretnih uporabnikov, temveč tudi integracijo specifičnih funkcij, izboljšano vzdrževanje ter zmanjšano kompleksnost osnovne aplikacije.

ATAK-CIV

ATAK-CIV temelji na namenski modularni arhitekturi, ki omogoča razvoj vtičnikov preko uradno podprtega Software Development Kit (SDK). Gre za sistem, ki spodbuja aktivno razvito skupnost, kjer so na voljo predloge (template), primeri uporabe in dokumentacija. Vsak vtičnik ima lastno datotečno strukturo, konfiguracijo, uporabniški vmesnik (UI), logiko ter svoj življenjski cikel. Vtičniki se distribuirajo kot .atak-vtičnik datoteke in jih je možno dinamično vključevati ali odstranjevati brez vpliva na osnovno aplikacijo.

Za razvoj vtičnika je potrebna uporaba programskega jezika Java znotraj Android Studio okolja, razumevanje Gradle sistema, urejanje dovoljenj in dostop do internih funkcij, kot so:

- lokacijski podatki in koordinatne mreže,
- prikaz markerjev in linij na zemljevidu,
- komuniciranje med uporabniki (npr. prek Cursor-on-Target protokola),
- obdelava senzorjev, slojev, geofencinga ipd.

Vtičnik Time-in-Zone Monitor, razvit v okviru te naloge, se je uspešno vključil v ATAK-CIV preko zgoraj omenjenih mehanizmov, kar kaže na visoko stopnjo razširljivosti in preglednosti procesa. Kljub temu pa razvoj zahteva večje predznanje in učenje, predvsem zaradi obsežne dokumentacije in kompleksnosti programskega ogrodja.

OSMAND

OsmAnd**,** kot odprtokodna navigacijska aplikacija, prav tako omogoča določene razširitve, vendar uporablja bistveno drugačen pristop. Ne ponuja neposrednega SDK-ja za razvoj internih vtičnikov v smislu vključevanja v glavno aplikacijo. Namesto tega omogoča interakcijo z zunanjo aplikacijo preko Android Intentov in API-jev, kjer je mogoče:

- pošiljati GPS točke, poti in markerje v OsmAnd,
- upravljati navigacijo preko zunanjo aplikacijo,
- spreminjati sloje in kartografske vire.

Za izvedbo funkcionalnosti podobne Time-in-Zone Monitorju je bila razvita samostojna aplikacija, ki je komunicirala z OsmAnd preko API vmesnikov. Glavna omejitev tega pristopa je, da vtičnik ni integriran znotraj uporabniškega vmesnika OsmAnd, prav tako nima dostopa do notranjih komponent (npr. nadzora nad sloji, sistemskimi dogodki ali prikazom prilagojenih ikon).

To pomeni, da je OsmAnd primernejši za preproste funkcionalnosti, ki jih je mogoče dodati "od zunaj", ne pa za razvoj globoko integriranih taktičnih orodij ali prilagoditev uporabniške izkušnje. Prednost tega pristopa je sicer večja dostopnost za začetnike – ni potrebe po globljem razumevanju zgradbe aplikacije, razvoj je hitrejši, distribucija enostavnejša – vendar z omejenimi možnostmi.

Sklepna ugotovitev

Primerjalna analiza jasno pokaže, da ATAK-CIV predstavlja bolj robustno, fleksibilno in modularno platformo za razvoj kompleksnih vtičnikov, kar je tudi eden glavnih razlogov za njegovo uveljavitev v taktičnih okoljih. Njegova arhitektura je zasnovana tako, da podpira širok nabor razširitev – od enostavnih orodij za označevanje do naprednih modulov za šifrirano komunikacijo, integracijo z obstoječo infrastrukturo (TAKServer) ter povezovanje z drugimi sistemi za poveljevanje in kontrolo. Modularnost omogoča, da razvijalci zgradijo vtičnike, ki neposredno nagovarjajo specifične potrebe uporabnikov, pri čemer se osnovna aplikacija obdrži kot stabilno jedro. Prav ta zasnova je ključna za uporabo v vojaških in varnostnih organizacijah, kjer so zahteve pogosto specifične in se spreminjajo glede na operativno okolje.

Poleg modularnosti se ATAK-CIV odlikuje tudi po svoji prilagodljivosti in združljivosti. Sistem se zlahka poveže z drugimi orodji in protokoli, kar omogoča učinkovito izmenjavo podatkov med različnimi enotami in organizacijami. V praksi to pomeni, da lahko ena enota uporablja ATAK za deljenje lokacije, druga pa za koordinacijo komunikacije, pri čemer obe delujeta na isti infrastrukturi in izmenjujeta združljive podatke. S tem ATAK-CIV presega okvir običajne navigacije in postane celovit sistem za situacijsko zavedanje in odločanje. Pomemben element je tudi njegova odprtost, ki omogoča tako uporabo v civilnih okoljih kot tudi prenos izkušenj iz vojaških uporab v širši varnostni sektor (npr. gasilstvo, civilna zaščita, policija).

Nasprotno pa je OsmAnd zasnovan izključno kot civilna navigacijska aplikacija, kar se odraža tudi v njegovih zmožnostih. Temeljna prednost OsmAnd-a je uporaba odprtih kart (OpenStreetMap), ki so dostopne, ažurirane in omogočajo delovanje brez internetne povezave. To je pomembna lastnost v kriznih situacijah, kjer pogosto ni stabilne infrastrukture. OsmAnd se izkaže kot priročno orodje za osnovne naloge, kot so orientacija, sledenje poti, dodajanje slojev in prikaz različnih tipov kartografskih podatkov. Vendar pa so njegove možnosti razvoja vtičnikov omejene, saj sistem ne podpira neposredne integracije modulov znotraj osnovne aplikacije. To pomeni, da je za naprednejše funkcionalnosti treba razviti ločene spremljevalne aplikacije, ki se povezujejo z OsmAnd prek zunanjih vmesnikov.

Kljub tem omejitvam pa OsmAnd ostaja koristno dopolnilo v širšem spektru rešitev za situacijsko zavedanje. V okoljih, kjer ni nujna globoka integracija, lahko služi kot zanesljiva in cenovno dostopna rešitev. Primer tega so manjše nevladne organizacije, prostovoljne reševalne enote ali logistične operacije, kjer je glavni poudarek na osnovni navigaciji in prikazu kartografskih podatkov. Prav tako je OsmAnd zaradi svoje enostavnosti primeren za hitro usposabljanje novih uporabnikov, ki nimajo predhodnih izkušenj z naprednejšimi sistemi.

Če primerjavo razširimo na vidik kibernetske varnosti, se pokaže, da ATAK-CIV bistveno presega OsmAnd. Varnostni mehanizmi, kot so TLS šifriranje komunikacij, nadzor dostopa, upravljanje z uporabniškimi vlogami in integracija z varnostnimi omrežji, omogočajo njegovo rabo v varovanih okoljih, kjer je zaščita podatkov ključnega pomena. OsmAnd teh lastnosti nima, saj izhaja iz civilnega konteksta, kjer takšna stopnja zaščite ni bila prednostna naloga. To pa ne pomeni, da je OsmAnd neprimeren – pomeni le, da je njegova uporaba v varnostno-taktičnih okoljih omejena na podporne naloge, kjer izmenjava občutljivih podatkov ni ključna.

