



PROJEKTNA NALOGA S TEHNIČNO SPECIFIKCIJO ZA NADGRADNJO SISTEMA UPRAVLJANJA PROMETA NA OBČINSKIH CESTAH





KAZALO

1	SEZNAM KRATIC	5
2	UVOD	7
2.1	Kaj prinaša C-ITS za MOL?	7
2.2	Kakšno je stanje področju semaforizacije v MOL?	7
2.3	Kakšne bodo dejanske spremembe na področju prometa v MOL?	7
3	CILJI MOL V OKVIRU PROJEKTA X4ITS	9
3.1	Nadgradnja informacijskega sistema v Centru za upravljanje prometa MOL	10
3.1.1	Kontekst informacijskih rešitev CUP	10
3.1.2	Vsebniki informacijske rešitve MOL-ITS	12
3.1.3	Vsebnik CUP API storitve	16
3.1.4	Hierarhični pogled arhitekture MOL-ITS	18
3.1.5	Zahteve za nadzorno ploščo v Centru za upravljanje prometa MOL	21
3.2	Nadgradnja naprav na cestni infrastrukturi MOL	23
3.2.1	Glavni cilji nadgradnje	25
3.2.2	Zahteve za detekcijo prometa	26
3.2.3	Zahteve za detekcijo pešcev in kolesarjev	28
3.2.4	Zahteve za prednostno uporabo vozil javnega prevoza in vozil s prednostjo	31
3.2.5	Zahteve za informacijske tehnologije v križišču	33
3.2.6	Zahteve za posodobitev semaforских naprav	47
3.2.7	Prihodnja razširitev: varnostna kamera PTZ in snemanje skorajšnjih nesreč	49
3.2.8	Ključni kazalniki uspešnosti	51
3.3	Izvedba povezlivosti z Nacionalno točko dostopa	52
3.3.1	Nabori podatkov MOL za objavo	53
3.3.2	Objava na NAP.si v okviru MOL C-ITS	53
3.3.3	Vsebnik NAP Adapter (DATEX II)	53
3.3.4	Podatkovni tokovi in nabori podatkov	56
3.3.5	Operativno delovanje	56





3.4	Izvedba povezljivosti z nacionalnim sistemom C-ITS	57
3.4.1	Nacionalni sistem C-ITS.....	57
3.4.2	Zahteve za vzpostavitev sistema C-ITS v MOL.....	58
3.4.3	Sistemska arhitektura C-ITS Vozlišče.....	59
3.4.4	Izmenjava z nacionalnim vozliščem (NCUP).....	60
3.4.5	Funkcionalni scenariji.....	61
3.5	Izvedba prototipne rešitve na testnem območju.....	62
3.5.1	Obstoječe stanje	62
3.5.2	Obseg predvidenega območja za prototipno rešitev	62
3.5.3	Pristop k nadgradnji obstoječe prometne infrastrukture.....	66
4	Projektni načrt za implementacijo MOL-ITS sistema	70
4.1	Pregled projekta	70
4.2	Časovni načrt projekta	70
4.3	Struktura delovnih paketov	70
4.3.1	DP1: Projektno vodenje in upravljanje	70
4.3.2	DP2: Analiza in načrtovanje sistema	71
4.3.3	DP3: Infrastruktura in platforme	72
4.3.4	DP4: Razvoj osnovnih mikroservisov	73
4.3.5	DP5: C-ITS integracija	74
4.3.6	DP6: Pametna cestna infrastruktura	75
4.3.7	DP7: Uporabniški vmesnik in nadzorna plošča	76
4.3.8	DP8: Integracije z zunanjimi sistemi.....	76
4.3.9	DP9: Testiranje in validacija	77
4.3.10	DP10: Uvajanje v produkcijo	78
4.4	Ključni mejniki.....	78
4.5	Kvalitativni kriteriji	79
4.5.1	Funkcijski kriteriji	79
4.5.2	Nefunkcijski kriteriji	79
5	Repozitorij izvirne kode in dokumentacija.....	80





5.1	Repozitorij in predaja izvirne kode	80
5.2	Tehnična dokumentacija	80
5.3	Uporabniška dokumentacija	80
6	PRILOGA 1: Mikroservisi in REST API metode MOL-ITS	82
7	PRILOGA 2: Specifikacija adapterja za krmilnik semaforja	83
8	PRILOGA 3: Konfiguracije krmilnih programov križišč (semaforjev) v referenčnem zapisu JSON	84
9	PRILOGA 4: Specifikacija računalniške in strojne opreme za CUP	85
9.1.1	Infrastruktura strojne opreme nadzornega centra CUP	85
9.1.2	Arhitektura podatkovnega centra	85
9.1.3	Specifikacija strežniške omare	88





1 SEZNAM KRATIC

AMQP	Odpri standardni protokol za izmenjavo sporočil. Namenjen je omogočanju medopravilnosti med različnimi implementacijami sporočilnih sistemov. (ang. Advanced Message Queuing Protocol)
API	Aplikacijski programski vmesnik (angl. Application Programming Interface)
BI	Osnovni komunikacijski vmesnik za izmenjavo C-ITS sporočil med podsistemi C-ITS, vozili, cestno infrastrukturo ter drugimi elementi v prometnem sistemu (ang. Basic Interface)
C-ITS	Kooperativni inteligentni prometni sistemi (angl. Cooperative Intelligent Transport Systems)
CAM	Infomacija o statusu in položaju vozil (ang. Cooperative Awareness Message)
CIVITAS	Evropska pobuda za urejanje mestnega prometa (CIty-VITality-Sustainability),
DENM	Obvestilo o nevarnem dogodku (ang. Decentralized Environmental Notification Message)
FLS	Facility Layer Services (FLS) so del inteligentnih transportnih sistemov (ITS), ki zagotavljajo komunikacijske funkcionalnosti med različnimi aplikacijami in storitvami znotraj ITS. FLS omogočajo izmenjavo podatkov in sporočil med vozili, infrastrukturo in drugimi komponentami v prometnem sistemu.
HLN	Opozorilo o nevarnih lokacijah (ang. Hazardous Locations Notification)
HLN-TJA	Opozorilo o približevanju prometnemu zastoju (ang. Traffic Jam Ahead)
HLN-SV	Opozorilo o stoječem vozilu na cesti (ang. Stationary Vehicle)
HLN-WCW	Opozorilo o vremenskih razmerah (ang. Weather Condition Warning)
HLN-ERVI	Informacija o intervenciji vozil s prednostjo (ang. Emergency or Rescue/Recovery Vehicle in Intervention)
HLN-EPVA	Opozorilo o približevanju vozila s prednostjo (ang. Emergency or Prioritized Vehicle Approaching)
HLN-RLX	Informacija o stanju na nivojskih železniških prehodih (ang. Railway Level Crossing)
HLN-PTVS	Informacije o vozilih javnega potniškega prometa na postajališčih (ang. Public Transport Vehicle at a Stop)
II	Vmesnik, ki izboljša medopravilnost in učinkovitost izmenjave podatkov med različnimi segmenti C-ITS ekosistema (ang. Improved Interface)
IJPP	Integrirani javni potniški promet
ITS	Inteligentni transportni sistemi (angl. Intelligent Transport Systems)
ITS-g5	Evropski standard za ad-hoc komunikacijo kratkega dosega vozil med seboj (V2V) in s postajami ITS na cestah (V2I). ITS-g5 se nanaša na standard IEEE 802.11p, ki uporablja frekvenčni pas 5,9 GHz za podporo varnostnim in ne-varnostnim aplikacijam ITS
IVIM	Sporočilo o infrastrukturi in prometni signalizaciji (ang. Infrastructure to Vehicle Information Message)
IVS	Prenos prometne signalizacije v vozilo (ang. In-Vehicle Signage)





IVS-TS	Sporočilo o prometni signalizaciji: prometni znaki
IVS-FT	Sporočilo o prometni signalizaciji: prosto besedilo
MAPEM	Sporočilo, namenjeno prenosu topoloških podatkov o prometnem omrežju (ang. Map Extended Message)
NAP	Nacionalna točka dostopa
NCUP	Nacionalni center za upravljanje prometa
NEZ	Nacionalna evidenca zapor, ki jo je vzpostavil NCUP
OBU	Enota v vozilu, ki omogoča sprejemanje in oddajanje C-ITS sporočil (ang. On Board Unit)
PGIS	Prometni geografski informacijski sistem, ki ga je vzpostavil NCUP
PKI	Infrastruktura javnih ključev (ang. Public Key Infrastructure)
RSU	Obcestna ITS postaja (ang. Road Side Unit - roadside ITS station)
RWW	Opozorilo o delih na cesti
RWW-LC	Opozorilo o zaprtem voznem pasu (ang. Lane closure (and other restrictions))
RWW-RC	Opozorilo o zapori ceste (ang. Road Closure)
RWW-RM	Informacije o premični zapori ceste zaradi del (ang. Road Works - Mobile)
SI-GLOSA	Svetovanje voznikom o optimalni hitrosti za vožnjo skozi zeleno luč (ang. Signalized Intersections-Green Light Optimal Speed Advisory)
SPATEM	Informacija o fazah in časih prometnih signalov (ang. Signal Phase And Timing Extended Message)
SREM	Zahtevek za določeno fazo signala semaforja (ang. Signal Request Extended Message)
SSEM	Sporočilo o statusu zahtevka za signalizacijo (ang. Signal request Status Extended Message)
TEN-T	Vseevropsko prometno omrežje (angl. Trans-European Transport Network)
V2V	Izmenjava sporočil med vozili (ang. vehicle-to-vehicle)
V2I	Izmenjava sporočil med vozilom in infrastrukturo C-ITS (ang. vehicle-to-infrastructure)
X4ITS	Naziv evropskega projekta »Central European cross – border cooperation for ITS«





2 UVOD

Projekt X4ITS je evropski projekt za izboljšanje upravljanja prometa, v katerem sodeluje tudi Mestna občina Ljubljana (MOL). Glavni cilj je nadgradnja mestnega prometnega sistema z uporabo inteligentnih transportnih sistemov – ITS in kooperativni ITS – C-ITS. Inteligentni transportni sistemi (ITS) so tehnološke rešitve, ki omogočajo zbiranje, analizo in uporabo prometnih podatkov za boljše upravljanje prometa.

Poleg MOL sta slovenska partnerja v projektu še Nacionalni center upravljanja prometa v okviru Ministrstva za infrastrukturo (MZI – NCUP oz. NCUP) in Družba za avtoceste v Republiki Sloveniji d.d. (DARS).

2.1 Kaj prinaša C-ITS za MOL?

Sočasno se opredeli tudi vso potrebno opremo za vzpostavitev Kooperativnega Inteligentnega transportnega sistema (C-ITS).

Funkcionalnost C-ITS za MOL omogoča sinhronizirano izmenjavo sporočil (SPaT, MAP, DENM, CAM) in komunikacijo V2X z nizko latenco z namenom izboljšane komunikacije med infrastrukturo, vozili in centralnimi storitvami. To poveča situacijsko ozaveščenost, omogoča hitro zaznavo in takojšnje obveščanje o nevarnostih ter podpira storitve, kot je GLOSA, ki voznikom oziroma sistemom v vozilih svetuje optimalno hitrost za prehod skozi križišča z minimalnim številom zaustavitev. Posledično se izboljša varnost (zgodnje opozarjanje in preprečevanje nevarnih dogodkov), poveča pretočnost (dinamična optimizacija semaforizacije, usklajevanje z GLOSA in prilagajanje faz glede na prometne vzorce). Dodatno se zmanjšajo emisije in čas potovanja. Integracija C-ITS in V2X z MOL ITS omogoča proaktivno upravljanje, boljše dolgoročno načrtovanje in ustvarja podlago za naprednejšo avtomatizacijo mobilnosti ob spoštovanju zasebnosti podatkov.

2.2 Kakšno je stanje področju semaforizacije v MOL?

V Ljubljani imamo 292 semaforiziranih križišč, od tega 58 semaforiziranih prehodov za pešce in kolesarje.

Križišča so različno opremljena in različnih topologij. Obstoječi sistem načeloma dobro deluje, vendar je v občutnem deležu na skrajni zmogljivosti delovanja ter deluje le statično z v naprej določenimi fiksnimi krmilnimi programi. Trenutna oprema ne omogoča dinamičnega krmiljenja semaforizacije - enostavnega in hitrega prilagajanja trenutnim prometnim razmeram. Vse željene spremembe delovanj posameznih krmilnih naprav (krmilni programi,...) je treba zdaj spremeniti ročno na mestu samem ter tudi ni možna konkretna analitike prometa v realnem času (potrebno štetje prometa in podobno).

Vse te nadgradnje ni mogoče izvesti brez celovitega posega v infrastrukturo, tako v križiščih (na cesti) kot še posebej pomembno, treba je nadgraditi in modernizirati nadzorni center za vodenje in upravljanje prometa - CUP.

2.3 Kakšne bodo dejanske spremembe na področju prometa v MOL?

V okviru izvajanja projekta X4ITS je načrtovana nadgradnja in modernizacija CUP in nadgradnja 41 prometno reguliranih križišč na trasi Tržaška cesta, Bleiweisova, Tivolska in Dunajska cesta (pilotno območje).

Predvidene aktivnosti so;

- Modernizacija in nadgradnja Centra za upravljanje prometa mesta Ljubljana (CUP). CUP je digitalno središče za upravljanje mestnega prometa z neposrednim vpogledom v stanje





semaforjev, možnostjo spreminjanja delovanja križišč, vpogledom v stanje cest in križišč v realnem času, izmenjava podatkov med napravami in sistemi ter z državnim centrom (NCUP).

- Modernizacija obstoječe semaforske infrastrukture:
 - zamenjava in nadgradnja neustreznih krmilnih naprav
 - vgradnja detekcijskih sistemov za analitične namene (kamere, računalniške enote v semaforih napravah,...)
 - nadgradnja sistema za obveščanje in zaznavanje pešcev in kolesarjev
 - zamenjava halogenskih signalnih dajalcev na LED tehnologijo
 - zamenjava in nadgradnja neustreznih tipk za pešce (zvočni signal za slepe in slabovidne, ...)
- Vzpostavitev sistema GLOSA na ključnih križiščih (na vstopno/izstopnih točkah koridorjev za vzpostavitev zelenega vala), dodatno nameščeni dinamični LED-zasloni, ki voznikom brez opreme V2X vizualno prikazujejo priporočeno hitrost za optimalni pretok prometa (zeleni val).
- Vgradnja obcestnih (RSU) enot za komunikacije med sistemi (C-ITS) na ključnih točkah (križiščih).





3 CILJI MOL V OKVIRU PROJEKTA X4ITS

MOL želi v okviru projekta X4ITS izvesti nadgradnjo sistema upravljanja prometa na občinskih cestah in izboljšati povezljivost s sistemi ITS in NAP na nacionalnem nivoju.

Cilji MOL za sodelovanje v projektu so izhajali iz želje po iskanju tehničnih rešitev za naslednje aktualne in prihodnje izzive:

- Povečanje količine podatkov iz vse večjega števila virov (detektorji, semaforji, javni prevoz, parkirni sistemi, meteorološki senzorji)
- Integracija multimodalnih podsistemov (pešci, kolesarji, vozila, električni skuterji, logistika)
- Digitalizacija in interoperabilnost z nacionalnimi in evropskimi arhitekturami ITS
- Potreba po napovedni analitiki namesto zgolj reaktivnega delovanja
- Usklajevanje v kriznih in načrtovanih situacijah (intervencije, dela, nesreče, ekstremne vremenske razmere, množični dogodki)

Za dosego teh ciljev je potrebno izvesti naslednje naloge:

- Tehnična nadgradnja informacijskega sistema v Centru za upravljanje prometa (CUP) v MOL (MOL-ITS) na način, ki bo omogočal učinkovitejše upravljanje prometa na občinskih cestah
- Nadgradnja cestne infrastrukture z napravami, ki bodo CUP omogočale učinkovitejše zbiranje podatkov o prometu in posledično njegovo učinkovitejše upravljanje
- Izvedba povezljivosti z zunanjimi sistemi, Nacionalno točko dostopa (NAP) v okviru Nacionalnega centra za upravljanje prometa (NCUP) in nacionalnim vozliščem C-ITS.