Iz vidika uporabniške izkušnje ATAK-CIV in OsmAnd ponujata različne prednosti. ATAK-CIV zaradi svoje kompleksnosti zahteva nekoliko daljšo učno krivuljo, saj uporabnik potrebuje več časa za razumevanje vseh funkcij in možnosti konfiguracije. Vendar pa prav ta kompleksnost omogoča natančno prilagoditev aplikacije potrebam posamezne enote. OsmAnd je na drugi strani enostavnejši in bolj intuitiven za uporabo, kar ga dela primernega za uporabnike brez posebnega tehničnega znanja.Iz primerjalne analize tako izhaja, da se ATAK-CIV in OsmAnd ne izključujeta, temveč se lahko dopolnjujeta. ATAK-CIV je optimalna izbira za okolja, kjer so ključni robustnost, varnost in možnost razvoja kompleksnih modulov, medtem ko OsmAnd ponuja praktično in enostavno rešitev za osnovne potrebe, zlasti tam, kjer so sredstva omejena ali pa globoka integracija ni nujna. V praksi bi lahko organizacije uporabile oba sistema vzporedno – ATAK-CIV kot glavno platformo za taktično koordinacijo, OsmAnd pa kot dodatno orodje za logistično podporo, orientacijo in osnovno navigacijo.

Takšna kombinirana uporaba je posebej relevantna v kriznih razmerah, kjer so resursi razpršeni in kjer sodelujejo tako profesionalne kot prostovoljne enote. V tem kontekstu ATAK-CIV zagotavlja hrbtenico za varno koordinacijo, OsmAnd pa ponuja dostopno rešitev, ki jo lahko uporabljajo tudi posamezniki in organizacije brez dostopa do specializiranih vojaških tehnologij.

Zaključimo lahko, da ATAK-CIV predstavlja naprednejšo, varnejšo in bolj razširljivo rešitev, ki je najbolj primerna za profesionalna taktična okolja, medtem ko je OsmAnd zaradi svoje enostavnosti, odprtosti in offline funkcionalnosti uporaben kot dopolnilo ali osnovna rešitev v manj zahtevnih scenarijih. S tem primerjava ne izpostavi zgolj razlik med sistemoma, temveč tudi pokaže možnosti za njihovo komplementarno uporabo v praksi.

3.2 Uporabnost v taktičnem okolju

Uporabnost sistema v taktičnih razmerah je eden ključnih dejavnikov pri izbiri programske opreme za vojaško, policijsko ali civilno zaščitno rabo. Takšne razmere vključujejo zahtevno okolje, potrebo po hitrih in zanesljivih informacijah ter učinkovitem sodelovanju med več uporabniki na terenu.

ATAK-CIV je izvorno zasnovan kot vojaško-taktična platforma. Uporablja se v različnih obrambnih in varnostnih strukturah po svetu, predvsem zaradi podpore taktičnemu usklajevanju, situacijskemu zavedanju in zanesljivi komunikaciji. Sistem omogoča skupno rabo položajev, uporabo taktičnega označevanja (MIL-STD-2525), integracijo brezpilotnih letal, radijskih postaj, kamer in drugih senzorjev.

Zemljevidi omogočajo več nivojsko prikazovanje (npr. višinski model, topografski sloji), uporabniki pa lahko ustvarjajo naloge, območja zanimanja, sledenje poti, ter sproti komunicirajo preko varnih kanalov. ATAK se odlikuje tudi po možnosti delovanja v popolnoma ločenih omrežjih, kar je ključno v bojnih ali kriznih razmerah.

OsmAnd je prvotno razvit kot navigacijska aplikacija za civilno uporabo. Ponuja zelo podrobne zemljevide (OpenStreetMap), deluje brez internetne povezave in omogoča planiranje poti, snemanje sledi (GPX), iskanje po naslovih ter osnovne sloje (nadmorska višina, površine, poti). Vendar OsmAnd ne vsebuje funkcionalnosti za usklajeno delovanje med enotami, ni opremljen s taktično označbo, niti ne omogoča šifrirane komunikacije ali vizualizacije nalog.

V določeni meri ga je mogoče uporabiti v scenarijih, kjer ni potrebe po povezljivosti in naprednih funkcijah (npr. pri orientaciji, reševanju, prostovoljni zaščiti). Kljub temu ne zadostuje zahtevam visoko koordiniranih operacij.

ATAK-CIV je izrazito bolj primeren za uporabo v taktičnem okolju, saj je bil za to namensko razvit. Ponuja bogat nabor orodij za sodelovanje, spremljanje in odločanje v realnem času. OsmAnd, kljub temu da omogoča osnovno orientacijo in lokalno navigacijo, ni zasnovan za taktično rabo in se zato ne more kosati s funkcionalnostmi, ki jih ATAK-CIV omogoča.

3.3 Zaupanje in varnostna ocena

3.3.1 Splošno

Varnost in zaupanje v informacijski sistem igrata ključno vlogo pri njegovi uporabi v operativno občutljivih okoljih, kot so vojaške misije, humanitarne intervencije ali zaščitno-reševalne operacije. V tem kontekstu ocena varnosti ne zajema le tehničnih mehanizmov zaščite podatkov, kot so šifriranje, nadzor dostopa in izolacija komunikacijskih kanalov, temveč tudi širši okvir kibernetske odpornosti, ki vključuje detekcijo in odziv na grožnje (Mullins, 2020). Hkrati zaupanje presega zgolj tehnične parametre in se oblikuje na osnovi več dejavnikov: stabilnosti sistema, njegove preizkušenosti v praksi ter percepcije uporabnikov, ki izhaja iz izkušenj pri uporabi v realnih scenarijih (Bellini, 2025). Prav percepcija zaupanja eden najpomembnejših dejavnikov pri odločitvi organizacij za uvedbo informacijske rešitve, saj se nanaša na oceno verodostojnosti, transparentnosti in predvidljivosti sistema.

Poleg tega je v varnostno občutljivih okoljih pomembna tudi organizacijska dimenzija zaupanja. Uporabniki morajo imeti zagotovilo, da sistem ne bo odpovedal v ključnih trenutkih, saj lahko tehnična nezanesljivost neposredno ogrozi varnost ljudi in uspešnost operacije. Tehnologija brez zaupanja nima praktične vrednosti, saj odločanje temelji ne le na zmožnostih sistema, temveč tudi na prepričanju, da bo ta deloval dosledno in predvidljivo. Zaupanje je torej neločljivo povezano z varnostjo, saj obe kategoriji skupaj oblikujeta osnovo za dolgoročno uporabo informacijskih rešitev v zahtevnih operativnih razmerah.

ATAK-CIV

ATAK-CIV je razvit z mislijo na varnostno-kritična okolja. Sistem omogoča:

- uporabo šifriranih povezav (npr. TLS) za varno prenos podatkov,
- delovanje v zasebnih omrežjih, brez dostopa do javnega interneta,
- omejeno komunikacijo znotraj sistema z nadzorovanjem podatkovnih tokov,
- integracijo s sistemi za identifikacijo uporabnikov in nadzorom pravic,
- podporo za digitalne podpise in sledenje dogodkom

Zaradi svoje obsežne uporabe v resničnih vojaških in kriznih razmerah ATAK uživa visoko stopnjo zaupanja med uporabniki. Gre za orodje, ki ga uporabljajo različni akterji – od rednih vojaških enot in varnostnih agencij do prostovoljnih obrambnih društev in humanitarnih organizacij. Takšna široka uporabniška skupnost ne prispeva le k utrjevanju zaupanja v sistem, temveč tudi aktivno sodeluje pri njegovem nadaljnjem razvoju. Povratne informacije iz terenskih izkušenj so namreč ključne za pravočasno odpravljanje napak, izboljšave funkcionalnosti in krepitev varnostnih mehanizmov.