Za vse informacijske rešitve bo izvedena prototipna rešitev na območjih:

- Pilotno območje: 41 križišč na trasi Dunajska cesta – Tivolska cesta – Bleiweisova cesta – Tržaška cesta. Gre za ceste strateškega pomena za radialni prometni sistem Ljubljane, ki predstavljajo hrbtenico povezav z regionalno cestno infrastrukturo.
- V nadaljnjih fazah se prenova razširi na celotno območje MOL.

Tehnična nadgradnja MOL-ITS mora omogočati zbiranje, shranjevanje in analizo prometnih podatkov za kar potrebujemo kvalitetne prometne podatke, ki jih pridobimo iz naprav cestne in obcestne infrastrukture.

Za pridobivanje prometnih podatkov so potrebne naprave za zaznavanje prometa in klasifikacijo vozil in ostalih udeležencev v prometu. Za učinkovitejše upravljanje prometa bo potrebna posodobitev infrastrukturne opreme na cesti, vključno s podpornimi sistemi:

- sistem za prometno odvisno krmiljenje semaforjev,
- sistem za vzpostavitev zelenih valov,





- sistem za prioritarno vožnjo vozil na nujni vožnji in prioritarno vožnjo vozil javnega potniškega prometa

Sistem mora omogočati tudi:

- analizo in napoved prometnih obremenitev po kategorijah udeležencev v prometu
- prometno modeliranje z uporabo zbranih podatkov

V nadaljevanju je predstavljena specifikacija zahtev za celotni sistem.

3.1 Nadgradnja informacijskega sistema v Centru za upravljanje prometa MOL

MOL že leta sistematično razvija integriran prometni sistem, ki sledi načelom trajnostne urbane mobilnosti. Naraščajoča kompleksnost prometnih tokov, vse večja odvisnost od podatkov v realnem času in cilji podnebne nevtralnosti zahtevajo nadaljnjo nadgradnjo in funkcionalno širitev tega središča. V okviru CUP bo vzpostavljen informacijski sistem za integracijo informacijskih tokov in prometnih podatkov (MOL-ITS).

Minimalne prostorske in kadrovske zahteve za CUP:

- predvidena površina prostora je najmanj 40 m², strešniški prostor je lahko tudi na drugi lokaciji
- za stalno aktivno delovanje (po principu 24/7) je potrebnih 8 ljudi + IT strokovnjak + vodja

3.1.1 Kontekst informacijskih rešitev CUP

Kontekst informacijskih rešitev za CUP prikazuje Slika 1. Prikazana je povezanost sistema MOL-ITS z zunanjimi sistemi; nacionalnim vozliščem za C-ITS, nacionalno točko dostopa (NAP) in komunikacija z vozili z nameščenimi enotami C-ITS OBU (angl. On-Board Unit). C-ITS OBU je naprava, nameščena v vozilu, ki omogoča komunikacijo z drugimi vozili (V2V) in prometno infrastrukturo (V2I) v okviru kooperativnih inteligentnih transportnih sistemov.

Informacijska rešitev MOL-ITS je prikazana v odnosu do ključnih zunanjih akterjev in nacionalnih platform. Notranje podrobnosti (vsebniki/komponente) na tem diagramu niso prikazane; osredotoča se na to, kdo komunicira s sistemom in kako.

MOL-ITS zbira in obdeluje prometne podatke ter podpira operativno upravljanje prometa v MOL. Izvaja objave odprtih podatkov na nacionalni portal NAP. Izmenjuje C-ITS sporočila prek nacionalnega vozlišča C-ITS v skladu s specifikacijo Basic Interface (BI). Operater (upravljaliec) prometa dostopa do sistema prek nadzorne plošče (angl. dashboard), ki je del internega sistema, za spremljanje stanja, opozorila in ukrepanje. Postaja iz podatkovnih virov aplikacij ustvarja vsebino sporočil skladno s specifikacijami BI, ki jih opremi z lupino AMQP za pošiljanje preko omrežja. Sporočila so geo-locirana tako, da jih je mogoče ustrezno geografsko filtrirati pri posredovanju v relevantne dele omrežja. Prav tako so sporočila varnostno podpisana.

Nacionalna točka dostopa NAP je namenjena dostopu in objavi javnih naborov podatkov (npr. dela na cesti, zapore, dogodki). Namen implementacije povezljivosti z NAP je transparentnost, ponovna uporaba podatkov in skladnost z nacionalnimi politikami odprtih podatkov.

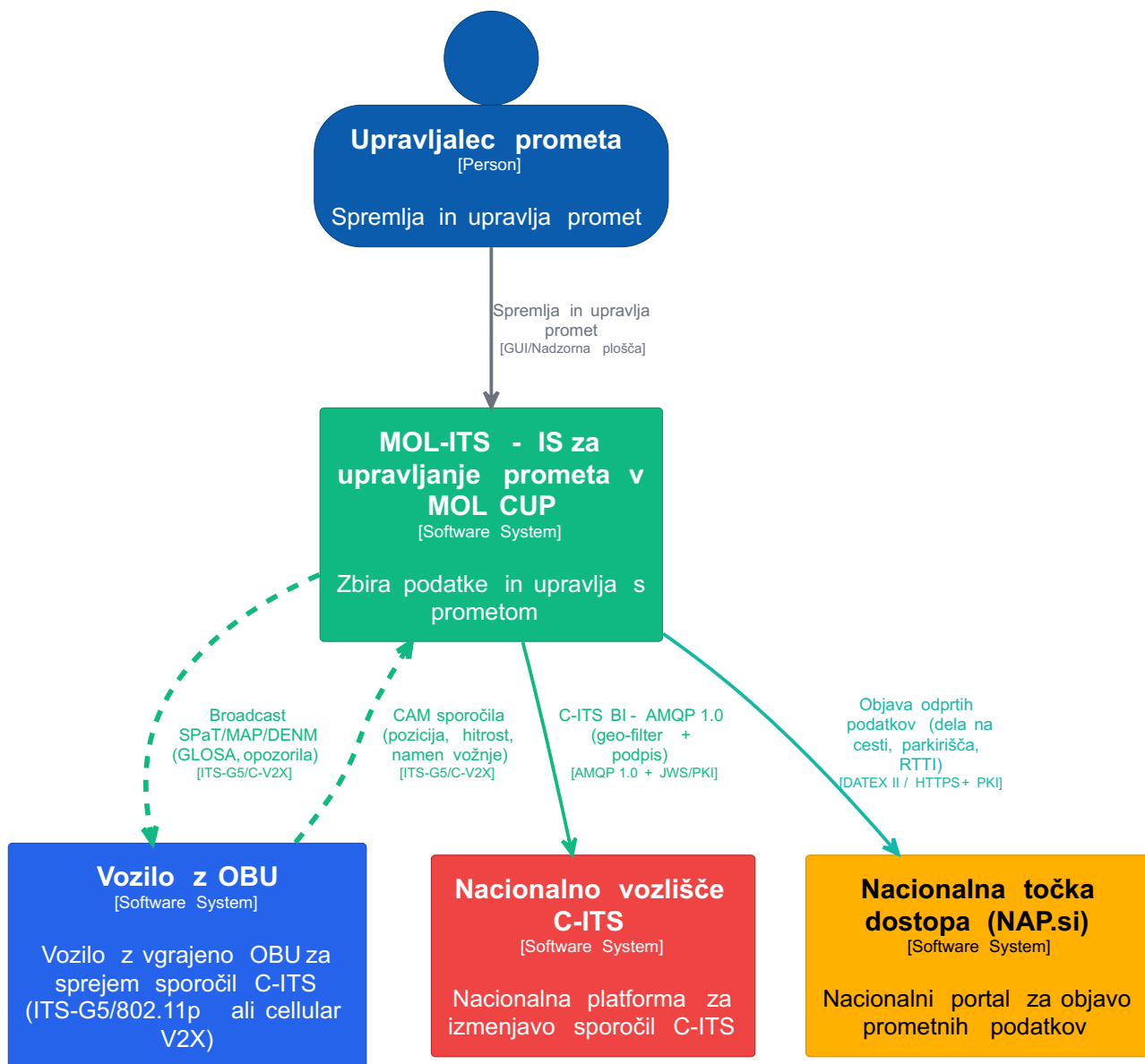
Nacionalno vozlišče C-ITS omogoča izmenjavo sporočil C-ITS prek BI (npr. CAM, DENM, IVI/SPaT/MAP, skladno z uveljavljenimi profili). Namen implementacije povezave z nacionalnim



vozliščem C-ITS je interoperabilna izmenjava prometno-varnostnih sporočil in storitev C-ITS z nacionalno platformo.

Slika 1 prikazuje »notranjost« CUP, to je njegove programske komponente. Na tem diagramu ima osrednjo vlogo MOL-ITS, ki je osrednja komponenta v tem arhitekturnem modelu.

X4ITS - Diagram konteksta informacijskih rešitev MOL CUP (rev: 2025-11-30)



Slika 1. Diagram arhitekture glavnih programskih rešitev za nadgradnjo CUP

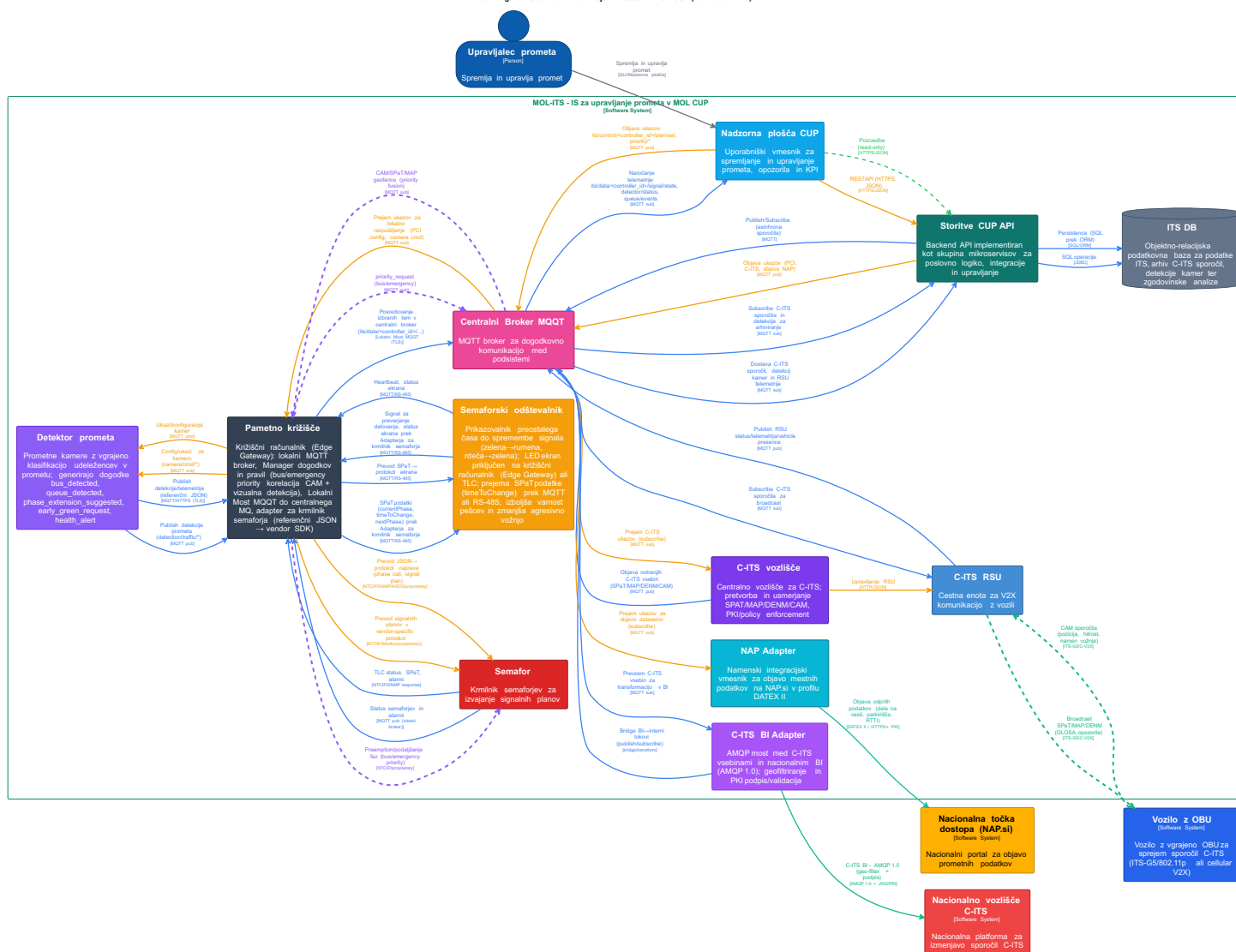


3.1.2 Vsebniki informacijske rešitve MOL-ITS

Slika 2 prikazuje vsebnike (angl. containers) sistema MOL-ITS, ki predstavlja srednjo raven abstrakcije v programskem arhitekturnem modelu CUP in ga razčlenjuje na posamezne tehnološke vsebnike, ki skupaj tvorijo celotno rešitev za upravljanje mestnega prometa. Medtem, ko kontekstni diagram (Slika 1) prikazuje MOL-ITS kot enoten sistem v interakciji z zunanjimi akterji in platformami, vsebniški pogled razkriva notranjo strukturo sistema in prikazuje sedem ključnih vsebnikov, njihove tehnološke značilnosti ter način komunikacije med njimi. Ta raven podrobnosti omogoča razumevanje, kako so različne funkcionalnosti sistema razdeljene med specializirane komponente, katere tehnologije so uporabljene za njihovo realizacijo ter kako poteka pretok podatkov in kontrolnih signalov skozi celotno arhitekturo.

Jedro sistema predstavlja CUP API (storitve), implementiran kot skupina mikroservisov, ki zagotavljajo poslovno logiko, integracije z zunanjimi sistemi ter upravljanje vseh notranjih podsistemov. CUP API deluje kot centralna koordinacijska točka, ki sprejema zahteve iz nadzorne plošče CUP, jih procesira prek poslovne logike, dostopa do podatkovnega skladišča (objektno-relacijske podatkovne baze, npr. PostgreSQL) ter komunicira z nacionalnimi platformami - nacionalnim vozliščem C-ITS s protokolom Basic Interface in nacionalno točko dostopa NAP za objavo odprtih prometnih podatkov. Mikroservisna arhitektura omogoča neodvisno povečevanje zmogljivosti (skaliranje) posameznih funkcionalnih enot, lažje vzdrževanje ter prilagodljivost pri dodajanju novih funkcionalnosti. Storitve API komunicirajo z vsemi notranjimi vsebniki preko vmesnikov REST API/HTTPS za sinhrono kontrolne operacije ter preko sporočilne vrste MQTT za asinhrono izmenjavo prometnih podatkov in dogodkov.

Nadzorna plošča CUP predstavlja uporabniški vmesnik, implementiran kot sodobna spletna aplikacija, ki prometnim operaterjem omogoča spremljanje trenutnega stanja prometa, upravljanje prometne infrastrukture, pregled opozoril in ključnih kazalnikov uspešnosti (KPI). Operaterji prek nadzorne plošče dostopajo do vseh funkcionalnosti sistema, kot npr. spremljajo pretok vozil na posameznih odsekih, upravljajo s semaforizacijo prek sistema pametne cestne infrastrukture, pregledujejo detekcije udeležencev iz prometnih kamer, spremljajo delovanje obcestnih enot RSU (angl. Road Side Units) ter koordinirajo odziv na prometne dogodke. Nadzorna plošča komunicira s storitvami CUP API preko protokola HTTPS/JSON, kar zagotavlja varno in učinkovito izmenjavo podatkov.



Slika 2. Diagram vsebnikov informacijske rešitve MOL-ITS



Grafični vmesnik nadzorne plošče vizualizira prometne razmere na zemljevidu mesta, prikazuje stanje vseh kritičnih sistemov ter omogoča konfiguracijo in upravljanje prometne infrastrukture.

Vsebnik C-ITS vozlišče predstavlja mestno vozlišče za kooperativne inteligentne transportne sisteme in deluje kot ključna povezava med mestno prometno infrastrukturo ter nacionalno platformo C-ITS. Ta vsebnik implementira funkcionalnosti za obdelavo, transformacijo in usmerjanje sporočil C-ITS, sporočil SPaT (angl. Signal Phase and Timing) s semaforiziranih križišč, sporočil MAP (angl. Map Data) z informacijami o topologiji prometne infrastrukture, sporočil DENM (angl. Decentralized Event Notification Messages) za obveščanje o prometnih dogodkih ter CAM (angl. Cooperative Awareness Messages) za ozaveščanje o prisotnosti vozil. C-ITS vozlišče komunicira z nacionalnim vozliščem C-ITS preko Basic Interface protokola, ki temelji na komunikaciji HTTPS/REST s certifikati PKI za zagotavljanje varnosti in zaupanja. Navzdol upravlja obcestne enote RSU preko kontrolnega vmesnika HTTP/JSON ter izmenjuje sporočila C-ITS in telemetrijo preko sporočilne vrste MQTT. Ta arhitektura omogoča centralizirano upravljanje funkcionalnosti C-ITS ter učinkovito distribucijo sporočil do enot RSU na terenu.

Obcestne enote RSU predstavljajo fizično infrastrukturo sistema za realizacijo komunikacije Vehicle-to-Everything (V2X). Te enote so strateško nameščene na križiščih s semaforizacijo, na območjih s povečanim tveganjem za prometne dogodke ter na vstopno-izstopnih točkah mestnega območja. Enote RSU podpirajo dve komplementarni tehnologiji za komunikacijo V2X, ETSI ITS-G5 standard (temelji na IEEE 802.11p), ki uporablja namenske radio frekvence v pasu 5.9 GHz za neposredno komunikacijo z vozili na kratkih razdaljah z nizko latenco, ter cellular V2X (C-V2X), ki izkorišča mobilna omrežja 4G/5G za komunikacijo na daljših razdaljah in v urbanih območjih z gosto pozidavo, kjer je neposredna radio povezava otežena. Enote RSU prejemajo sporočila SPaT in MAP od vozlišča C-ITS Vozlišče ter jih razširjajo do vozil v svojem dosegu, kar omogoča aplikacije, kot so opozorila o rdeči luči (angl. Red Light Violation Warning), optimizacija hitrosti za zeleni val GLOSA (angl. Green Light Optimal Speed Advisory) ter obveščanje o nevarnostih na cesti. Hkrati enote RSU zbirajo podatke o prisotnosti vozil, telemetrijo svojega delovanja ter diagnostične informacije, ki jih pošiljajo nazaj v sistem prek protokola MQTT. Ta dvosmerna komunikacija omogoča tako distribucijo sporočil C-ITS kot tudi nadzor nad delovanjem obcestnih enot.

Vozila z vgrajeno OBU (angl. On-Board Unit) predstavljajo mobilni del C-ITS ekosistema. OBU sprejema SPaT/MAP/DENM broadcast enote C-ITS RSU in v vozilu prikazuje GLOSA priporočila, opozorila na rdečo luč ter druge varnostne dogodke, hkrati pa periodično oddaja CAM sporočila (pozicija, hitrost, smer, namen vožnje) proti RSU. CAM sporočila se na RSU povežejo z lokalnimi detekcijami in se preko MQTT posredujejo v centralni sistem za arhiviranje in analitiko. Komunikacija OBU↔RSU poteka po ITS-G5/802.11p ali C-V2X, zaščitena z namensko PKI infrastrukturo, kar zagotavlja zaupnost in integriteto sporočil V2X.

V okviru pilotne implementacije bo OBU nameščen na omejenem številu testnih vozil (npr. testni osebni avtomobili) ter na izbranih avtobusih/JPP vozilih, da se v realnih prometnih razmerah preveri delovanje storitev (GLOSA, opozorila, prioriteta signalizacija) in interoperabilnost z RSU ter nacionalnim vozliščem.

Prometne kamere predstavljajo ključno komponento za zajem realnih prometnih podatkov in so implementirane kot naprave z vgrajenimi algoritmi za detekcijo in klasifikacijo udeležencev v prometu (angl. edge computing/AI). Ključna arhitekturna odločitev je, da kamere izvajajo procesiranje videa lokalno na sami napravi in v informacijsko infrastrukturo MOL-ITS ne prenašajo video tokov, temveč





samo strukturirane podatke o zaznanih udeležencih; kategorija (minimalno 8 kategorij: pešec, otroški voziček, invalidski voziček, kolesar, e-skiro, osebno vozilo, tovornjak, avtobus, in po možnosti še vozilo na nujni vožnji), čas, število, hitrost, lokacija po voznem pasu ter smer gibanja. Ta pristop prinaša več pomembnih prednosti: drastično zmanjšanje potrebne pasovne širine omrežja (namesto gigabajtov video podatkov sistem prenaša samo nekaj kilobajtov strukturiranih podatkov na minuto), zagotavljanje zasebnosti, saj surovi video posnetki ne zapuščajo naprave in se ne shranjujejo centralno, ter možnost implementacije kompleksnih algoritmov za detekcijo na zmogljivejši strojni opremi naprave namesto v centraliziranem podatkovnem centru. Kamere so napajane preko tehnologije PoE (angl. Power over Ethernet), kar poenostavlja namestitve, saj ni potrebna dodatna električna infrastruktura, en sam ethernet kabel zagotavlja tako prenos podatkov kot napajanje. Vse kamere delujejo znotraj varnega tunela VPN, kar zagotavlja šifriranje komunikacije in preprečuje nepooblaščen dostop. Podobno kot enote RSU tudi kamere uporabljajo hibridni komunikacijski vzorec, kontrolna raven (HTTPS/JSON) za upravljanje, konfiguracijo in posodobitve ter podatkovna raven (MQTT) za visokofrekvenčno pošiljanje detekcij in sprejem ukazov.

V primerjavi s pristopi, ki temeljijo na centralizirani ali lastniški analitiki video toka (npr. prenos RTSP/ONVIF videa v podatkovni center ali v ponudnikov oblak), pristop »edge AI + strukturirani dogodki« bistveno zniža operativne stroške in tehnična tveganja: (1) omrežje ni ozko grlo (ni potrebe po stalnem prenosu visokoločljivostnega videa), (2) latenca je manjša in bolj deterministična, ker se detekcija izvede lokalno in sistem lahko deluje tudi ob delnih izpadih povezljivosti (kamere še vedno zaznavajo in pošiljajo dogodke, ko je povezava na voljo), (3) zasebnost je privzeta (angl. privacy by design), ker se obdeluje in hrani zgolj anonimizirana, agregirana telemetrija namesto posnetkov, (4) zmanjšuje se odvisnost od enega dobavitelja (angl. vendor lock-in), saj je vmesnik do sistema definiran kot standardiziran nabor dogodkov/detekcij (MQTT/JSON), ne pa kot specifična lastniška platforma za analitiko videa. Takšna zasnova zato bolje podpira postopno nadgradnjo algoritmov (modeli na napravi), kombinacije dobaviteljev kamer ter transparentno arhiviranje in analitiko v okviru MOL-ITS.

Sporočilna vrsta, implementirana kot broker za MQTT, predstavlja osrednjo komponento za asinhrono komunikacijo med vsemi podsistemi. Protokol MQTT je posebej primeren za IoT in prometne aplikacije zaradi nizke latence, majhne porabe pasovne širine ter vzorca komunikacije publish/subscribe, ki omogoča enostavno dodajanje novih naprav brez potrebe po rekonfiguraciji obstoječih sistemov. Prek sporočilne vrste poteka izmenjava sporočil C-ITS med vozliščem C-ITS vozlišče in enotami RSU (SPaT/MAP/DENM/CAM), telemetrija enot RSU, podatki o detekcijah iz prometnih kamer ter ukazi za upravljanje obcestnih naprav.

Storitve CUP API se lahko naročajo na vse te podatkovne tokove in tako v realnem času procesirajo prometne dogodke, spremljajo stanje infrastrukture ter izvajajo analitiko za podporo odločanju. Asinhronost komunikacije omogoča, da težave na posamezni napravi ne blokirajo celotnega sistema, broker MQTT začasno shranjuje sporočila za nedosegljive naprave in jih dostavi, ko postanejo ponovno dostopne. Takoimenovano tematsko usmerjanje (angl. "topic-based routing") omogoča ločevanje sporočil za naprave ali servise, kar zmanjšuje obremenitev omrežja in izboljšuje varnost.

Podatkovna baza (predlog PostgreSQL) zagotavlja shranjevanje (angl. persistence) vseh podatkov sistema in mora biti zasnovana kot objektno-relacijska baza, ki združuje prednosti relacijskega modela s sodobnimi možnostmi za shranjevanje polstrukturiranih podatkov. Tradicionalne relacijske tabele se uporabljajo za strukturirane podatke, kot so konfiguracija naprav, zgodovina prometnih dogodkov,





uporabniški računi ter revizijske sledi. Formati JSON in JSONB omogočajo fleksibilno shranjevanje kompleksnih sporočil C-ITS, konfiguracijskih datotek ter podatkov iz kamer brez potrebe po vnaprejšnji definiciji stroge sheme. Razširitev PostGIS dodaja podporo za prostorske podatke in omogoča napredne geografske poizvedbe, iskanje vseh enot RSU ali kamer v določenem območju, izračun razdalj med lokacijami, analizo pokritosti prometne infrastrukture ter prostorsko korelacijo prometnih dogodkov. Razširitev TimescaleDB optimira shranjevanje in poizvedovanje časovnih vrst, kar je ključno za analizo prometnih trendov, zgodovinskih podatkov o obremenitvah, telemetrije naprav ter metrik KPI. Ta kombinacija tehnologij omogoča bazi podatkov, da učinkovito podpira tako operativne potrebe sistema v realnem času kot tudi analitične poizvedbe za načrtovanje in optimizacijo prometne infrastrukture.

Ključna funkcionalnost arhitekture MOL-ITS je sistemsko arhiviranje vseh sporočil C-ITS in detekcij iz prometnih kamer, kar omogoča prehod iz reaktivnega v proaktivno platformo za upravljanje mestnega prometa.

Ločitev med kontrolno ravni in podatkovno ravni komunikacije je temeljni arhitekturni vzorec v vsebniški arhitekturi MOL-ITS. Kontrolna raven uporablja sinhrono protokole HTTP/HTTPS za operacije, ki zahtevajo potrditev in takojšnji odgovor, konfiguracijo naprav, diagnostiko, ročne posege operaterjev, integracijo z zunanjimi sistemi. Ta komunikacija poteka preko vmesnikov REST API storitev CUP API, ki delujejo kot centralna točka za avtentikacijo, avtorizacijo in revizijo vseh kontrolnih operacij. Podatkovna raven uporablja asinhrono vzorce MQTT publish/subscribe za visokofrekvenčno izmenjavo prometnih podatkov, dogodkov in telemetrije, kjer takojšnja potrditev ni kritična, pomembna pa je nizka latenca in možnost distribucije istih podatkov večim prejemnikom. Ta ločitev omogoča neodvisno skaliranje obeh ravni, kontrolna raven je dimenzionirana za občasne operacije z visoko kompleksnostjo, podatkovna raven pa za kontinuiran tok velikih količin enostavnih sporočil.

Arhitektura MOL-ITS je zasnovana za visoko razpoložljivost, skalabilnost in prilagodljivost prihodnjim potrebam. Mikroservisna struktura CUP API omogoča horizontalno skaliranje posameznih funkcionalnosti glede na obremenitev, enostavno dodajanje novih funkcionalnosti brez vpliva na obstoječe ter postopno nadgrajevanje komponent brez prekinitve delovanja sistema. Uporaba koncepta »edge computing« za kamere in enote RSU zagotavlja, da sistem deluje tudi ob izpadih mrežne poveztivosti, naprave lahko začasno shranjujejo podatke in jih prenesejo, ko se poveztivost obnovi. Sporočilna vrsta MQTT z možnostjo shranjevanja in ponovnega pošiljanja zagotavlja zanesljivost komunikacije tudi v nestabilnih pogojih. Uporaba odprtih standardov (C-ITS Basic Interface, ETSI ITS-G5, MQTT) omogoča integracijo opreme različnih proizvajalcev ter interoperabilnost z rešitvami drugih mestnih območij (in držav). Kombinacija strukturiranih relacijskih podatkov, pol strukturiranih dokumentov JSON, prostorskih analiz in časovnih vrst v enotni podatkovni bazi omogoča podporo raznolikih uporabniških scenarijev, od operativnega upravljanja v realnem času do strateške analize in načrtovanja prometne politike.

3.1.3 Vsebnik CUP API storitve

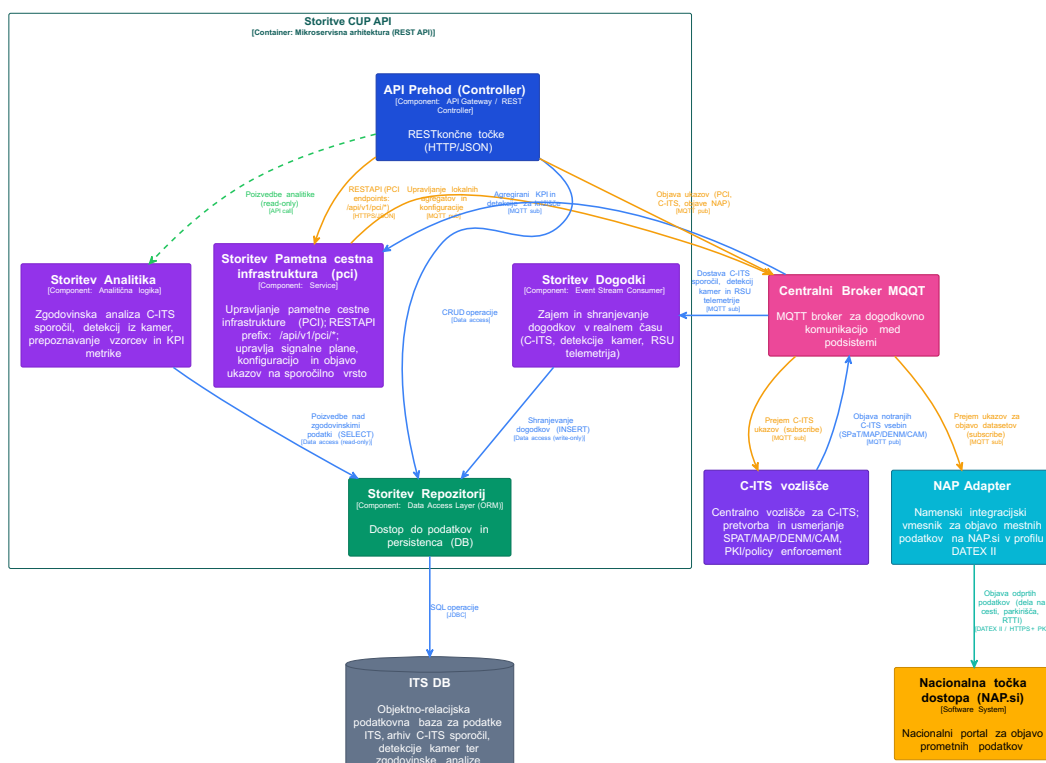
Interni pogled v CUP API storitve (Slika 3) prikazuje notranjo strukturo storitev API, ki tvorijo jedro sistema MOL-ITS za upravljanje mestnega prometa. Medtem ko kontekstni diagram prikazuje sistem MOL-ITS v odnosu do zunanjih akterjev in sistemov, kot so nacionalno vozlišče C-ITS, nacionalna točka dostopa NAP.si ter prometni operaterji, komponentni pogled razčlenjuje mikroservisno



arhitekturo znotraj vsebnika CUP API in razkriva, kako posamezne komponente vsebnika sodelujejo pri izvajanju poslovne logike, integraciji s podsistemi ter upravljanju podatkov. Kontekstni pogled torej odgovarja na vprašanje "kaj sistem počne in s kom komunicira", medtem ko komponentni pogled pojasnjuje "kako sistem interno realizira svoje funkcionalnosti".

Storitve CUP API so zasnovane kot skupina mikroservisov, kjer vsaka komponenta lahko deluje kot samostojen servis z lastno bazo podatkov in vmesnikom REST. Takšen pristop omogoča neodvisne cikle razvoja in namestitve novih ali posodobljenih verzij, lažje skaliranje posameznih funkcionalnih enot ter boljšo odpornost sistema proti izpadom. Arhitektura sledi vzorcu API Gateway in načelu CQRS: komponenta Controller je vstopna točka za poizvedbe HTTPS/JSON (QUERY, read-only), medtem ko ukaze in orkestracijo (CONTROL) objavlja asinhrono prek sporočilne vrste MQTT. Dogodke CONTROL prevzamejo specializirani servisi (C-ITS, PCI, NAP Adapter), poizvedbe QUERY pa Controller usmeri do ustreznih storitev (npr. Storitve Analitika) prek notranjih API-jev.