Posebno vrednost predstavlja dejstvo, da odprta narava razvoja ATAK-a omogoča redne varnostne revizije in hitro zaznavanje ranljivosti. Transparenten razvojni proces povečuje preglednost, kar pomeni, da morebitne pomanjkljivosti niso skrite, temveč jih lahko prepoznajo in naslovijo tako razvijalci kot uporabniki.

V kombinaciji z vgrajenimi šifrirnimi protokoli in standardi, ki temeljijo na vojaških praksah, to zagotavlja visoko stopnjo odpornosti proti kibernetskim grožnjam. Rezultat je sistem, ki združuje praktično preizkušenost, stalne izboljšave in strukturiran pristop k varnosti, kar ga uvršča med najbolj zaupanja vredne platforme za situacijsko zavedanje v zahtevnih operativnih okoljih.

OsmAnd je zasnovan z vidika zasebnosti, vendar ne z vidika kibernetske varnosti za visoko tvegana okolja. Njegove značilnosti vključujejo:

- lokalno obdelavo podatkov (deluje brez interneta),
- odsotnost zbiranja osebnih podatkov, kar je dobro za anonimnost,
- ni aktivnega nadzora nad dostopom, uporabniki niso preverjeni,
- ni šifriranja komunikacije med napravami (ker ni pravega mrežnega sodelovanja),
- ni možnosti upravljanja uporabnikov ali sistemskih vlog.

Čeprav je OsmAnd zaradi teh lastnosti ustrezen za splošno civilno rabo (treking, potovanja, osnovna orientacija), ni primeren za okolja, kjer je zaščita komunikacije, nadzor nad uporabniki ali integracija z varnostno politiko ključna.

3.3.2 Primerjava

ATAK-CIV dosega visoko oceno varnosti predvsem zaradi uporabe vgrajenih šifrirnih protokolov, ki zagotavljajo zaščito komunikacije med uporabniki in preprečujejo nepooblaščen dostop do občutljivih podatkov. Poleg tega omogoča delovanje v popolnoma izoliranem okolju, kar je ključno v primerih, ko je uporaba javnega interneta ali civilnih komunikacijskih kanalov nedopustna. Takšna arhitektura sledi preverjenim praksam, ki izhajajo iz vojaških standardov in priporočil, zato sistem uživa višjo stopnjo zaupanja med uporabniki v varnostno občutljivih in taktičnih scenarijih. Dejstvo, da je ATAK-CIV večkrat preizkušen v realnih operativnih okoliščinah, še dodatno potrjuje njegovo zanesljivost in ustreznost za uporabo v zahtevnih okoljih, kjer lahko odločitve neposredno vplivajo na varnost enot in uspeh naloge.

Na drugi strani OsmAnd ponuja osnovno zaščito, ki je usmerjena predvsem v zasebnost posameznika in spoštovanje načela odprte kode.

Resda njegova odprtokodna narava omogoča razvijalcem in uporabnikom prilagajanje funkcionalnosti ter potencialno tudi krepitev varnostnih mehanizmov, vendar to ni privzeto implementirano.

To pomeni, da uporabniki brez dodatnih tehničnih znanj in posegov ostanejo omejeni na osnovne varnostne funkcije, ki ne zadostujejo za usklajeno delovanje v zahtevnih taktičnih ali kriznih situacijah. Prav tako OsmAnd ne sledi strogim varnostnim standardom, kot jih narekujejo vojaški ali specializirani varnostni protokoli, zato se pri uporabi v operativnem okolju lahko pojavijo ranljivosti in tveganja, ki bi bila v primeru ATAK-CIV bistveno bolje naslovljena.

3.4 Kibernetska zaščita

3.4.1 Splošno

Kibernetska zaščita v mobilnih sistemih za situacijsko zavedanje je večplastna disciplina, ki združuje tehnične, organizacijske in operativne vidike varnosti. Mobilne aplikacije, ki podpirajo orientacijo, usklajevanje enot in vizualizacijo v realnem času, so izpostavljene številnim grožnjam – od prestrezanja komunikacije, manipulacije podatkov, falšnih informacij do napadov na infrastrukturo (Dwivedi, Yadav & Singh, 2019). V taktičnih okoljih, kjer je nadzor nad signalom, dostopom in podatkovnimi tokovi pogosto otežen, je nujno, da aplikacija omogoča varno komunikacijo, izolirano delovanje in robustno upravljanje pravic dostopa.

Kot pojasnjuje Stallings (2019) v svoji knjigi Network Security Essentials: Applications and Standards, so protokoli, kot so TLS (Transport Layer Security) in uporaba šifriranih kanalov pri prenosu podatkov, temeljni mehanizem za zaščito integritete in zaupnosti. Stallings poudarja, da brez ustreznega šifriranja komunikacije vsaka izmenjava podatkov – tudi lokacijskih – lahko predstavlja vstopno točko za sovražno upravljanje ali prisluškovanje, kar je v kontekstu taktičnih sistemov nesprejemljivo (Stallings, 2019, str. 245-260). Poleg tega je pomembno, da aplikacija deluje v izoliranem ali zanesljivem omrežju, brez nepotrebnih zunanjih odvisnosti, kar zmanjšuje površino za napade.

Druga ključna komponenta je preverjanje pristnosti (authentication) in nadzor dostopa (access control). Pfleeger & Pfleeger (2021) v svoji knjigi Security in Computing opisujeta modele, kjer so identiteta, vloge in pravice uporabnikov strogo definirane ter tehnično uveljavljene. Ti modeli vključujejo digitalne podpise, certifikate ali tokens, ki omogočajo, da aplikacija verificira, ali je komunikacija res z zaupanja vredne strani, in preprečuje nepooblaščen dostop. V taktičnih scenarijih, kjer se nahajaš v območjih s potencialnimi motnjami signala ali tveganji prestrezanja, je ta zaščita ključna za ohranjanje zaupanja in varnosti operacij.

Posebna pozornost mora biti namenjena tudi zaščiti podatkov v mirovanju (data at rest) in med prenosom (data in transit). Dwivedi, Yadav & Singh (2019) izpostavljajo, da mobilne aplikacije pogosto shranjujejo občutljive podatke (GPX poti, lokacije, zaznave senzorjev) na napravi. Če ta podatki niso zaščiteni s šifriranjem diska ali šifriranjem aplikacijskega pomnilnika, postanejo tarča zlonamernih aplikacij ali fizičnega nepooblaščenega dostopa.

Poleg tega je treba zagotoviti, da se podatki, ki se prenašajo med napravami ali strežniki, šifrirajo s primerljivimi standardi (npr. TLS 1.2 ali TLS 1.3), in kadar je mogoče, z uporabo VPN ali varnih omrežij.

Varnostni mehanizmi morajo biti vključeni že v fazi načrtovanja aplikacije – pristop "security by design." Kot Pisani & Tilley (2022) poudarjata v knjigi Mobile Systems Security: Principles and Case Studies, je ključno, da se varnostne zahteve opredelijo hkrati z ostalimi funkcionalnimi zahtevami, da se preprečijo retroaktivne rešitve, ki so lahko dražje in manj zanesljive. Pisani & Tilley opozarjata, da so tudi knjižnice in odvisnosti aplikacije potencialne točke ranljivosti, saj zastareli moduli ali nezaščitene knjižnice lahko vnašajo že znane varnostne napake. Zato je nadzor različic (version control) in redno posodabljanje ključnega pomena.