X4ITS - Komponentni pogled CUP API (mikroservisi: API Prehod (Controller)/Storitve CUP API/Storitev Repozitorij/Storitev Analitika/Storitev Dogodki/Storitev Pametna cestna infrastruktura (pci)/C-ITS Service) (rev: 2025-12-18)



Slika 3. Diagram s komponentami CUP API

Podatkovni tokovi in telemetrija prav tako tečejo prek MQTT. Ta pristop zagotavlja, da težave na posamezni napravi ne blokirajo celotnega sistema, saj sporočilna vrsta deluje kot centralna točka za distribucijo sporočil in lahko začasno hrani sporočila za nedosegljive odjemalce.

Storitev Dogodki je centralna točka za ingestijo: naroča na C-ITS sporočila, detekcije iz kamer in telemetrijo prek MQTT ter podatke konsistentno arhivira v ITS DB. Storitev Analitika deluje kot bralni (QUERY) odjemalec nad ITS DB in izvaja zgodovinske poizvedbe, KPI metrike, poročila in napredne



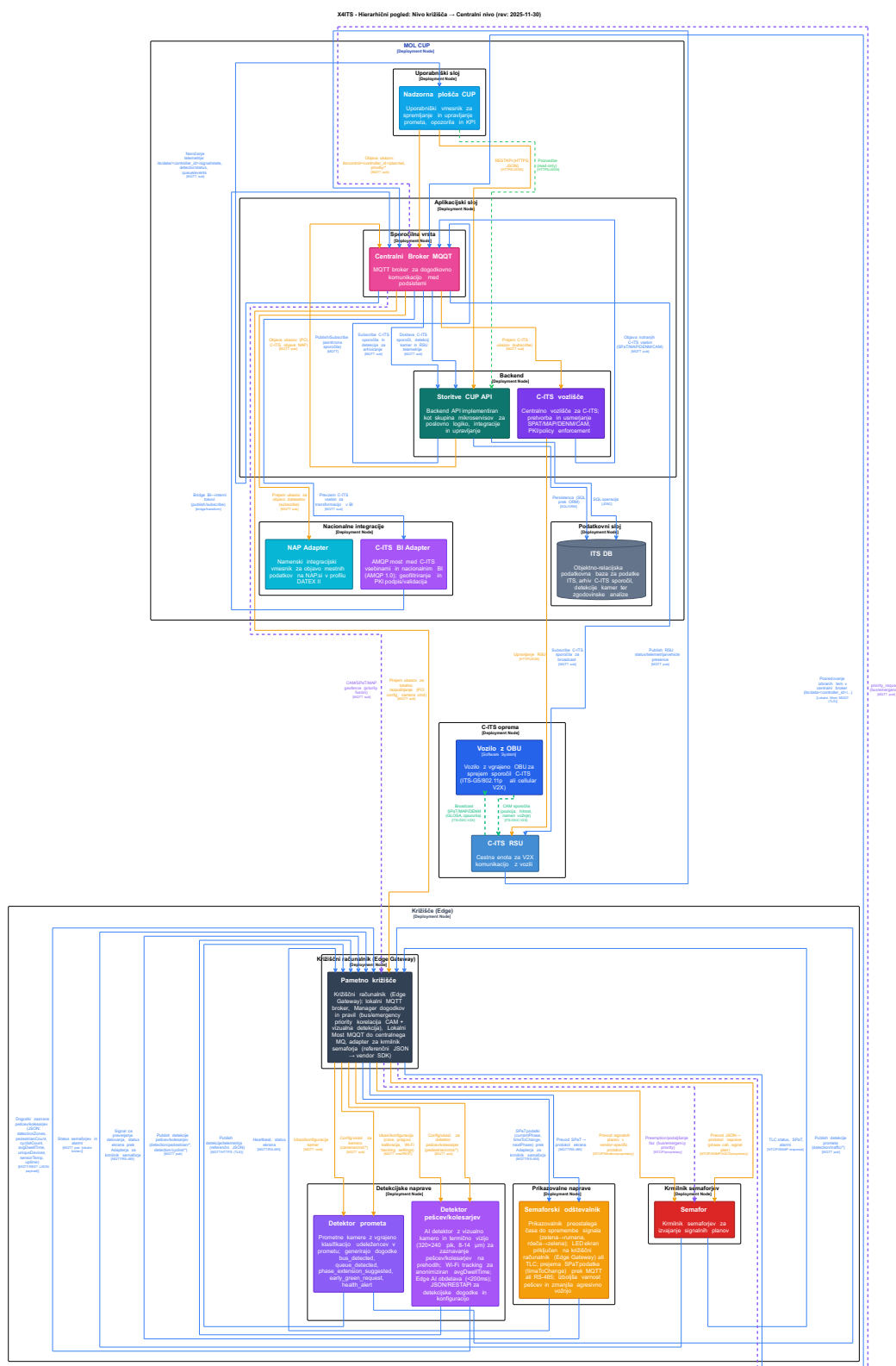
analize. TimescaleDB optimizacije omogočajo učinkovito shranjevanje in poizvedovanje velikih količin časovno zaporednih podatkov. Analitika izvaja prepoznavanje vzorcev zastojev, analizo učinkovitosti semaforizacije, detekcijo ponavljajočih se prometnih dogodkov na kritičnih točkah, validacijo natančnosti senzorjev ter izračun KPI metrik za podporo odločanju.

Storitev Analitika znotraj mikroservisne arhitekture CUP API, naroča (subscribe) na sporočilno vrsto MQTT ter prejema vsa sporočila SPaT (stanja semaforjev), MAP (topologija križišč), DENM (prometni dogodki), CAM (prisotnost vozil) ter detekcije prometnih udeležencev iz kamer. Ta sporočila takoj trajno shrani v podatkovno bazo prek komponente Storitev Repozitorij, ki zagotavlja konsistentno abstrakcijo podatkovnega sloja in transakcijsko integriteto. Ta zgodovinski arhiv omogoča več ključnih funkcionalnosti: prepoznavanje ponavljajočih vzorcev zastojev za optimizacijo semaforske logike, analizo učinkovitosti semaforskih intervalov in MAP sporočil glede na dejanske prometne tokove, validacijo natančnosti senzorjev s primerjavo podatkov iz različnih virov (kamere napram CAM sporočila vozil), rekonstrukcijo prometnih dogodkov pri preiskavi nesreč ali kršitev, izračun metrik KPI (povprečni časi potovanja, zanesljivost napovedanih časov, razpoložljivost infrastrukture) ter napovedovanje prometnih razmer z uporabo algoritmov strojnega učenja na zgodovinskih podatkih. Analitične funkcionalnosti omogočajo mestnim prometnim inženirjem identifikacijo sistemskih težav, vrednotenje učinkovitosti prometnih ukrepov ter optimizacijo parametrov prometne infrastrukture na podlagi evidenčnih podatkov namesto subjektivnih ocen.

3.1.4 Hierarhični pogled arhitekture MOL-ITS

Arhitektura MOL-ITS sistema je organizirana v dveh ključnih hierarhičnih nivojih, ki jasno ločujeta nivo križišča in centralni nivo obdelave prometnih podatkov ter nadzora. Ta logična razdelitev je prikazana v diagramu razporeditve (Slika 4), ki omogoča razumevanje fizične razporeditve komponent in njihovih komunikacijskih vzorcev.





Slika 4. Hierarhični pogled programske arhitekture MOL-ITS





Nivo križišča predstavlja prvi nivo obdelave, kjer se izvaja lokalna obdelava prometnega upravljanja neposredno na križiščih. Ta nivo vključuje križiščni računalnik (Pametno križišče), ki deluje kot osrednja točka za koordinacijo vseh lokalnih naprav: prometnih kamer (Detektor prometa), samostojnih detektorjev pešcev in kolesarjev (Detektor pešcev/kolesarjev) ter krmilnikov semaforjev (Semafor). Na Križiščnem računalniku (sinonim za angl. Edge Gateway) se izvaja lokalni posrednik MQTT za hitro komunikacijo z nizko zakasnitvijo med napravami, izvaja algoritme združevanja in agregacije za obdelavo podatkov detekcije v realnem času ter deluje kot protokolni adapter za pretvorbo ukazov v zapisu JSON v protokole posameznih proizvajalcev semaforških krmilnikov. Vgrajen je tudi mehanizem MQTT, ki izbrane teme posreduje v osrednji posrednik. Ta arhitektura omogoča hitro odzivnost sistema (npr. zelena faza za pešce v < 500 ms od zaznave) ter avtonomno delovanje križišča ob izpadu povezljivosti z osrednjim sistemom.

Osrednji nivo CUP je organiziran v štiri logične sloje, ki skupaj tvorijo jedro prometnega upravljanja.

Uporabniški sloj vsebuje Nadzorno ploščo CUP, ki operaterjem zagotavlja vizualizacijo stanja prometa, upravljanje s prometno infrastrukturo in dostop do analitičnih orodij.

Aplikacijski sloj združuje zaledne storitve (CUP API, C-ITS vozlišče, PCI) in Sporočilno vrsto, ki je ključno vozlišče za asinhrono izmenjavo podatkov med podsistemi in v smeri robnih naprav. Sporočilna vrsta posreduje ukaze za konfiguracijo in krmiljenje prek mehanizma MQTT do križiščnih računalnikov, medtem ko sprejema telemetrijo, podatke detekcij in statusna sporočila s terena.

Podatkovni sloj vsebuje ITS DB (PostgreSQL z razširitvami PostGIS, TimescaleDB, JSONB), ki shranjuje zgodovinske prometne podatke, C-ITS arhiv, konfiguracijske podatke križišč ter podpira analitične poizvedbe.

Zunanje komunikacije so razdeljene na dve skupini: V2X komunikacijo (RSU za oddajanje sporočil SPATEM/MAPEM vozilom) in nacionalne integracije (BI Adapter za AMQP izmenjavo z nacionalnim vozliščem C-ITS, NAP Adapter za objavo odprti podatkov v formatu DATEX II).

Komunikacijski vzorci med nivoji sledijo strogi arhitekturni politiki ločevanja odgovornosti. Naprave v križišču komunicirajo izključno z lokalnim križiščnim računalnikom, nikoli neposredno z osrednjimi storitvami. Križiščni računalnik izvaja funkcijo povezovanja (angl. bridge): lokalni dogodki in statusna sporočila se selektivno posredujejo v osrednjo Sporočilno vrsto (npr. agregirani KPI vsako minuto, alarmi takoj), medtem ko ukazi iz osrednjega sistema (npr. sprememba signalnega programa iz MOL PCI) potujejo prek Sporočilne vrste do ustreznega križiščnega računalnika, ki jih razporedi lokalnim napravam. Ta vzorec zagotavlja modularnost (angl. decoupling), omogoča razširljivost (dodajanje novih križišč brez sprememb osrednjega sistema) ter omogoča varno delovanje ob napakah (izpad osrednje povezave ne prekine avtonomnega delovanja križišča).

Prednosti hierarhične arhitekture vključujejo odpornost sistema (porazdeljeno procesiranje zagotavlja delovanje tudi ob izpadu povezave), zmanjšano omrežno obremenitev (samo relevantni agregati potujejo v CUP), prilagodljivost (od proizvajalca neodvisna referenčna shema za opis krmiljenja križišča omogoča enotno upravljanje opreme različnih proizvajalcev) in varnost (vse komunikacijske poti so zaščitene s TLS, mehanizem MQTT ima konfigurirane politike ACL). Diagram razporeditve



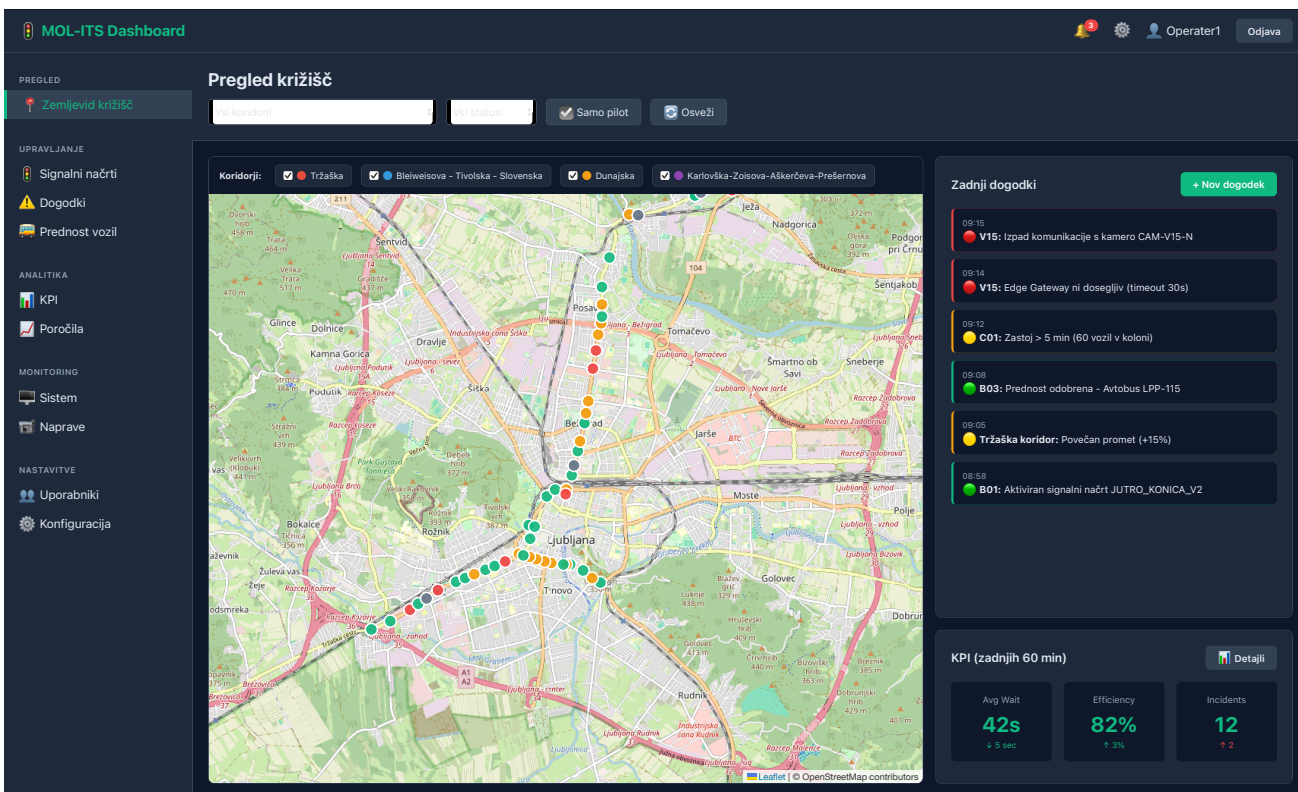


jasno prikazuje, da Sporočilna vrsta ni na istem nivoju kot naprave v križišču, temveč je osrednja infrastrukturna komponenta, ki omogoča dogodkovno vodeno arhitekturo in usklajevanje vseh podsistemov MOL-ITS.

3.1.5 Zahteve za nadzorno ploščo v Centru za upravljanje prometa MOL

Nadzorna plošča CUP je »okno« v živi prometni sistem mesta (Slika 5): operater pred sabo ne vidi zgolj statičnih ikon, temveč dinamičen zemljevid pulzirajočih koridorjev, barvnih stanj in majhnih časovnih indikatorjev faz. V ozadju se neprestano prepletajo trije komunikacijski tokovi, sinhroni REST klici za poizvedbe in upravljanje, stalni WebSocket/SSE kanal za drobnozrnat tok dogodkov ter posredni MQTT prehod, ki čisti ter agregira podatke iz križišč, da brskalnik ostane lahek in varen. Ta večslojna komunikacijska zasnova omogoča, da kritična sprememba (izpad komunikacije na križišču ali zahteva za avtobusno prednost) postane vidna v nekaj sekundah, medtem ko obsežnejša telemetrija (temperatura kamer, zasedenost CPU na križiščnem računalniku) prihaja z nekoliko daljšim intervalom, ne da bi obremenila izkušnjo.

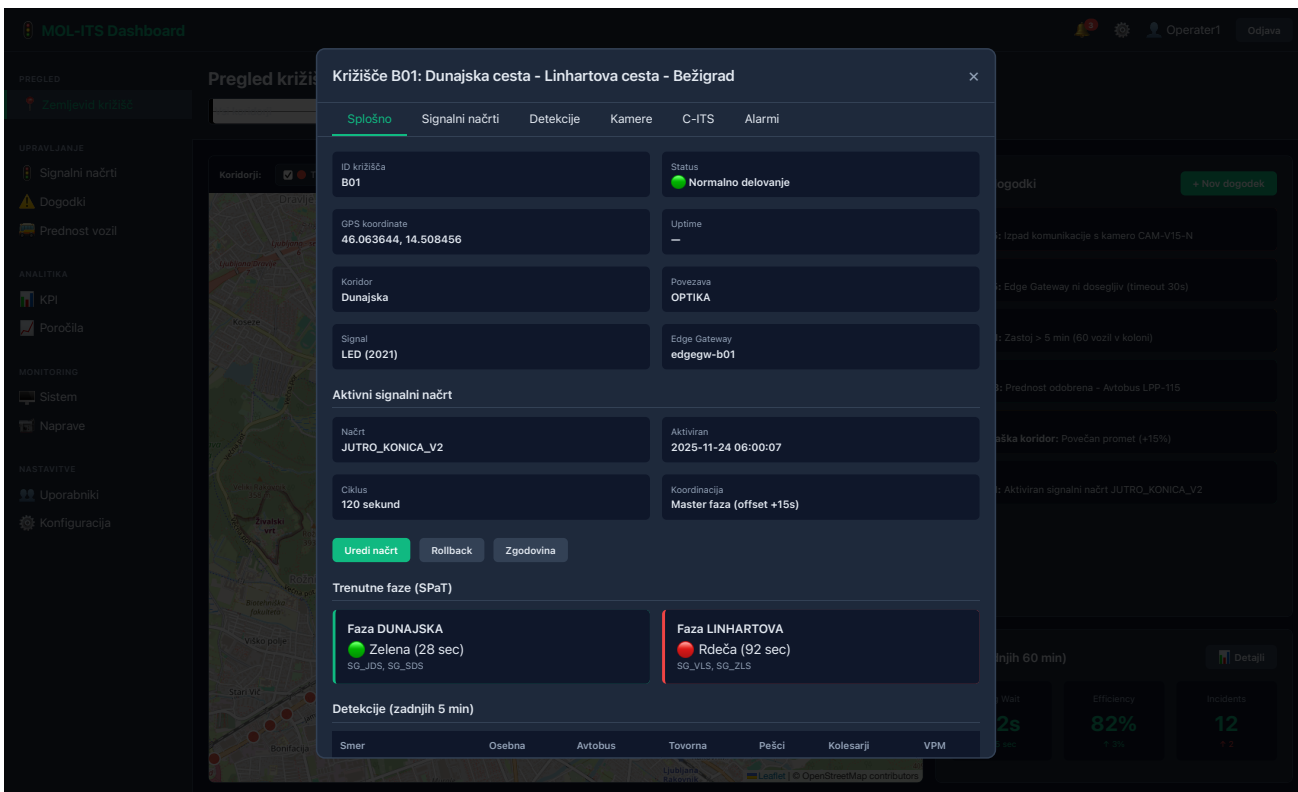
Ko operater pregleda glavni zaslon, ga najprej nagovori interaktivni zemljevid. Vsako križišče je označeno z barvo, ki intuitivno povzame stanje: zelena kot miren tok, rumena kot opozorilo zaradi naraščajočih kolon ali neoptimalnih časov, rdeča kot signal za neposredno ukrepanje (izpad, incident, kritična napaka), siva za objekti brez aktualnih podatkov ali začasno izven režima. Ikonografija ima izrazito informativno vlogo, razlike med križišči, prisotnost RSU enot, aktivna PTZ kamera ali dodatni detektor pešcev se vizualno zgoščajo v pregled, kjer je filtriranje po koridorjih, tipu opreme ali statusu takojšnje. V osnovni fazi obsega pilotnih 41 križišč arhitektura pa je zasnovana za razširitev nad 300, ne da bi se degradirala odzivnost.



Slika 5. Primer nadzorne plošče za aplikacije za spremljanje MOL ITS

Ob kliku na posamezno križišče se odpre detajlni pogled, kot tematsko strukturiran panel (Slika 6). Najprej osnovni identifikatorji (ID, naziv, GPS koordinata, povezljivost in uptime), nato trenutni signalni načrt z jasno prikazano aktivacijo, ciklusom ter koordinacijskim offsetom. Fazni prehodi so predstavljeni s preostalim časom (SPaT) in sklopom signalnih skupin, kar omogoča operaterju intuitiven občutek ritma križišča. Podatki o detekcijah niso gole številke, ampak kontekst: pretok (VPM, število vozil na minuto), klasifikacija udeležencev, dolžine kolon, povprečne hitrosti in krivulja zadnjih intervalov, vpogledi, ki pomagajo oceniti ali se prilagodljiva logika odziva skladno s pričakovanji. Sledi sloj kamer in senzorjev, kjer krožni indikatorji stanja razkrijejo temperaturo in trajanje delovanja, brez izpostavljanja videa. Če je prisotna PTZ varnostna kamera, se prikaz razširi z zadnjim forenzičnim posnetkom dogodka tveganja (skorajšnja nesreča, angl. nearmiss), pri čemer so povezave časovno omejene in revizijsko sledljive.

Upravljanje signalnih načrtov je zasnovano kot kontroliran potek: pregled knjižnice načrtov (jutranja konica, popoldne, vikend, prazniki, posebni dogodki), varnostnih parametrov (intergreen, konfliktne skupine) ter časovnih razmerij faz. Pred aktivacijo lahko operater izvede validacijo z referenčno shemo za opis krmiljenja križišča, pri kritičnih spremembah potrdi z dvofaktorsko avtentikacijo in dobi zagotovljen žeton za povrnitev (angl. “rollback”), ki omogoča povrnitev v prejšnje stanje znotraj kratkega varnostnega okna. Aktivacija ne pomeni slepega zaupanja, sistem namreč zahteva povratno potrdilo krmilnika (TLC) v manj kot treh sekundah; šele nato se sprememba zapiše v revizijski dnevnik skupaj z razlogom in primerjalno razliko v konfiguraciji.



Slika 6. Tematski panel za prikaz podrobnosti o križišču



Prometni dogodki se pojavljajo kot tekoč seznam časovno označenih vnosov: nesreče, zapore, nenadni zastoji, načrtovani posebni dogodki. Vsak vnos se lahko poveže z geografskim prikazom in sproži verigo: avtomatsko oblikovanje sporočila DENM, pošiljanje v NAP (če relevantno), predlog aktivacije alternativnega signalnega načrta ali ročno dodelitev prednosti vozilu na nujni vožnji. Incidentni posnetki, kjer obstajajo, so omejeni na kratke časovne odseke, šifrirani in dostopni le vlogam z ustreznimi privilegiji. Cilj ni naključno snemanje, temveč precizna forenzična sled, ki podpira varnostne izboljšave.

Analitika presega trenutni pogled. Operater in analitik lahko primerjata povprečni čas čakanja med koridorji, spremljata učinkovitost (angl. flow efficiency), razpoložljivost sistema in odzivni čas med detekcijo ter ukrepom. Tedenski in sezonski vzorci osvetlijo konice, napovedni modeli pa opozorijo na pričakovane zastoje naslednje ure. Poročila se izvažajo v PDF ali Excel ter so ob pogosti rabi pospešena z medpomnjenjem. Napoved prometnih tokov ni samostojen cilj, temveč podpora za proaktivno preklapljanje načrtov pred nastopom obremenitve.

Prednost za avtobuse in za vozila s prednostjo poteka kot jasna hierarhija zahtev (EMERGENCY > BUS > STANDARD). Operater vidi aktivne zahteve, njihov ETA do križišča, status (zahtevano / odobreno / izvršeno) in lahko po potrebi ročno sproži prednost ali mehko prioriteto. Latenca od zadnjega dogodka do odločitve ostaja nizka (cilj pod pol sekunde), sistem pa samodejno prekine zahteve, ki se niso uresničile v predvidenem časovnem okviru. Statistika uporabe prednosti se konsolidira za kasnejše evalvacije vpliva na povprečne čase vožnje.

Monitoring sistema zbere status porazdeljenega sistema: centralni strežniki (C-ITS prehodi, podatkovna baza, MQTT broker), vozlišča s kamerami na terenu, stanje kamer, RSU enot in semaforских krmilnikov. Latenca posredovanja, izgubljeni paketi in zasedenost pasovne širine so prikazani ob alarmih, ki izpostavijo resnost (kritično napram opozorilu). Ob kritičnih dogodkih sistem izvede eskalacijo (npr. epošta/SMS) in hkrati zapiše dogodek v trajno zgodovino za analizo vzrokov. Če backend začasno ni dosegljiv, nadzorna plošča ne zamrzne ampak preide v degradiran način, kjer prikazuje zadnje znane podatke ter označi, da spremembe niso dovoljene.

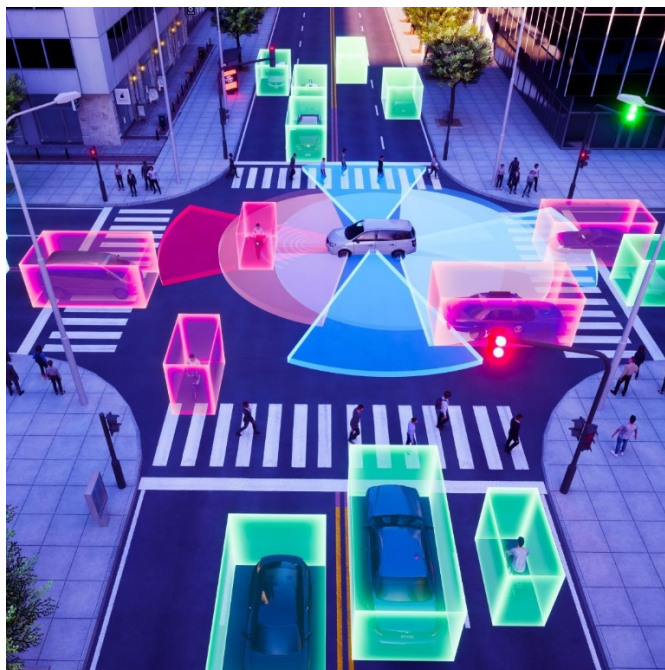
Upravljanje uporabnikov temelji na jasni delitvi vlog (administrator, operater, analitik, samo branje) in načelu najmanjših privilegijev. Dvofaktorska avtentikacija je obvezna za vse operaterje; časovne omejitve sej preprečujejo naključne zlorabe, medtem ko revizijski dnevnik beleži vsako spremembo konfiguracije ali nadzorno akcijo. Geografsko omejevanje dostopa (npr. koridor, specifična vidnost) omogoča specializacijo brez izpostavljanja celote.

Nefunkcijski vidiki so enako pomembni kot funkcionalni: odzivnost uporabniškega vmesnika mora omogočiti občutek tekočega dela (pod 200 ms za osnovne prikaze, pod 300 ms za detajlni panel), skalabilnost dopušča rast števila križišč in povezav brez naknadnega preoblikovanja arhitekture; visoka razpoložljivost ($\geq 99.9\%$) je dosežena z redundantnimi instancami in hitrim preklopom (angl. failover). Varnost se ne sklicuje le na TLS 1.3, temveč na konsistentno RBAC (angl. Role-Based Access Control.), strogi audit in prepoved neposrednega dostopa brskalnika do surovih tokov MQTT. Uporabniška izkušnja upošteva ergonomijo nadzorne sobe, temni način kot privzeto, tipkovne bližnjice za ponavljajoče se akcije in možnost preklopa v angleški jezik za mednarodno sodelovanje (C-ITS konteksti).

3.2 Nadgradnja naprav na cestni infrastrukturi MOL



Cilji nadgradnje naprav na cestni infrastrukturi MOL sledijo posodobitvi CUP in imajo prometno-tehnične cilje, ki jih lahko plastično ponazorimo z naslednjim opisom možne situacije na cestni povezavi Dunajska – Tivolska – Bleiweisova - Tržaška. IP-kamere z IR-osvetlitvijo in detektorji na prehodih za pešce v realnem času razvrščajo udeležence: pešci, kolesarji, eskiroji, osebna in tovorna vozila, avtobusi (Slika 7). Obdelava podatkov (križiščni računalnik) na lokaciji generira strukturirane dogodke (JSON), kategorija, smer, hitrost, gostota, dolžina kolone, ter jih prek MQTT objavlja na tematske sporočilne kanale (npr. detections/križišče123). Sistem MOL PCI prejme dogodke in lahko takoj optimira faze semaforja (skrajša nepotrebno rdečo, podaljša zeleno v smeri obremenitve), Sistem Storitev Analitika pa vse podatke trajno arhivira prek Storitev Repozitorij za poznejše KPI in napovedi. Surovi video nikoli ne zapusti križišča, zato zasebnost ostaja zaščitena.



Slika 7. Princip delovanja detekcije in klasifikacije udeležencev v prometu

Nekaj postaj pred križiščem se avtobus približuje po voznem redu. Njegov položaj GNSS/AVL se v CUP API pretvori v napoved prihoda (ETA) na naslednje križišče. CUP API storitve izvede pravila za prednost: če je avtobus v zamudi in so izpolnjeni varnostni pogoji, MOL PCI predlaga krmilniku prilagoditev faz (npr. kratko podaljšanje zelene ali pospešen prehod v zeleno). Če je lokacija opremljena tudi z napravo C-ITS RSU, lahko lokalna V2X interakcija (OBU↔RSU) dodatno zmanjša latenco pri aktivaciji prednosti. Zaščitni mehanizmi (anti-lock-in¹, maksimalna dolžina podaljšanja, koordinacija koridorjev) ohranjajo pretočnost celotnega omrežja.

¹ Anti lock-in je varnostni mehanizem pri adaptivnem krmiljenju in prioritetah, ki z omejitvami trajanja/številčnosti podaljšanj in minimalnimi zelenimi za nasprotno smeri preprečuje, da bi križišče zaradi ponavljajočih se zahtev (npr. OBU/AVL ali okvarjenih detektorjev) obstalo v dolgotrajni "zeleni" za eno smer.

Slika 8 prikazuje pešca (ali kolesarja), ki čaka na prečkanje. Namesto fizičnega pritiskanja gumba sistem samodejno odda »najavo«, tipka ostane le za zvočno pomoč slabovidnim. Krmilnik prejme zahtevek in v varnih mejah dinamično prilagodi zeleno fazo. Če detekcija začasno odpove, se sistem varno povrne na privzeti program.



Slika 8. Zaznavanje pešcev na pločniku pri prečkanju prehoda za pešce

V ozadju naprave C-ITS RSU na kritičnih točkah (na vstopno/izstopnih točkah koridorjev za vzpostavitev zelenega vala) oddajajo SPaT/MAP v vozila in sprejemajo CAM; ob dogodkih (npr. nenadna zapora) se izda DENM. GLOSA storitev svetuje optimalno hitrost za »zeleni val«. Naprava RSU komunicira z C-ITS Vozlišče (HTTP/JSON) in prek MQTT oddaja telemetrijo, certifikati PKI pa zagotavljajo zaupanje. Celoten tok informacij je poravnan z delovanjem Controller-ja (API Prehod), ki orkestrira klice, MOL PCI upravlja naprave, C-ITS vozlišče skrbi za sodelovalni komunikacijski ekosistem, Storitvev Repozitorij zagotavlja persistenco, Storitvev Analitika izvaja obdelavo, ki omogoča zgodovino dogodkov.

Prilagodljivi sistemi ITS za upravljanje prometa uporabljajo senzorje, kamere za detekcijo udeležencev v prometu in komunikacijske naprave (usmerjevalniki) za neprekinjeno zbiranje podatkov o prometnih tokovih. Na podlagi teh podatkov nadzorni algoritmi v (skoraj) realnem času prilagajajo dolžino zelene in rdeče faze na križiščih, s čimer vplivajo na optimalnejši prometni tok in posledično zmanjšajo zastoje. Omogočajo tudi zagotavljanje prednosti vozilom javnega prevoza, zlasti avtobusom, kar omogoča zmanjšanje njihovih zamud. CUP lahko intervenira tudi v primeru prometnih incidentov.