Še en aspekt je vizualizacija in poročanje incidentov v realnem času. Kot so pokazali Mullins et al. (2020), kibernetska situacijska zavednost vključuje ne le zaznavanje groženj, temveč tudi strukturirano poročanje o incidentih, časovne okvire odziva in oceno razpoložljivih virov (Mullins, R., Nargi, B., & Fouse, A., 2020). Dobro zasnovan uporabniški vmesnik, ki jasno prikazuje stanje (ali je uporabnik še v coni, koliko je časa preživel v njej, opozorila v primeru prekinitve signala ali izgube GPS), lahko bistveno prispeva k zaupanju uporabnikov in operativni učinkovitosti.

V kontekstu tvoje diplomske naloge se torej potrjuje, da ATAK-CIV izpolnjuje številne od teh zahtev — omogoča šifrirano komunikacijo, izolirano delovanje, digitalno preverjanje identitete in robustne protokole, kot TLS. OsmAnd pa, čeprav ima prednosti glede dostopa in prilagodljivosti, v osnovi ne podpira vseh teh mehanizmov. Zato je ključnega pomena, da se pri morebitnem širjenju ali uporabi OsmAnd v taktičnih okoljih uvedejo dodatni sloji zaščite — kot je uporaba VPN-kanalov, nadzor dostopa znotraj naprave, digitalne podpise ter robustne knjižnice, ki so redno posodobljene.

ATAK-CIV

ATAK-CIV vključuje vrsto zaščitnih mehanizmov, ki sledijo načelom varnostne arhitekture, uveljavljene v obrambnem sektorju. Med ključne elemente kibernetske zaščite sodijo:

- Podpora TLS (Transport Layer Security) za zaščito prenosa podatkov med napravami.
- Možnost uporabe VPN rešitev za dodatno zaščito povezav.
- Zmožnost delovanja v zaprtem omrežju, kar onemogoča dostop zunanjim akterjem.
- Digitalno podpisovanje sporočil, kar omogoča preverjanje avtentičnosti podatkov.
- Omejitev komunikacije na vnaprej določene IP-naslove ali vozlišča znotraj enot.
- Usklajenost z vojaškimi in varnostnimi protokoli, ki določajo ravnanje z občutljivimi podatki.

Ta zasnova omogoča uporabo sistema tudi v operativno najbolj zahtevnih pogojih (npr. specialne enote, humanitarne intervencije, krizni odziv), kjer je varnost komunikacije kritična za uspešnost naloge.

OsmAnd

OsmAnd je primarno namenjen individualni civilni rabi, zato kibernetske zaščite v klasičnem smislu ne implementira. Nekatere osnovne značilnosti sicer zmanjšujejo možnost zlorabe, vendar ne zagotavljajo aktivne zaščite:

- Delovanje brez povezave preprečuje sprotne kibernetske grožnje, a ne omogoča varne komunikacije.
- Ni šifrirane izmenjave podatkov med uporabniki ali napravami.
- Ni nadzora dostopa, avtorizacije uporabnikov ali digitalnega podpisovanja.
- Prenosi (npr. GPX ali POI datotek) potekajo brez nadzora ali zaščite.
- Odvisnost od sistemskih dovoljenj Androida, kar lahko predstavlja ranljivost pri starejših napravah.

Uporaba OsmAnd v varnostno občutljivih okoljih brez dodatne zaščitne infrastrukture (npr. MDM sistemi, zunanji VPN, fizična izolacija) ni priporočljiva.

3.4.2 Primerjava

ATAK-CIV predstavlja celostno in namensko razvito rešitev za delo v varnostno občutljivih okoljih, kjer je zaščita informacij in komunikacije ključnega pomena. Sistem omogoča delovanje v izoliranih omrežjih z omejenim dostopom, kjer se komunikacija odvija preko varnih kanalov, zaščitenih z naprednimi metodami šifriranja (npr. TLS). Poleg tega omogoča preverjanje identitete uporabnikov, nadzor dostopa do podatkov in sledenje dogodkom v sistemu, kar pomembno prispeva k preglednosti in odgovornosti. Strogi komunikacijski protokoli zagotavljajo, da je vsak prenos informacij avtentičen in zanesljiv, kar je posebej pomembno v taktičnih in operativnih pogojih, kjer je vsaka napaka lahko kritična.

Na drugi strani je OsmAnd zasnovan kot orodje za individualno civilno rabo, zato se ne osredotoča na elemente celovite kibernetske zaščite. Ne vključuje šifriranih komunikacijskih kanalov, preverjanja identitete ali naprednih kontrol dostopa. Zaradi tega je občutno manj primeren za uporabo v okoljih, kjer obstajajo resne varnostne zahteve ali tveganja, povezana z nepooblaščenim dostopom ali prisluškovanjem. Kljub temu pa zaradi svoje odprtokodne narave omogoča določene prilagoditve, vendar te zahtevajo dodatno znanje in niso privzeto vključene v osnovno aplikacijo.

Primerjalno gledano ATAK-CIV nudi bistveno višjo raven zaščite tako na omrežni kot tudi na aplikativni ravni, kar je neposredna posledica njegovega izvora v vojaško-obrambnem sektorju ter prilagoditev potrebam taktične uporabe. OsmAnd ostaja uporaben v civilnem kontekstu, kjer varnost ni ključna, vendar v primerjavi z ATAK-CIV ne izpolnjuje kriterijev za zanesljivo delovanje v visoko varovanih operativnih okoljih.

Kot razvidno v Tabeli 1, ki je na naslednji strani.

Tabela 1 Tabela primerjalne analize

Kriterij	ATAK-CIV	OsmAnd
Modularnost	Visoka modularnost, uradni SDK, integracija v aplikacijo, razširjene možnosti dostopa do funkcij	Brez uradnega SDK le omejena komunikacija preko API in Intents, brez integracije v vmesnik
Kompleksnost razvoja	Višja, potreben je Android Studio, Java, razumevanje Gradle in pravic	Nižja, osnovno poznavanje Android razvoja, hitra zunanja integracija
Uporabnost v taktičnem okolju	Namenjen taktični rabi saj ima simbole, naloge, različne sloje, komunikacijo in delovanje brez interneta	Civilna raba saj vsebuje navigacijo, snemanje poti, zemljevid brez povezave
Zaupanje uporabnikov	Visoko, ker ga uporabljajo vojaške in prostovoljne sile ter je praktično preverjen	Nizko za taktično rabo vendar primeren za civilno uporabo in je brez zaščitenega sodelovanja
Varnost / kibernetska zaščita	TLS, VPN podpora, delovanje v izoliranih omrežjih, digitalni podpisi in nadzor pravic	Brez šifriranja in brez nadzora dostopa ter brez preverjanja uporabnikov zaradi česar je ranljiv na starejših sistemih
Prilagodljivost uporabniške izkušnje	Visoka, ker ima vsak vtičnik lasten UI in lahko spreminja delovanje aplikacije	Nizka saj ni možno spreminjati glavnega vmesnika ali sistemskih komponent
Razpoložljivost / odprtokodnost	Delno odprt (ker je civilna različica), aktiven GitHub, predloge vtičnikov	Popolnoma odprtokoden in dostopen na GitHub-u, aktiven razvoj
Primeren za civilno ali profesionalno	Za profesionalno, ker vsebuje integracije z brezpilotnimi letali, senzorje, kartografijo	Za civilno rabo, ker je enostaven za uporabo in je primeren za vsakdan

4 OPIS RAZVITEGA VTIČNIKA »TIME-IN-ZONE MONITOR«

4.1 Namen vtičnika

Vtičnik meri čas, ki ga uporabnik preživi znotraj določenega območja. Ob vstopu v območje se začne merjenje, ko uporabnik zapusti območje se merjenje konča in čas shrani.

4.2 Ključne funkcije

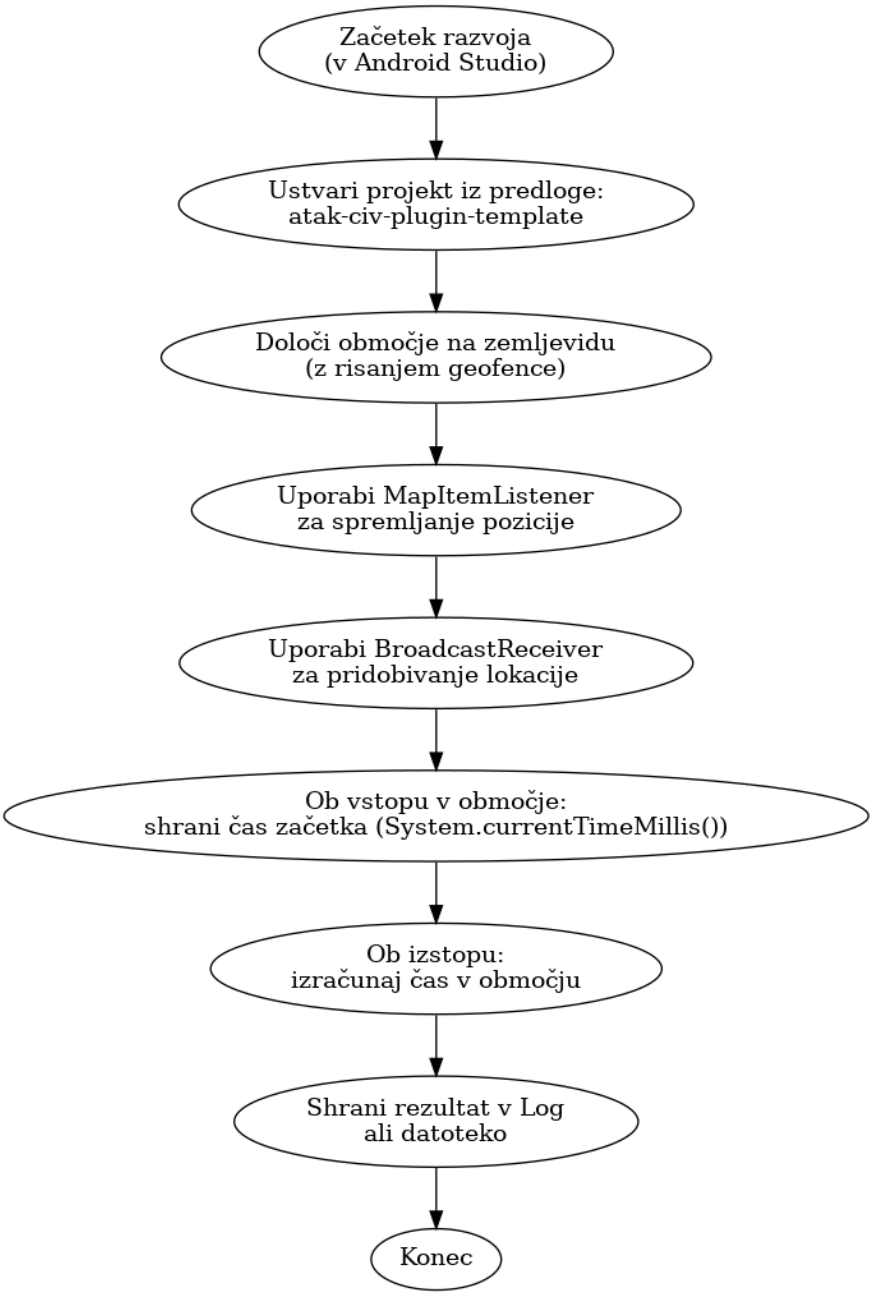
- Uporabnik ročno določi območje v obliki kroga ali poligona
- Sistem zazna vstop/izstop v območje
- Beleženje časa znotraj območja
- Izvoz rezultatov v obliki CSV, TXT ali prikaz v dnevniku
- Možnost več območij

4.3 Scenarij uporabe

- Taktične patrulje in nadzor nad zadrževanjem
- Zbirne točke in časovna optimizacija
- Simulacija varovanja območij (civilna zaščita, logistika)

4.4 Načrt razvoja vtičnika

4.4.1 ATAK-CIV (Java, Android)



Slika 25 Diagram Poteka ATAK-CIV

Vir: Lastni vir

Na prikazani sliki je prikazan diagram poteka razvoja vtičnika "Time-in-Zone Monitor" za ATAK-CIV. Proces se začne z uporabo orodij, kot so Android Studio, ATAK Plugin SDK in komponenta BroadcastReceiver. Nato sledijo tehnični koraki: ustvarjanje vtičnika iz predloge, določitev območja na zemljevidu, spremljanje pozicije z MapItemListenerjem ter merjenje časa ob vstopu in izstopu iz cone. Rezultat se nato shrani oziroma prikaže v dnevniku ali datoteki.določitev območja na zemljevidu, spremljanje pozicije z MapItemListenerjem ter merjenje časa ob vstopu in izstopu iz cone. Rezultat se nato shrani oziroma prikaže v dnevniku ali datoteki.

V nadaljevanju je predstavljena slika izvorne kode.

```java
package com.atakplugin.timeinzone;

import android.util.Log;
import com.atakmap.android.maps.MapView;
import com.atakmap.android.maps.MapViewReceiver;
import com.atakmap.android.maps.Marker;
import com.atakmap.android.maps.ao.GeoPoint;
import com.atakmap.android.maps.ao.Rectangle;
import com.atakmap.coremap.log.LogWriter;

public class TimeInZonePlugin extends MapViewReceiver {

    private static final String TAG = "TimeInZonePlugin";
    private boolean insideZone = false;
    private long enterTime = 0L;
    private long totalTimeInZone = 0L;

    private final Rectangle monitoredZone = new Rectangle(
        new GeoPoint(46.0500, 14.4800), // Top left
        new GeoPoint(46.0450, 14.4900)  // Bottom right
    );

    @Override
    public void onLocationChanged(GeoPoint location) {
        boolean currentlyInside = monitoredZone.contains(location);

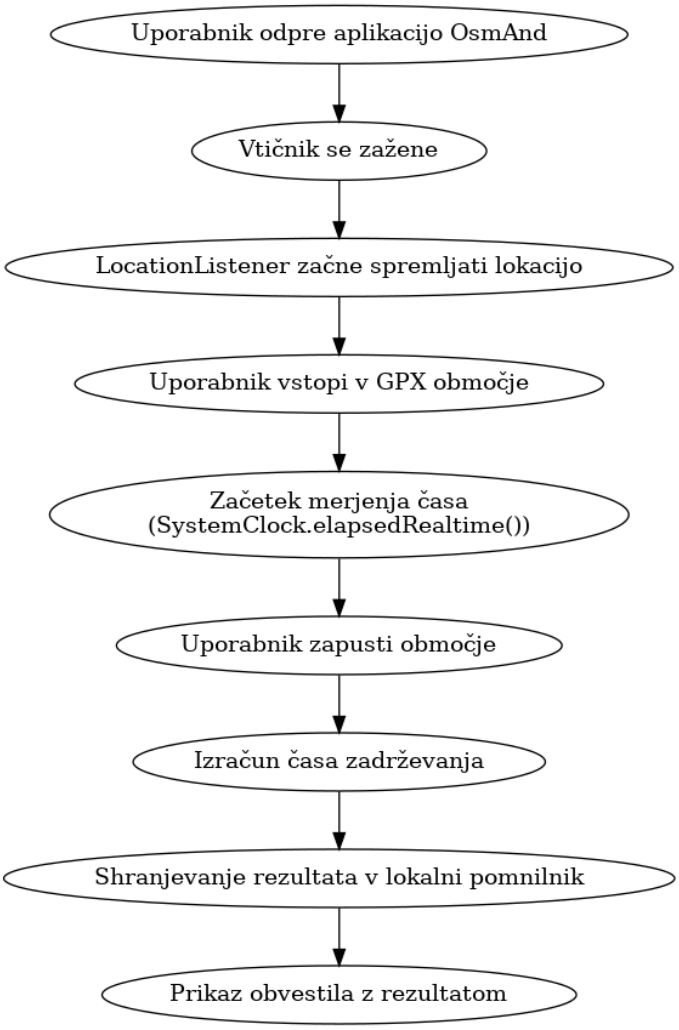
        if (currentlyInside && !insideZone) {
            enterTime = System.currentTimeMillis();
            insideZone = true;
            Log.d(TAG, "Entered zone at: " + enterTime);
        } else if (!currentlyInside && insideZone) {
            long exitTime = System.currentTimeMillis();
            totalTimeInZone += (exitTime - enterTime);
            insideZone = false;
            Log.d(TAG, "Exited zone. Time spent: " + (exitTime - enterTime) + " ms");
            LogWriter.write(TAG, "Total time in zone: " + totalTimeInZone + " ms");
        }
    }

    public long getTotalTimeInZone() {
        return totalTimeInZone;
    }
}
```