3.2.1 Glavni cilji nadgradnje

Seznam glavnih ciljev nadgradnje za podporo zgornjega prometno-tehničnega scenarija je sledeč:

- Detekcija prometa z AI kamerami v križiščih
- Klasifikacija udeležencev (minimalno 8 kategorij: pešec, otroški voziček, invalidski voziček, kolesar, e-skiro, osebno vozilo, tovornjak, avtobus, in po možnosti še vozilo na nujni vožnji, štetje, smer, hitrost, gostota, dolžina kolon.
- Delovanje v slabih razmerah (noč, megla, dež, sneg) z IR podporo ali termičnimi detektorji; brez prenosa videa v CUP.
- Detekcija pešcev in kolesarjev v križiščih/na prehodih



- Zamenjava tipk za »najavo« z video/termalno detekcijo; tipke ostanejo zgolj za zvočno signalizacijo za slepe in slabovidne.
- Dinamično prilagajanje faz (podaljšanje/skrajšanje zelene) glede na dejansko prisotnost pešcev/kolesarjev.
- Infrastruktura C-ITS RSU (ITS-G5 in/ali C-V2X)
- Namestitev na kritičnih lokacijah za razpošiljanje SPaT/MAP in opozoril (DENM), ter sprejem CAM; podpora GLOSA (na vstopno/izstopnih točkah koridorjev za vzpostavitev zelenega vala).
- Integracija z C-ITS Vozlišče (Basic Interface, PKI), telemetrija in dogodki preko MQTT.
- Prednost avtobusov in vozil s prednostjo
- Primarno: na GNSS/AVL temelječa prednost (centralna napoved prihoda vozila povzroči aktivacijo prednostne faze).
- Opcijsko / komplementarno: V2X/RSU interakcija za lokalno, nizkolatenčno prednost.
- Modernizacija semaforских krmilnikov
- LED signalizacija, TCP/IP komunikacija, daljinsko upravljanje, varnostni načini, nočna zatemnitev, integracija z RSU in prilagodljivimi algoritmi.
- Enotna komunikacijska in podatkovna hrbtenica
- Asinhroni podatkovni tokovi prek MQTT; kontrolne operacije prek HTTPS/REST.
- Uskladitev z MOL PCI (upravljanje infrastrukture, kamere), C-ITS Vozlišče (ekosistem C-ITS), Storitev Repozitorij (persistenca), Storitev Analitika (zgodovinska analiza), Controller (API Prehody).

3.2.2 Zahteve za detekcijo prometa

Podsistem *Detektor prometa* na nivoju križišča, kot ga prikazuje model (vsebnik Detektor prometa z relacijama MQTT/HTTPS proti Pametno križišče), vsebuje večmodalne kamere z lokalno umetno inteligenco, ki v realnem času zaznavajo osebna in dostavna vozila, tovornjake, avtobuse, motorna kolesa ter tudi nemotorizirane udeležence (kolesarje, pešce, če se premikajo po voznih pasovih) in iz teh zaznav tvorijo strukturirane dogodke. Objave potekajo asinhrono prek lokalnega posrednika MQTT (angl. data topic), medtem ko se upravljanje konfiguracije, posodobitve vdelane programske opreme in spremembe detekcijskih con izvajajo prek REST ali MQTT (angl. control topic). Jedro funkcionalnosti vključuje večrazredno klasifikacijo z možnostjo razširitve nabora razredov, zanesljivo sledenje več objektom hkrati (angl. multitarget) z vzdrževanjem identifikatorja seje skozi trajanje prisotnosti v območju, dinamično štetje po smeri gibanja in agregacijo v intervalih (5 s, 60 s, 15 min, dan) ter napredno logiko detekcije stanj: zasedenost pasu, tvorjenje kolone, počasno gibanje, nenadna ustavitev, vožnja skozi rdečo fazo (v korelaciji s signalnim stanjem krmilnika) in zaznavo potencialnih konfliktov (skorajšnja nesreča, angl. nearmiss). Sistem iz trajektorij izračunava OD matriko (izvor → cilj) ob zagotavljeni anonimizaciji, predlaga podaljšanje zelene faze z dogodkom »phase_extension_suggested« ter z lokalnim filtriranjem in dušenjem (angl. debounce) zmanjšuje podvojene kratkotrajne zaznave.





Strojna zasnova temelji na namestitvi kamer na obstoječe nosilce (stebri, konzole) pod kotom približno 10–30° nad območjem detekcije, z napajanjem prek PoE (802.3af ali 802.3at) in porabo manj kot 25 W na enoto. Delovanje je zagotovljeno v temperaturnem razponu –20 °C do +55 °C ob zaščiti IP66. Optična komponenta obsega vidni spekter (RGB), kritična križišča pa je možno opremiti s termičnim modulom. Minimalna efektivna ločljivost za analitiko je 1920×1080 pri vsaj 15 FPS, s prilagodljivim znižanjem frekvence slik pri slabši osvetlitvi. Krožna medpomnilniška shramba z zadrževanjem do 24 ur je šifrirana in namenjena forenzični analizi brez trajnega hranjenja surovih video posnetkov.

Analitični sloj (Edge AI) zagotavlja nizko latenco od zajema do objave dogodka (≤ 300 ms povprečno), visoko natančnost klasifikacije ($F1 \geq 0,85$ podnevi in $\geq 0,75$ ponoči), natančno detekcijo tvorjenja kolone ($\geq 0,90$ pri kolonah z več kot štirimi vozili) ter omejen odmik identifikatorja pri reidentifikaciji ($< 10\%$ ob prehodu med več conami). Modeli so lokalno optimirani (kvantizacija, pospeševanje CPU/GPU/NPU) brez pošiljanja surovih slik v oblak; na voljo je tihi način, ki onemogoči izvoz video toka in objavlja zgolj metapodatke. Komunikacijski vmesnik uporablja MQTT pub/sub (QoS 1 za kritične dogodke, QoS 0 za visoko frekvenčno telemetrijo) ter REST/MQTT ukaze za upravljanje. Zapis JSON definira minimalna polja `timestamp`, `deviceId`, `intersectionId`, seznam `objects[]` (type, lane, speed_kph, heading_deg, length_m), `events[]` (eventType, severity, phaseRef), agregate z intervalom in množicami `counts{class→value}` ter stanje naprave `health{cpuLoad, memFree, sensorTemp, uptime, status}`. Posamezni dogodek ne preseže 8 KB, agregiran paket 64 KB.

Sistem dosega operativni uptime $\geq 99\%$ mesečno, izguba dogodkov ostaja pod 0,5 % v 24 urah, časovna sinhronizacija (NTP stratum ≤ 3) zagotavlja odmik pod 100 ms, ocena hitrosti vozil pa dosega povprečno absolutno napako ≤ 6 km/h. Varnost in zasebnost temeljita na agregiranih podatkih brez biometričnih identifikatorjev; video tok se ne izvaža brez eksplicitnega dovoljenja. Konfiguracijske posodobitve so šifrirane (TLS 1.2+) in integriteta je potrjena s podpisanim certifikatom ali HMAC. Skladnost pokriva EN 50132-7 (CCTV), ISO 14813-1 (ITS arhitektura), NTCIP 1202² (posredno prek Edge GW) ter ETSI ITS (časovna koordinacija SPaT/MAP).

Vzdrževanje vključuje objave “heartbeat” vsakih 60 sekund s statusi operational/degraded/fault in samodejno detekcijo degradacije (latenca, FPS) z generiranjem dogodka `health_alert`. Posodobitve vdelane programske opreme (OTA) uporabljajo podpisano verifikacijo in omogočajo povrnitev. Lokalni dnevniški medpomnilniški prostor rotira pri 50 MB, kritični dogodki pa se dodatno posredujejo Križiščnemu računalniku za centralni arhiv. Arhitektura je razširljiva: dodajanje novih senzorskih modalitet (lidar, radar) prek abstraktnega vmesnika `sensors[]`, uvedba semantične segmentacije (vozišče, kolesarska steza, pločnik) za napredne KPI ter vključitev algoritmov za zaznavo anomalij (angl. ghost vehicle, wrongway driving) prek modularnih vtičnikov.

Spodaj je primer minimalnega dogodka v zapisu JSON:

```
{  
  "timestamp": "2025-11-23T14:45:07Z",  
  "deviceId": "CAM-V05-S-01",  
  ...  
}
```

² NTCIP 1202 v03 - National Transportation Communications for ITS Protocol - Object Definitions for Actuated Signal Controllers (ASC), <https://www.ntcip.org/library/documents/>





```
"intersectionId": "V05",
"intersectionName": "Tržaška - Cesta v Gorice",
"objects": [
  {"type": "car", "lane": "S1", "speed_kph": 42.5, "heading_deg": 180, "length_m": 4.5},
  {"type": "van", "lane": "S1", "speed_kph": 38.2, "heading_deg": 182, "length_m": 5.2},
  {"type": "truck", "lane": "S2", "speed_kph": 28.7, "heading_deg": 178, "length_m": 12.3},
  {"type": "bus", "lane": "S1", "speed_kph": 35.0, "heading_deg": 181, "length_m": 18.0},
  {"type": "motorcycle", "lane": "S1", "speed_kph": 48.3, "heading_deg": 179, "length_m": 2.1}
],
"events": [
  {"eventType": "queue_detected", "severity": "medium", "phaseRef": "FAZA_SJ"},
  {"eventType": "bus_detected", "severity": "high", "phaseRef": "FAZA_SJ"}
],
"aggregates": {
  "interval_s": 60,
  "counts": {"car": 42, "van": 8, "truck": 5, "bus": 3, "motorcycle": 12}
},
"health": {"cpuLoad": 0.62, "memFree": 512, "sensorTemp": 44.1, "uptime": 86400, "status":
"operational"}
}
```

Arhitekturno je komponenta umeščena kot izvor dogodkov na INTERSECTION_LEVEL; tok DATA (molCamera -> molEdgeGW) prek MQTT/HTTPS TLS prenaša detekcije in telemetrijo, tok CONTROL (molEdgeGW -> molCamera) pa omogoča konfiguracijo con in posodobitev vdelane programske opreme. Križiščni računalnik izvaja normalizacijo in po potrebi agregacijo pred posredovanjem v centralni MQTT. Opisane zahteve skupaj tvorijo zanesljivo, varno in razširljivo osnovo za večmodalno zaznavanje prometa na križiščih ter podporo naprednim funkcijam prilagodljivega upravljanja semaforjev, analitike in integracij C-ITS brez odvisnosti od posameznega proizvajalca.

3.2.3 Zahteve za detekcijo pešcev in kolesarjev

Podsistem *Detektor pešcev in kolesarjev* predstavlja komponento sistema pametne cestne infrastrukture, zasnovano za samodejno zaznavanje prisotnosti pešcev in kolesarjev na prehodih ter v območjih križišč. Osnovni namen je optimizacija faz semaforjev, povečanje varnosti nemotoriziranih udeležencev in zmanjšanje nepotrebnih prometnih zastojev. Sistem nadomešča klasične tipke za pešce z neprekinjenim zaznavanjem v realnem času, kar omogoča dinamično upravljanje zelene faze in boljše prilagoditev dejanskim prometnim razmeram. Funkcija klasične tipke ostane prisotna izključno kot zvočno opozorilno sredstvo za slepe in slabovidne osebe, kar zmanjšuje potrebo po fizičnem stiku s površinami in poenostavlja uporabniško izkušnjo.

Za učinkovito zaznavanje pešcev in kolesarjev na prehodih ter križiščih je predvidena uporaba naprednih AI kamer s termičnim videnjem, ki omogočajo zanesljivo detekcijo v vseh svetlobnih in vremenskih razmerah. Termični senzorji temeljijo na zaznavanju toplotnih podpisov, kar zagotavlja neprekinjeno delovanje tudi v popolni temi, megli ali sneženju, kjer klasične RGB kamere ne dosegajo





zadostne natančnosti. Sistem temelji na video analitiki z vgrajeno umetno inteligenco, ki ne le zazna prisotnost, temveč tudi razlikuje med pešci in kolesarji ter izvaja štetje prehodov v realnem času.

Takšna kamera združuje termični senzor, video analitiko (detekcija/štetje) ter Wi-Fi sledenje. Tipično dimenzioniranje namestitev je:

- 4-krako križišče: 4 enote (ena na vsak uvoz)
- 3-krako križišče: 3 enote
- samostojen prehod za pešce/kolesarje v sredini odseka: 1 enota (pokrije obe strani prehoda, če je nameščena centralno)

Če je kamera nameščena na drog ob prehodu (ali na ločilnem otoku), usmerjena vzdolž prehoda in opremljena s širokokotno optiko, lahko doseže približno 180° horizontale pokritosti. Takšna postavitve zmanjša mrtve kote in zakrivanje pešcev/kolesarjev (npr. zaradi skupin, dežnikov ali mimo vozečih vozil) ter omogoča stabilnejše štetje in zaznavanje vstopa/izhoda iz prehoda. Doseganje pričakovane pokritosti se potrdi s terensko kalibracijo con in preizkusom v tipičnih pogojih (tema, dež, sneg, visoka gostota pešcev).

Poleg termične komponente sistem vključuje tudi Wi-Fi tracking funkcionalnost, ki omogoča zaznavanje mobilnih naprav v bližini prehoda ali križišča. Ta pristop predstavlja dodatno redundanco in omogoča boljše razumevanje vzorcev gibanja pešcev, saj je mogoče slediti povprečnemu času zadrževanja v čakalnem območju, frekvenci prehodov in gostoti prometa nemotoriziranih udeležencev. Wi-Fi tracking deluje pasivno, brez potrebe po aktivni participaciji uporabnikov, saj sistem zaznava MAC naslove naprav, ki oddajajo Wi-Fi signal, pri čemer se vsi podatki anonimizirajo in obdelujejo v skladu z GDPR zakonodajo.

Integracijska arhitektura sistema temelji na odprtih standardih z uporabo JSON formata za izmenjavo podatkov in REST API vmesnika za komunikacijo s centralnim sistemom upravljanja prometa ter lokalnim vozliščem Križiščnega računalnika. Vsaka detekcijska enota v realnem času generira strukturirane dogodke o zaznavah pešcev in kolesarjev, ki vključujejo attribute kot so časovni žig, tip udeleženca, smer gibanja, število zaznanih oseb in ocenjeno hitrost gibanja. Ti podatki se prek REST API posredujejo Križiščnemu računalniku v križišču, ki na podlagi prejetih informacij aktivira ustrezno fazo semaforja ali prilagodi trajanje zelene faze.

Dimenzioniranje števila enot je odvisno od tipa križišča. Pri standardnem štirikrakem križišču se namestijo štiri detekcijske enote, ena za vsak uvoz, kar omogoča celovito pokritost vseh smeri približevanja pešcev in kolesarjev. Takšna postavitve zagotavlja, da sistem zajame udeležence, ki čakajo na posameznih vogalih križišča, ter tiste, ki se že nahajajo na samem prehodu. Trikrako križišče zahteva tri enote, postavljene na vsak uvoz, saj gre za tri ločene cone detekcije. Pri samostojnih prehodih za pešce v sredini odseka, ki niso del križišča, zadostuje ena centralno nameščena detekcijska enota, če je montirana na ustrezni višini in z optimalnim kotom, ki omogoča pokritje obeh smeri približevanja pešcev.

Tehnične specifikacije predvidevajo, da vsaka enota podpira istočasno termično in video detekcijo z ločljivostjo termičnega senzorja najmanj 320×240 slikovnih točk in spektralnim območjem 8–14 μm . Vgrajena AI procesna enota mora omogočati obdelavo video tokov v realnem času z minimalnim zamikom, priporočljivo pod 200 ms od zaznave do generiranja dogodka. Komunikacijski vmesnik





mora zagotavljati standardno Ethernet povezavo za integracijo v lokalno omrežje križišča, podpirati pa mora tudi PoE (angl. Power over Ethernet) za enostavno napajanje prek omrežnega kabla. REST API mora omogočati obojesmerno komunikacijo, tako za pošiljanje dogodkov kot tudi za sprejemanje konfiguracijskih ukazov iz centralnega sistema.

Funkcija klasične tipke za pešce se v tem sistemu transformira in ostane prisotna izključno kot zvočno opozorilno sredstvo za slepe in slabovidne osebe, medtem ko primarno vlogo najave prevzame avtomatska detekcija. Ta pristop zmanjšuje potrebo po fizičnem stiku s površinami gumbov, kar je posebej relevantno iz higienskega vidika, hkrati pa poenostavlja uporabniško izkušnjo, saj pešci niso več zavezani k aktivaciji tipke, temveč so samodejno zaznani ob vstopu v detekcijsko območje.