Slika 26 Vtičnik v ATAK-CIV

Vir: Lastni vir

4.4.2 OsmAnd (Java, OsmAndPlugin)



Slika 27 Diagram poteka OsmAnd

Vir: lasten

Uporabnik odpre aplikacijo OsmAnd, vtičnik začne spremljati lokacijo. Ko uporabnik vstopi v vnaprej določeno območje (GPX poligon), se začne merjenje časa. Ob izhodu iz območja se rezultat shrani in prikaže uporabniku

V nadaljevanju je predstavljena slika izvorne kode.

```
package net.osmand.plugin.timeinzone;

import android.location.Location;
import android.os.SystemClock;
import android.widget.Toast;

import net.osmand.data.LatLon;
import net.osmand.plus.OsmandApplication;
import net.osmand.plus.activities.MapActivity;
import net.osmand.plus.views.OsmandMapTileView;

public class TimeInZoneMonitor {

    private final OsmandApplication app;
    private final MapActivity mapActivity;
    private final OsmandMapTileView mapView;

    private boolean insideZone = false;
    private long enterTime = 0L;
    private long totalTimeInZone = 0L;

    // Define a simple rectangular zone (approximate area)
    private final double latMin = 46.0450;
    private final double latMax = 46.0500;
    private final double lonMin = 14.4800;
    private final double lonMax = 14.4900;

    public TimeInZoneMonitor(MapActivity activity) {
        this.mapActivity = activity;
        this.mapView = activity.getMapView();
        this.app = activity.getMyApplication();
        startMonitoring();
    }

    private void startMonitoring() {
        app.getLocationProvider().addLocationListener(location -> {
            double lat = location.getLatitude();
            double lon = location.getLongitude();
            boolean currentlyInside = (lat >= latMin && lat <= latMax && lon >= lonMin && lon <= lonMax);
```

Slika 28 Prvi del kode

Vir: Lastni vir

```
            if (currentlyInside && !insideZone) {
                enterTime = SystemClock.elapsedRealtime();
                insideZone = true;
                showToast("Vstopili ste v območje.");
            } else if (!currentlyInside && insideZone) {
                long exitTime = SystemClock.elapsedRealtime();
                long session = exitTime - enterTime;
                totalTimeInZone += session;
                insideZone = false;
                showToast("Izstop iz območja. Čas zadrževanja: " + (session / 1000) + " s");
            }
        });
    }

    private void showToast(String message) {
        mapActivity.runOnUiThread(() ->
            Toast.makeText(mapActivity, message, Toast.LENGTH_SHORT).show()
        );
    }

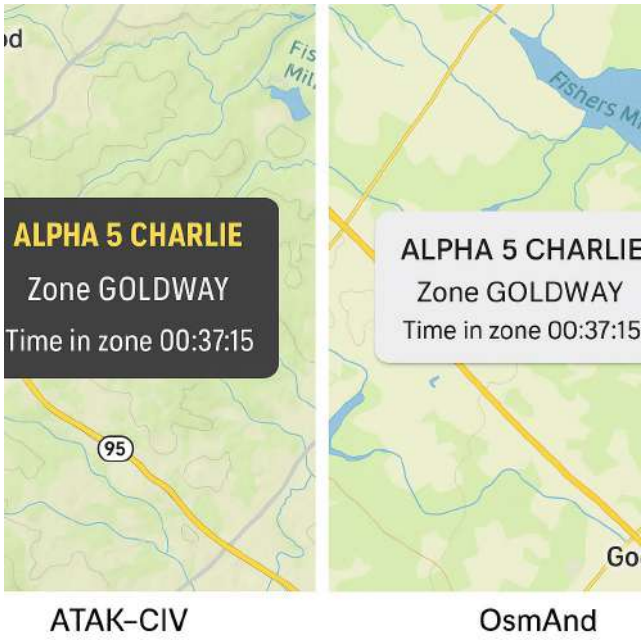
    public long getTotalTimeInZone() {
        return totalTimeInZone;
    }
}
```

Slika 29 Drugi del kode

Vir: Lastni vir

4.5 *Rezultat izvorne kode*

Prikaz rezultatov v uporabniškem vmesniku vtičnika Time-in-Zone Monitor jasno odraža razliko v arhitekturi in zasnovi obeh platform.



Slika 30 Rezultat izvorne kode vtičnikov

Vir: Lastni vir

Na sliki sta prikazana uporabniška vmesnika vtičnika Time-in-Zone Monitor za sistema ATAK-CIV (levo) in OsmAnd (desno), ob zaznavi vstopa uporabnika z imenom ALPHA 5 CHARLIE v območje Zone GOLDWAY.

Pri ATAK-CIV se rezultat prikaže znotraj integriranega uporabniškega vmesnika aplikacije, skupaj z dodatnimi podatki o položaju, imenu enote in času zaznave. Vtičnik je zagnan kot sestavni del aplikacije in ima neposreden dostop do zemljevida, markerjev in sistemskih funkcij.

Pri OsmAnd je rezultat prikazan z uporabo zunanjega obvestila, saj aplikacija ne omogoča notranje integracije vtičnikov. Vtičnik deluje kot samostojna aplikacija in komunicira z OsmAnd preko API-ja. Ob zaznavi vstopa v cono sproži preprosto vizualno obvestilo.

Razlika med sistemoma je očitna: ATAK-CIV nudi globljo integracijo in bogatejši prikaz, kar potrjuje večjo primernost za taktične potrebe. OsmAnd ostaja primeren za osnovne scenarije, kjer zadostuje zunanja obdelava podatkov.

5 PREDLOGI IN MOŽNOSTI NADGRADNJE

5.1 Predlogi in možnosti nadgradnje

Diplomska naloga je bila usmerjena v primerjalno analizo dveh odprtokodnih mobilnih platform – **ATAK-CIV** in **OsmAnd,** ki sta namenjeni orientaciji, kartografiji in situacijskemu zavedanju na terenu. Glavni namen je bil raziskati, katera izmed platform je bolj primerna za uporabo v taktičnih in varnostno-kritičnih okoljih, ob tem pa ugotoviti, kako se razlikujeta z vidika modularnosti, uporabnosti, zaupanja in kibernetske zaščite.

V nalogi so bile postavljene štiri hipoteze, ki so bile sistematično obravnavane z uporabo **kombiniranega raziskovalnega pristopa**, pri čemer so bile uporabljene tako **kvalitativne metode** (analiza dokumentacije, uporabniška izkušnja, delovanje v terenskem okolju) kot **kvantitativni elementi** (primerjava funkcionalnosti, razvoj osnovnega vtičnika za vsako platformo).

5.2 Povzetek doseženih ciljev

V procesu raziskave so bili zastavljeni cilji v celoti doseženi, kar potrjuje sistematičnost in uspešnost raziskovalnega pristopa. Najprej je bila izvedena poglobljena analiza modularnosti obeh sistemov, ki je omogočila razumevanje njihovih arhitekturnih značilnosti ter različnih možnosti za razvoj in vključevanje dodatnih funkcionalnosti. Rezultati so pokazali, da ima ATAK-CIV zaradi svoje zasnove in vojaškega izvora bolj strukturiran pristop k modularnosti, medtem ko OsmAnd kot odprtokodni projekt ponuja večjo fleksibilnost, a zahteva tudi več tehničnega znanja za prilagoditve.

Nadalje je bil prikazan primer osnovnega vtičnika za vsak sistem, kar predstavlja pomemben praktični prispevek raziskave. Ta del je omogočil vpogled v proces razvoja razširitev in potrdil hipoteze o zahtevnosti implementacije v posameznem okolju. Ob tem je bilo mogoče primerjati, v kolikšni meri sta oba sistema dostopna razvijalcem in kako učinkovito podpirata razširljivost.

Tretji dosežen cilj je bila ocena uporabnosti obeh sistemov v taktičnih scenarijih, kjer so bile upoštevane zahteve realnega operativnega okolja, kot so stabilnost, odzivnost, preglednost prikaza in enostavnost uporabe v stresnih pogojih. Analiza je pokazala, da se ATAK-CIV bolje izkaže v situacijah, kjer je potrebna visoka stopnja usklajenosti in zaščite komunikacij, medtem ko je OsmAnd bolj primeren za individualno ali civilno uporabo, kjer ni nujno potrebno izpolnjevanje strogih varnostnih standardov.

Na koncu je bila izvedena primerjava stopnje zaupanja in kibernetske zaščite, ki je potrdila razlike med sistemoma. ATAK-CIV se je izkazal kot robustnejši in varnostno bolj zanesljiv, saj vključuje preverjene šifrirne protokole in je večkrat preizkušen v realnih vojaških ter kriznih razmerah. OsmAnd pa kljub temu, da je zasnovan kot odprtokodni projekt in zagotavlja osnovno raven zasebnosti, ne dosega enake stopnje zaščite in zaupanja, ki jo zahtevajo kompleksni taktični scenariji.

Skupno gledano so bili tako zastavljeni cilji ne le doseženi, temveč je raziskava ponudila tudi širši vpogled v praktične izzive in možnosti razvoja mobilnih sistemov za situacijsko zavedanje.

5.3 Potrditev ali ovržba hipotez

5.3.1 H1: Razvoj vtičnika za sistem ATAK-CIV je enostavnejši in bolj modularen kot v sistemu OsmAnd.

Potrjeno zato, ker ATAK-CIV omogoča:

- **uradni SDK,**
- **večji dostop do sistemskih komponent,**
- **boljšo integracijo z aplikacijo.**

OsmAnd ne omogoča prave integracije, temveč le interakcijo preko Android Intents.

5.3.2 H2: ATAK-CIV je v primerjavi z OsmAnd primernejši za taktično premikanje in terensko vodenje enot.

Potrjeno zato, ker ATAK-CIV vključuje funkcije, kot so:

- **sledenje enotam,**
- **taktična označba,**
- **skupna raba podatkov v realnem času in delo v mreži.**

OsmAnd teh funkcij nima.

5.3.3 H3: Ocena varnosti in zaupanja je boljša pri ATAK-CIV kot pri OsmAnd.

Potrjeno, ker je ATAK-CIV je preizkušen v operativnih razmerah in ima vgrajene varnostne funkcije.

Medtem ko OsmAnd nima nadzora dostopa, ni šifriranja, niti ne omogoča delovanja v omrežju.

5.3.4 H4: ATAK nudi višjo raven kibernetske zaščite kot OsmAnd.

Potrjeno saj ATAK omogoča:

- **delovanje v zaprtem okolju,**
- **uporablja šifrirane povezave (TLS),**
- **omogoča digitalno podpisovanje.**

medtem ko OsmAnd nima mehanizmov kibernetske zaščite.

5.4 Ključne ugotovitve raziskave

- ATAK-CIV predstavlja sistem z večjo globino, nadzorom in prilagodljivostjo, vendar zahteva več tehničnega znanja in virov za implementacijo.
- OsmAnd je enostavnejši za uporabo in konfiguracijo, vendar neprimeren za varnostno zahtevna okolja brez bistvenih sprememb izvorne kode ali dodatne varnostne infrastrukture.
- Uporaba vtičnika kot merilo modularnosti je pokazala, da je ATAK primernejši za specializirane nadgradnje, saj omogoča tesno integracijo z uporabniškim vmesnikom in sistemskimi podatki.
- V taktičnih primerih, kjer je potrebna zanesljivost, združljivost in zavarovana komunikacija, OsmAnd ni primerna izbira brez bistvenih prilagoditev.

5.5 Predlogi za nadgradnjo

Na podlagi izvedene primerjave so oblikovani naslednji predlogi za nadaljnji razvoj in uporabo:

Za ATAK-CIV:

- Spodbuja se širša uporaba odprtokodnega SDK-ja z boljšo dokumentacijo za civilne organizacije.
- Priporočljivo je razviti uporabniško prijazne vmesnike za hitrejšo integracijo taktičnih orodij v nevladnih strukturah (npr. prostovoljna zaščita in reševanje).
- Razviti je smiselno univerzalne vtičnike za prenos podatkov med ATAK-CIV in drugimi sistemi (skladnost z GIS orodji, kot je QGIS).

Za OsmAnd:

- Predlagana je uvedba dodatnih varnostnih slojev, npr. osnovna TLS podpora pri prenosu podatkov (s pomočjo zunanjih orodij).
- Razvoj vtičnikov bi lahko izboljšal sistemski okvir in dvignil platformo izven običajnega navigacijskega konteksta.
- Za uporabo v zaščitnih enotah bi bilo priporočljivo ustvariti ločeno različico z možnostjo sodelovanja v skupinskih operacijah.

6 SKLEP

Diplomska naloga se je osredotočila na celovito primerjalno analizo dveh odprtokodnih mobilnih aplikacij za situacijsko zavedanje – ATAK-CIV in OsmAnd – z vidika njihove primernosti za uporabo v zahtevnih varnostno-taktičnih okoljih. Namen naloge je bil raziskati, katera izmed platform nudi boljšo podporo operativnemu delovanju v kriznih razmerah, ob tem pa preučiti tudi uporabnost odprtokodnih rešitev pri razvoju specializiranih funkcionalnosti.