Struktura podatkovnega paketa, ki ga detekcijska enota pošilja Križiščnemu računalniku prek REST API, sledi standardiziranemu JSON formatu. Spodnji primer prikazuje tipičen dogodek, generiran ob zaznavi pešcev in kolesarjev v različnih conah območja detekcije.

Primer paketa JSON (payload) za dogodek detekcije:

```
{
  "timestamp": "2025-11-23T14:32:15Z",
  "deviceId": "PED-DET-V04-01",
  "intersectionId": "V04",
  "detectionZones": [
    {
      "zoneId": "approach_north",
      "type": "pedestrian_waiting",
      "count": 4,
      "status": "occupied",
      "lastUpdate": "2025-11-23T14:32:14Z"
    },
    {
      "zoneId": "crosswalk_north",
      "type": "pedestrian_crossing",
      "count": 0,
      "status": "clear",
      "lastUpdate": "2025-11-23T14:32:10Z"
    },
    {
      "zoneId": "approach_south",
      "type": "cyclist_waiting",
      "count": 2,
      "status": "occupied",
      "lastUpdate": "2025-11-23T14:32:13Z"
    }
  ],
  "wifiTracking": {
    "uniqueDevices": 6,
  }
}
```





```
"avgDwellTime": 18.5  
,  
"health": {  
  "sensorTemp": 41.2,  
  "uptime": 864720,  
  "status": "operational"  
}  
}
```

Ključni elementi strukture paketa JSON vključujejo časovni žig dogodka, identifikator naprave in križišča, niz detekcijskih con s tipom (čakalna cona za pešce, prehod, čakalna cona za kolesarje), trenutnim številom zaznanih udeležencev, statusom (angl. occupied/clear) ter časom zadnje detekcije. Sekcija sledenje Wi-Fi dodaja agregiran podatek o številu unikatnih mobilnih naprav v območju in povprečnem času zadrževanja, medtem ko sekcija health omogoča spremljanje operativnega stanja naprave, vključno s temperaturo senzorja in časom neprekinjenega delovanja.

3.2.4 Zahteve za prednostno uporabo vozil javnega prevoza in vozil s prednostjo

Prednostno upravljanje vozil javnega prevoza in vozil s prednostjo je ključni segment za izboljšanje prometne učinkovitosti in varnosti v urbanih območjih. Izvajanje teh ukrepov v MOL prispeva k zmanjšanju zamud, povečanju operativne hitrosti javnega prevoza in zagotavljanju hitrejšega posredovanja služb za nujne primere, kar neposredno izboljšuje kakovost življenja državljanov in funkcionalnost prometnega sistema. Prednostne obravnave vozil javnega prevoza in vozil s prednostjo ni mogoče obravnavati ločeno od integriranega sistema upravljanja prometa in omrežij semaforjev. Učinkovito izvajanje zahteva usklajeno delovanje različnih tehnoloških komponent in sistemov.

Obstajata dve osnovni tehnologiji za določitev prioritete:

- Namestitev naprav OBU v vozila in RSU ob cesti (npr. ob semaforjih)
- Uporaba tehnologije GNSS za pozicioniranje in obveščanje sistemov za upravljanje prometa

Tradicionalni pristop temelji na opremljanju vseh ustreznih vozil (avtobusov javnega prevoza LPP, policijskih, gasilskih in reševalnih vozil) s terminalskimi napravami (angl. OBU »on board unit«), ki komunicirajo z RSU. Ta sistem omogoča takojšnje zaznavanje in samodejno prilagajanje semaforjev za zagotovitev prednosti. Čeprav gre za zanesljivo tehnologijo, njena izvedba zahteva znatno začetno naložbo, saj morajo biti vsi udeleženci v prometu opremljeni s fizično nameščenimi napravami. Poleg tega takšne naprave niso prenosne, kar še dodatno omejuje prilagodljivost sistema. Za funkcionalnost je treba sistem namestiti na velikem številu križišč, kar povečuje kompleksnost in stroške. V vse semaforne naprave je v tem primeru potrebno vgraditi RSU naprave (V2V ter V2I) - ter izvesti programsko integracijo.

Drug pristop uporablja globalne satelitske sisteme za določanje položaja (GNSS) za sledenje gibanja vozil javnega prevoza in vozil na nujni vožnji. Podatki o položaju v realnem času se pošiljajo v centralni sistem za upravljanje prometa, ki na podlagi natančnega zaznavanja položaja vozila predvidi njihov prihod na prometno nadzorovana križišča in aktivira prednostno signalizacijo.

Izkušnje iz drugih evropskih mest kažejo, da uvedba prednosti vozil javnega prevoza zmanjša povprečni čas čakanja na semaforjih za do 50 %, povprečna hitrost avtobusov pa se poveča za približno





10 %. To izboljša točnost javnega prevoza, zmanjša negativni vpliv prometnih zastojev in omogoči učinkovitejše načrtovanje voznega reda. Prednost se prilagodi prometnim razmeram in posebnostim posameznega križišča, s čimer se preprečijo neželeni negativni učinki na celoten prometni tok.

Po drugi strani pa ima obravnava vozil s prednostjo nedvomno prednost, saj zagotavlja brezpogojno hiter prehod skozi križišča, kar je ključnega pomena za hitro posredovanje in reševanje človeških življenj.

Kamera z večrazredno klasifikacijo zanesljivo prepozna avtobus ter ohranja njegovo trajektorijo skozi namenske detekcijske cone (npr. `BUS_APPROACH`, `BUS_STOP_LINE`). Ob izpolnitvi kombinacije pogojev (približevanje rdeči ali rumeni fazi, ocena časa do zaustavitvene linije pod konfiguriranim pragom, dolžina kolone pred avtobusom nad nastavljeno mejo) generira dogodek `bus_detected` (severity=high) in po potrebi predlog `phase_extension_suggested` ali zahtevo za zgodnji vklop zelene (`early_green_request`) prek MQTT CONTROL. Križiščni računalnik korelira te dogodke s trenutnim stanjem faz krmilnika in politiko omejitev (največje število zaporednih podaljšanj, minimalni odmik med zahtevami, absolutna zgornja meja skupne podaljšane zelene). Sistem deluje neodvisno od AVL integracije; opcijsko se lahko uporabi dodatni identifikacijski signal (RFID ali V2X) za potrjevanje, pri čemer kamera ostaja primarni (angl. failsafe) vir zaznave. V primeru konkurenčnih prioritet (npr. avtobus in vozilo nujne pomoči) se lokalno izračuna hierarhični vrstni red na podlagi konfigurirane matrike prednosti. Vsi dogodki ostajajo anonimni, brez podatkov, ki bi omogočali sledljivost posameznega vozila; statistični agregati omogočajo KPI (čas prihodov, povprečni zamik, delež uspešno realiziranih prioritet) za optimizacijo strateških ukrepov javnega prevoza.

Dodatno se prioriteta avtobusov optimira s združevanjem podatkov GNSS (iz podsistema C-ITS Vozlišče, CAM sporočila z geolokacijo, hitrostjo, smerjo in `stationId`) ter lokalne vizualne detekcije. Križiščni računalnik vzpostavi naročanje na CAM tok (filtriranje po poligonu križišča in smeri prihoda) in za vsako avtobusno enoto vodi drsečo evidenco napovedanih prihodov (ETA) z atributi: `stationId`, zadnja lokacija GNSS, projekcija na pristopni koridor, ocenjena razdalja do zaustavitvene linije, predvideni pas. Kamera ob detekciji avtobusa posreduje klasifikacijo, ocenjen pas, hitrost in heading; mehanizem ujemanja uporabi prostorsko – časovno okno (npr. razdalja < 40 m od napovedane pozicije, časovni odklon od ETA < 2 s) ter preveri konsistentnost smeri (razlika heading < 15°) in velikostnega profila. Pri več kandidatih se izračuna podobnostni rezultat (angl. weighted score) ter izbere najvišjega nad pragom; s tem se lokalni identifikator zaznave poveže s `stationId` brez razkritja trajne identitete (osebni podatki se ne hranijo). Če se GNSS psevdonim (rotacija StationID) zamenja znotraj aktivne seje, bridge modul začasno vzdržuje povezavo z verigo CAM sporočil (časovni kompromis < 30 s) in uporabi kontinuiteto trajektorije za ponovno mapiranje. Končni zapis omogoča sestavo obogatene dogodka `priority_request` z razlogoma "visual" in "gnss" ter zanesljivejši izračun ETA za fazno podaljšanje. Zavrnitev ujemanja (pod pragom) vodi do obravnave zaznanega avtobusa kot neavtorizirane instance z nižjo stopnjo vpliva na logiko prilagoditve.

Za vozila s prednostjo (reševalno vozilo, policija, gasilci na nujni vožnji) se uporablja višja stopnja prednosti in mehanizem prednosti (angl. preemption). CAM ali DENM sporočila nosijo tip posebnega vozila (specialVehicleType); Križiščni računalnik vzpostavi takojšnje spremljanje kandidatov znotraj širšega prehodnega območja (npr. 150–250 m od križišča). Kamera lahko dodatno potrdi vizualne





značilnosti (oblika, barvni vzorec, možnost detekcije svetlobnih signalov v prihodnjih modelih). Ob sočasni prisotnosti več zahtev se uporabi hierarhija: vozilo na nujni vožnji > avtobus > standardni prometni dogodki. Preemption lahko sproži prezgodnji preklon na fazo ali podaljšanje trenutne zelene mimo običajnih omejitev, ob tem pa se beleži metrika vpliva (časovna odstopanja od načrtovanega cikla, kumulativna poraba dodatnih sekund zelene). Če nujno vozilo ni vizualno potrjeno (npr. GNSS signal brez zaznave kamere) se uporabi konzervativni profil (omejeno podaljšanje); če kamera potrdi prisotnost, se aktivira polni profil za prednost. Vsi dogodki se objavljajo izključno kot anonimni operativni signali brez shranjevanja neobdelanih identifikatorjev; zadrževanje korelacijskih zapisov je časovno omejeno (npr. drseče okno 30 min) in šifrirano.

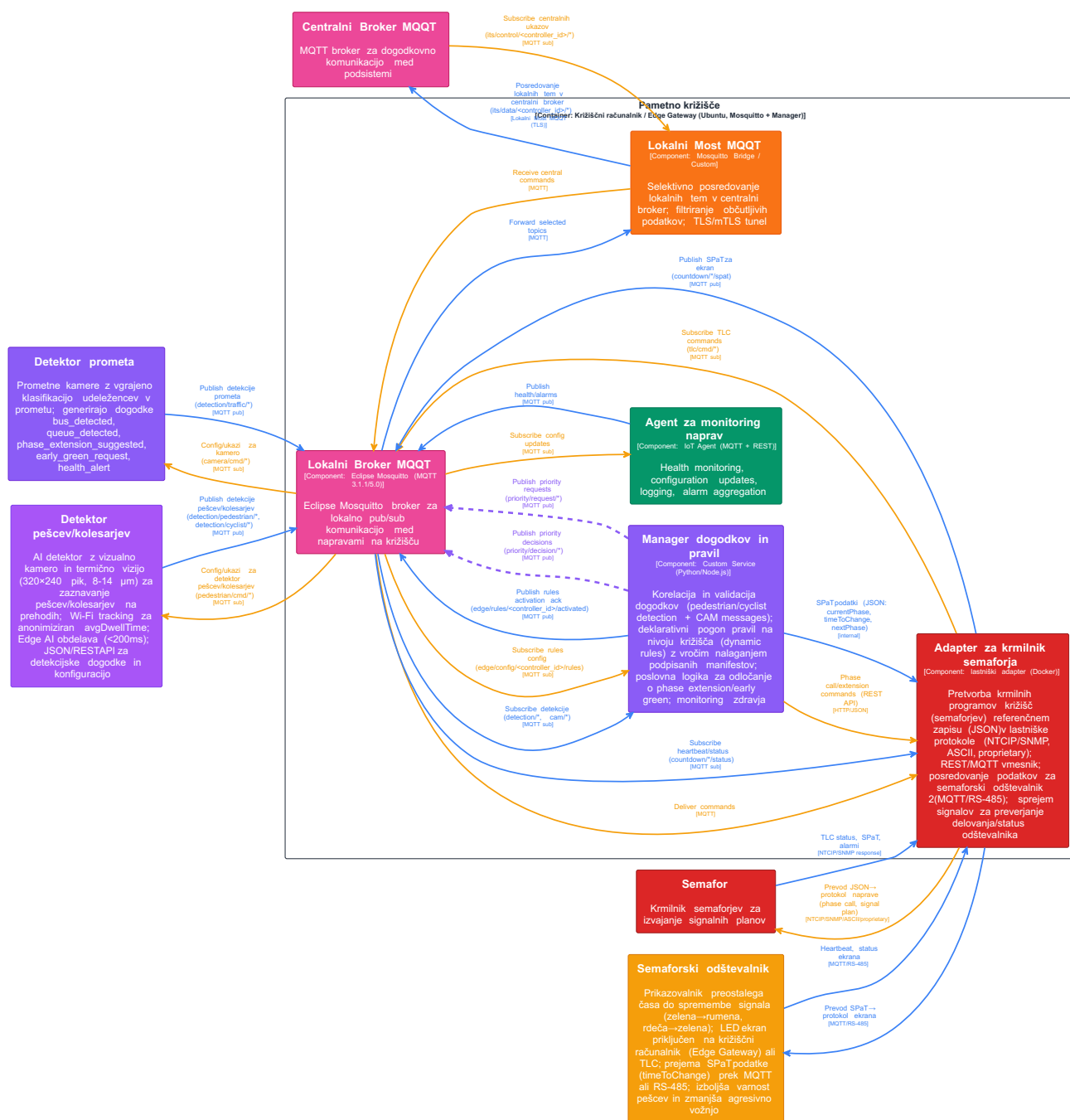
3.2.5 Zahteve za informacijske tehnologije v križišču

Računalniška oprema v križišču (vsebnik Pametno križišče), križiščni računalnik predstavlja lokalni integracijski in usklajevalni sloj med detekcijskimi napravami (prometne kamere, detektor pešcev/kolesarjev), krmilnikom semaforjev (TLC), morebitnim semaforskim odštevalnikom (prikaz preostalega časa faze; v študiji je predvidena ohranitev obstoječih odštevalnikov za pešce, lokacije razvidne iz risb grafičnih prilog), RSU ter centralnim MQTT posrednikom. Križiščni računalnik je sestavljen iz petih ključnih komponent, ki skupaj zagotavljajo nizko latenco, lokalno inteligenco, varnost in zanesljivost sistema.

Slika 9 prikazuje komponentni pogled križiščnega računalnika prikazuje pet ključnih komponent (Lokalni MQTT Broker, Manager dogodkov in pravil, Adapter za krmilnik semaforja združen tudi kot adapter za semaforski odštevalnik, MQTT Bridge, Agent za monitoring naprav) ter njihove povezave z napravami na križišču (MOL Detektor prometa, MOL Detektor pešcev/kolesarjev, MOL Semafor, MOL Semaforski odštevalnik) in centralnim sistemom (Sporočilna vrsta). Manager dogodkov in pravil odloča o zelenih fazah na podlagi korelacije detekcij in deklarativno definiranih pravil; Adapter za krmilnik semaforja prevaja ukaze v zapisu JSON v proizvajalcu specifične protokole in iz SPaT podatkov generira format za odštevalnik; MQTT Bridge posreduje izbrane teme v centralni MQTT broker.

Srce komunikacije na križišču (npr. križišče B01) je lokalni MQTT broker, implementiran z industrijsko preizkušenim Eclipse Mosquitto. Ta posrednik deluje kot nevtralen kanal, preko katerega kamere objavljajo detekcije prometa na teme `detection/B01/*`, detektor pešcev sporoča prisotnost na `triggers/B01/PED_*`, krmilnik semaforjev objavlja trenutno stanje (SPaT) na `C-ITS/spat/B01`, centralni sistem pa pošilja ukaze na `camera/cmd/B01/CAM_01` ali `tlc/cmd/B01`. Vzorec publish/subscribe omogoča, da vsaka naprava izmenjuje svojo komunikacijo neodvisno, brez eksplicitnega poznavanja prejemnikov – če se odloči dodati nov senzor (npr. meteorološko postajo), se ta preprosto naveže na lokalni broker in začne objavljati svoje podatke, ostale komponente pa jih uporabijo glede na svojo logiko.