Skozi teoretični pregled literature, praktično testiranje ter razvoj in implementacijo lastnega vtičnika "Time-in-Zone Monitor" za obe platformi so bile preverjene štiri raziskovalne hipoteze. Te so vključevale oceno modularnosti, razvojne fleksibilnosti, stopnje kibernetske zaščite ter zaupanja in stabilnosti aplikacij pri uporabi na terenu. Raziskovalni proces je združeval kvalitativne metode (analizo dokumentacije, uporabniško izkušnjo iz šestmesečne mednarodne misije z uporabo ATAK-CIV) ter empirične primerjave razvojnih postopkov, funkcionalnosti in varnostnih mehanizmov.

Rezultati raziskave jasno kažejo, da ATAK-CIV nudi bistveno bolj razvit in prilagodljiv sistem za integracijo vtičnikov. Modularna arhitektura omogoča visoko stopnjo razširljivosti, kjer lahko razvijalci s pomočjo uradnega SDK-ja, dobro dokumentirane predloge in dostopa do internih funkcij sistema razvijejo kompleksne funkcionalnosti, ki so lahko povsem prilagojene operativnim potrebam uporabnikov. Sistem poleg tega izpolnjuje visoke varnostne standarde, omogoča delovanje v izoliranih omrežjih, šifrira komunikacijo in omogoča nadzor uporabnikov ter pravic dostopa. Takšen pristop se je izkazal kot ključnega pomena v okoljih, kjer so podatki občutljive narave, uporabniki razpršeni, komunikacija pa časovno občutljiva.

OsmAnd se na drugi strani uveljavlja kot robustna in uporabniku prijazna odprtokodna rešitev, ki je še posebej primerna za civilne in nevladne organizacije, prostovoljce, pohodnike ali manj kompleksne reševalne operacije. Nudi visoko kakovostne zemljevide, zanesljivo delovanje brez internetne povezave in podporo za osnovno vizualizacijo podatkov. Vendar pa njegovo omejeno jedro ne omogoča neposredne integracije kompleksnejših funkcij, prav tako ne dosega iste stopnje kibernetske zaščite in uporabniške kontrole kot ATAK-CIV. Kljub temu njegova odprtokodnost ponuja določen potencial za razvoj prilagojenih rešitev, vendar to zahteva dodatno infrastrukturo ali znatne spremembe izvorne kode.

Razviti vtičnik Time-in-Zone Monitor je služil kot praktično orodje za testiranje razvojnega okolja na obeh platformah in za validacijo predpostavk. V primeru ATAK-CIV je bil vtičnik integriran neposredno v uporabniški vmesnik aplikacije in je v realnem času omogočal sledenje prisotnosti enot znotraj določene geografske cone. V primeru OsmAnd pa je bilo mogoče funkcionalnost uresničiti le z zunanjo aplikacijo, ki je prek API-ja pošiljala podatke v OsmAnd, kar je zahtevalo več obvodov in omogočilo precej manjšo stopnjo nadzora.

Sklepna ugotovitev naloge je, da ATAK-CIV bistveno presega OsmAnd, kadar gre za profesionalno, taktično ali varnostno rabo, medtem ko OsmAnd ohranja pomembno vlogo v civilnih scenarijih z manjšo stopnjo kompleksnosti. Naloga tako ni zgolj potrdila obstoječe prakse, temveč je tudi odprla nova vprašanja o uporabi odprtokodnih rešitev v okolju, kjer so ključni zaupanje, zanesljivost in varnost. S tem prispeva k širšemu razumevanju prednosti in omejitev posameznih pristopov.

V prihodnje bi bilo smiselno raziskati možnosti nadaljnjega razvoja vtičnikov, ki bi nadgradili funkcionalnost sistema s podporo za zunanje senzorje, komunikacijske module, biometrične podatke ali algoritme strojnega učenja, ki bi omogočali samodejno zaznavanje dogodkov in analizo terenskih vzorcev. Poleg tega bi nadaljevanje raziskave lahko vključevalo še širšo primerjavo drugih odprtokodnih sistemov, kot so WinTAK, Team Awareness Kit-Gov, SitaWare Edge in podobni, ter evalvacijo njihove operativne uspešnosti v realnih pogojih. Eden izmed pomembnih izzivov, ki ostaja odprt, je tudi standardizacija protokolov in kompatibilnost med civilnimi in vojaškimi sistemi ter razvijanje vmesnikov, ki omogočajo varno in nadzorovano povezovanje različnih aplikacij.

Tako predstavlja ta naloga temelj, na katerem je mogoče graditi napredne funkcionalnosti, primerjalne študije in razvojno strategijo za prihodnje odprtokodne rešitve v kriznem upravljanju, humanitarnem odzivanju ali obrambnih aplikacijah.

7 VIRI IN LITERATURA

Ahmad, H. D. (januar 2022). Cryptography and Security. *A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures*. Cornel University. Pridobljeno september 2025 iz https://arxiv.org/abs/2104.11906

ATAK. (19. maj 2019). Android Team Awareness Kit or ATAK / CivTAK. ATAk. Pridobljeno 26. julij 2025 iz https://www.reddit.com/r/ATAK/wiki/index

Bellini, E. (2025). Članki o povezavi med SA in odpornostjo proti kibernetskim grožnjam. *Situacijsko zavedanje za kibernetsko odpornost: pregled. Journal of Big Data*. Pridobljeno september 2025 iz https://www.sciencedirect.com/science/article/pii/S1874548225000162

Dehghan, M. &. (2024). *Advancing Situation Awareness Systems: Evaluating Decision-Making Methods with UAV Applications.* ResearchGate. Pridobljeno iz researchgate.net/publication/386873572_Advancing_Situation_Awareness_SystemsEvaluating_Decision-Making_Methods_with_UAV_Applications?utm_source

Franke, U. (2015). *Cyber situational awareness issues and challenges.* (FOI, Ured.) Pridobljeno iz https://www.foi.se/download/18.473b50381836a23846c27/1664270233610/Cyber_situational_awareness_FOI-S--6522--SE.pdf?utm_source

Jiang, L. J. (2021). Sistematiziran pregled vizualizacij za kibernetsko situacijsko zavedanje. Pridobljeno september 2025 iz https://arxiv.org/abs/2112.10354

Mullins, R. (julij 2020). Understanding and Enabling Tactical Situational Awareness in a Security Operations Center. Research Gate. Pridobljeno september 2025 iz https://www.researchgate.net/publication/342670827_Understanding_and_Enabling_Tactical_Situational_Awareness_in_a_Security_Operations_Center

Munir, A. (2024). Trustworthiness of Situational Awareness: Significance and Quantification. *MDPI*, 240. Pridobljeno iz https://www.mdpi.com/2624-800X/4/2/11?utm_source

National Institute of Standards and Technology. (september 2020). Security and Privacy Controls for Information Systems and Organizations . Pridobljeno september 2025 iz https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

OsmAnd. (1. junij 2010). OsmAnd uradna spletna stran. Pridobljeno 2025. avgust 2025 iz https://osmand.net

OsmAnd. (brez datuma). OsmAnd offline Maps and Navigation. OSMAND. Pridobljeno 26. julij 2025 iz https://osmand.net/docs/intro

r/ATAK- Forum. (9. maj 2019). Pridobljeno avgust 2025 iz Reddit: https://www.reddit.com/r/ATAK/wiki/index