X4ITS - Komponentni pogled križišnega računalnika (Edge Gateway) (Fusion/TLC Adapter/Bridge) (rev: 2026-02-27)



Slika 9. Programske komponente za MOL Pametno križišče (nameščene na križiščnem računalniku)

Broker uporablja MQTT protokol različic 3.1.1 in 5.0, podpira kakovost storitve (QoS) 0 in 1, šifriranje prek TLS ter Access Control Lists (ACL) za ločevanje pravic – kamera na primer lahko objavlja detekcije, ne sme pa sprožiti ukaza za podaljšanje zelene faze. Tipična latenca od objave dogodka do prejema pri naročniku je pod 10 milisekund, kar zagotavlja hitre reakcije tudi pri kritičnih dogodkih, kot je prepoznavanje urgentnega vozila.



Ključni tematski kanali MQTT (angl. topics) upoštevajo najnovejše zahteve večmodalne detekcije, fuzije GNSS/CAM za prioriteto avtobusov ter hierarhičnega razvrščanja prednosti za nujna vozila. Za vsak kanal so navedeni tipični QoS, status, namen, primer in JSON atributi.

Konvencije: časovni žig ISO 8601 UTC ('ts'), stabilni berljivi identifikatorji ('locationId', 'cameraId', 'intersectionId', 'rsuId', 'stationId'), odjemalci ignorirajo neznana polja, numerične enote so v SI, besedilne enum vrednosti VELIKE ČRKE.

Topic: 'detections/'

- QoS: 1, retained: false
- Namen: tok granularnih dogodkov video/termalne detekcije iz kamer (vozila, pešci, kolesarji, avtobus, kolona, incidenti). Vključuje osnovne objekte in opsijske agregate ter dogodke stanj ('queue_detected', 'bus_detected', 'phase_extension_suggested').

Primer:

```
{
  "ts": "2025-11-24T07:32:15Z",
  "locationId": "krizisce-123",
  "cameraId": "cam-01",
  "objects": [
    { "class": "car", "lane": "S1", "speedKmh": 43.1, "headingDeg": 180 },
    { "class": "bus", "lane": "S1", "speedKmh": 25.4, "headingDeg": 181, "matchSource": "visual" }
  ],
  "events": [
    { "eventType": "queue_detected", "severity": "MEDIUM" },
    { "eventType": "bus_detected", "severity": "HIGH" }
  ],
  "aggregates": { "intervalSec": 60, "counts": { "car": 18, "bus": 2 } },
  "health": { "cpuLoad": 0.62, "sensorTempC": 44.1 }
}
```

Bistvena polja:

```
`objects[].class|lane|speedKmh|headingDeg|matchSource`,
`events[].eventType|severity`,
`aggregates.intervalSec|counts{class→int}`,
`health.cpuLoad|sensorTempC`.
```

Polje 'matchSource' ("visual"|"gnss"|"fusion") označuje izvor identifikacije avtobusa.

Topic: 'priority/request'

- QoS: 1, retained: false
- Namen: Križiščni računalnik ali CUP objava zahtev za podaljšanje faze / preemption (avtobus, nujno vozilo).





Primer:

```
{  
  "ts": "2025-11-24T07:32:17Z",  
  "intersectionId": "krizisce-123",  
  "priorityType": "BUS",  
  "stationId": 456712,  
  "etaToStopLineSec": 9.4,  
  "reason": ["visual", "gnss"],  
  "suggestedAction": "PHASE_EXTENSION",  
  "phaseRef": "FAZA_SJ"  
}
```

Za vozilo s prednostjo (na nujni vožnji):

`priorityType`="EMERGENCY", dodatno
`emergencySubtype` ("AMBULANCE"|"POLICE"|"FIRE") in možen
`preemptionLevel` ("FULL"|"LIMITED").

Topic: `priority/decision`

- QoS: 1, retained: false
- Namen: rezultat hierarhične evalvacije (vozilo s prednostjo > avtobus > standardni dogodki); zabeleži izid in vpliv na signalni cikel.

Primer:

```
{  
  "ts": "2025-11-24T07:32:18Z",  
  "intersectionId": "krizisce-123",  
  "granted": ["EMERGENCY"],  
  "denied": ["BUS"],  
  "cycleImpactSec": 7,  
  "reason": "hierarchy",  
  "phaseRef": "FAZA_SJ"  
}
```

Topic: `rsu/telemetry`

- QoS: 0–1, retained: false
- Namen: stanje RSU (V2X enota) in diagnostika.

Primer (razširjen):

```
{  
  "ts": "2025-11-24T07:32:15Z",  
  "rsuId": "rsu-001",  
  ...  
}
```





```
"status": "OK",  
"uptimeSec": 172800,  
"tempC": 41.8,  
"fw": "1.3.0",  
"gnssFix": "3D",  
"cpuLoad": 0.27  
}
```

Topic: `C-ITS/spat`

- QoS: 1, retained: true
- Namen: poenostavljen SPaT (trenutna stanja faz + čas do spremembe).

Primer:

```
{  
  "ts": "2025-11-24T07:32:15Z",  
  "intersectionId": "krizisce-123",  
  "phases": [  
    {"id": 1, "state": "GREEN", "timeToChangeSec": 8},  
    {"id": 2, "state": "RED", "timeToChangeSec": 8}  
  ]  
}
```

Topic: `C-ITS/denm`

- QoS: 1, retained: false
- Namen: lokalni dogodki (zapora, nevarnost, vozilo na nujni vožnji, če se generira DENM).

Primer:

```
{  
  "eventId": "denm-2025-11-24-001",  
  "type": "ROAD_WORKS",  
  "priority": "HIGH",  
  "validFrom": "2025-11-24T08:00:00Z",  
  "validTo": "2025-11-24T16:00:00Z",  
  "location": {"lat": 46.056, "lon": 14.505, "radiusM": 50},  
  "description": "Dela na vozišču"  
}
```

Topic: `camera/health`

- QoS: 0, retained: false
- Namen: periodični heartbeat in degradacije (latenca, FPS, termalna temperatura).





```
{
  "ts": "2025-11-24T07:33:00Z",
  "cameraId": "cam-01",
  "status": "OPERATIONAL",
  "cpuLoad": 0.55,
  "memFreeMb": 512,
  "sensorTempC": 45.2,
  "latencyMsAvg": 272,
  "fps": 17,
  "alerts": []
}
```

Minimalna neformalna shema za `detections/`:

```
{
  "type": "object",
  "required": ["ts", "locationId", "objects"],
  "properties": {
    "ts": {"type": "string", "format": "date-time"},
    "locationId": {"type": "string"},
    "cameraId": {"type": "string"},
    "objects": {"type": "array", "items": {"type": "object", "required": ["class"], "properties": {
      "class": {"type": "string", "enum": ["pedestrian", "bicycle", "escooter", "car", "van", "truck", "bus", "motorcycle"]},
      "lane": {"type": "string"},
      "speedKmh": {"type": "number"},
      "headingDeg": {"type": "number"},
      "matchSource": {"type": "string", "enum": ["visual", "gnss", "fusion"]}
    }}}},
    "events": {"type": "array", "items": {"type": "object", "properties": {
      "eventType": {"type": "string", "enum": ["queue_detected", "bus_detected", "phase_extension_suggested", "early_green_request"]},
      "severity": {"type": "string"},
      "phaseRef": {"type": "string"}
    }}}},
    "aggregates": {"type": "object", "properties": {
      "intervalSec": {"type": "number"},
      "counts": {"type": "object", "additionalProperties": {"type": "number"}}
    }},
    "health": {"type": "object", "properties": {
      "cpuLoad": {"type": "number"},
      "sensorTempC": {"type": "number"}
    }}
  }
}
```



```
}  
}
```

Hierarhija prioritete (implementirana na Edge GW, objava rezultata `priority/decision`): `EMERGENCY > BUS > STANDARD`. Odjemalci, ki ne potrebujejo polj (npr. `matchSource`, `cycleImpactSec`), jih lahko ignorirajo. Vsa polja so brez osebnih podatkov; identifikacija vozil je prostorsko-časovna in psevdonimizirana.

Če je lokalni MQTT broker komunikacijsko vozlišče, je Manager dogodkov in pravil odločevalski center – komponenta, ki jo razvije MOL ali izbrani integrator in je odgovorna za implementacijo delovanja “politike” križišča. Manager dogodkov in pravil se naroči na vse relevantne dogodke (detekcije prometa z AI kamerami, CAM sporočila iz C-ITS sistema, detekcije pešcev z AI kamerami, Wi-Fi sledenje povprečnega časa zadrževanja), jih korelira in na podlagi hierarhične logike `EMERGENCY > BUS > PEDESTRIAN > STANDARD` odloča, katero zeleno fazo sprožiti, podaljšati ali prekiniti.

Predstavljajmo si konkreten scenarij: detektor pešcev objavi dogodek `detection/B01/PED_BTN_1` z informacijo, da so trije pešci čakali povprečno 12 sekund. Manager dogodkov in pravil ta dogodek prevzame, validira stanje senzorja (ali je latenca normalna, ali temperatura termične kamere ni presegla pragov, ali je frekvenca zaznav zadostna), preveri trenutno fazo križišča in, če ugotovi, da so pogoji izpolnjeni (npr. prag čakanja presežen, ni aktivne prioritete višjega ranga), sproži klic proti Adapterju za krmilnik semaforja (REST API):

```
POST /api/v1/controller/CTRL_B01/phase-call  
{  
  "signal_group_id": "SG5",  
  "source": "PEDESTRIAN_DETECTION"  
}
```

Adapter za krmilnik semaforja ta generični ukaz prevede v katerikoli specifični protokol naprave (NTCIP `SNMP set`, Swarco ASCII ukaz `:SG5r'n` ali Siemens binarni paket), fizični krmilnik pa aktivira zeleno fazo za pešce. Celoten tok, od detekcije do fizične spremembe luči, traja manj kot 100 milisekund, pri čemer je večina časa porabljena za validacijo, ne za prenos podatkov.

Manager dogodkov in pravil je odgovoren tudi za dušenje podvojenih dogodkov (angl. debouncing; npr. če detektor pešcev v roku ene sekunde objavi deset zaporednih detekcij istih pešcev, Manager zagotovi, da se zahteva za zeleno fazo sproži le enkrat), ter za lokalno agregacijo števcov (npr. koliko avtobusov je prečkalo križišče v zadnjih 60 sekundah), kar zmanjša obremenitev centralne infrastrukture. Da zagotovimo dinamično, križišču prilagojeno poslovno logiko (npr. podaljšanje faze na osnovi AI detekcij, omejevanje prednostnega preklopa, časovna okna idr.), križiščni računalnik vključuje deklarativni pogon pravil kot integralni del storitve »Manager dogodkov in pravil« (ni ločena komponenta). Aktivacija, uveljavljanje varovalk, revizijska sled in povrnitev (angl. rollback) se izvajajo znotraj iste storitve.





V praksi Manager dogodkov in pravil stalno bere lokalne teme (`detection/*`, `cam/*`, `C-ITS/spat`/`C-ITS/map`, `tlc/status/*`) in sistemske metrike ter jih poveže v trenutni kontekst križišča. Na ta kontekst se aplicirajo deklarativna pravila, podpisan, verzioniran JSON dokument, ki opiše pogoje (kdaj), operatorje (kako) in akcije (kaj). Manifest je objavljen na `edge/config/<controller_id>/rules` in je validiran proti formalni shemi `tools/schemas/rules-manifest.schema.json` (JSON Schema 2020-12, <https://json-schema.org/draft/2020-12/schema>) ter kriptografsko podpisan. Po uspešni verifikaciji se aktivacija potrdi na `edge/rules/<controller_id>/activated` s podatki `rulesVersion`, `activatedAt` in `hash`.

Brez deklarativnih pravil bi bila logika prilagajanja faz kodirana v aplikaciji, kar oteži hitro odzivnost na spremembe prometa (ali prometne politike). Pravila omogočajo predvidljivost in varnost (varovalke se uveljavijo enako ob vsakem dogodku), preglednost in sledljivost (odločitve so razložljive iz manifesta in revizijske sledi), agilnost (prometni inženirji uvajajo spremembe z novo verzijo manifesta brez posega v kodo), interoperabilnost (isti jezik pravil deluje nad različnimi krmilniki prek Adapterja za krmilnik semaforja) in robustnost (staged activation in rollback zmanjšata operativno tveganje).

Ko so pogoji izpolnjeni, Manager izvede odločitev: zabeleži jo v telemetriji na `priority/decision/<controller_id>` in ali sproži zahtevo na `priority/request/<controller_id>`. Za neposredne ukaze proti krmilniku semaforja uporabimo enoten kanal prek Adapterja za krmilnik semaforja (`tlc/cmd/<controller_id>/*` ali ustrezne REST metode). Pred vsako akcijo se strogo uveljavijo varovalke (angl. guardrails): minimalne zelene, intergreeni, izpraznitveni časi za pešce, matrika konfliktov signalnih skupin in največje trajanje podaljšanj. S tem preprečimo neželene konflikte in ohranjamo varnost.

Proces je odporen: podpira fazno (angl. staged) aktivacijo pravil in samodejni povratek na zadnjo stabilno verzijo ob napaki. Če bi pogon pravil začasno izpadel, krmilnik semaforja nadaljuje s statičnimi plani, ukazi z zastarelim `ttlMs` pa se zavrnejo. Vse odločitve so revizijsko sledljive: shranimo `rulesVersion`, povzetek vhodnega stanja, izhodno akcijo, rezultat na adapterju in točen časovni žig.

Pred aktivacijo vsakega manifesta križiščni računalnik preveri skladnost s shemo in veljavnost digitalnega podpisa. Vsaka odločitvena akcija mora imeti določen `ttlMs`, rok veljavnosti ukaza, po katerem se ukaz ne sme več izvršiti.

Primer poenostavljene shematske strukture pravila:

```
{
  "rulesVersion": "2025-11-29",
  "conditions": [
    { "all": [
      { "topic": "detection/pedestrian/zoneA", "op": ">=", "value": 3, "forMs": 800 },
      { "topic": "C-ITS/spat/timeToChange", "op": "<=", "value": 5 }
    ] }
  ],
}
```





```
"actions": [  
  { "type": "PRIORITY_REQUEST", "topic": "priority/request/${controller_id}", "payload": {  
    "phase": "G2", "extensionSec": 6, "reason": "PEDESTRIAN_CLUSTER" } }  
],  
"guardrails": { "minGreenSec": 7, "maxExtensionSec": 10, "intergreenSec": 3 }  
}  
...
```

Poenostavljeni primer pravila bi lahko bil:

- Ob najavi T1 ali T2 nastavi V2 = 20 s in vklopi odštevalnik:

```
{  
  "conditions": [{"any": [  
    { "topic": "detector/T1/call", "op": "=", "value": true, "forMs": 200 },  
    { "topic": "detector/T2/call", "op": "=", "value": true, "forMs": 200 }  
  ]}],  
  "actions": [  
    { "type": "DIRECT_TLC_CMD", "topic": "tlc/cmd/${controller_id}/stage-override", "payload":  
      { "target": ["V2"], "param": "durationSec", "mode": "absolute", "valueSec": 20, "scope": "window",  
        "windowSec": 60, "ttlMs": 1500 },  
    { "type": "DIRECT_TLC_CMD", "topic": "countdown/${controller_id}/mode", "payload":  
      { "enabled": true, "ttlMs": 1500 }  
    ]  
  }  
}
```

V nasprotju z Managerjem dogodkov in pravil, ki ga razvije MOL, je Adapter za krmilnik semaforja odgovornost posameznega proizvajalca krmilnikov semaforjev. Vsak dobavitelj mora implementirati adapter, ki izpostavlja enotni vmesnik REST API, kot je opisan v 7. PRILOGA 2: Specifikacija adapterja za krmilnik semaforja, hkrati pa interno komunicira s svojim krmilnikom prek lastniških protokolov (NTCIP/SNMP, Swarco ASCII, Siemens proprietary). Ta arhitekturni vzorec omogoča, da lahko Manager dogodkov in pravil govori univerzalni jezik zapisa JSON, adapter pa prevaja v »narečje« posameznega krmilnika in obenem standardizira posredovanje sprememb do nadzorne plošče.

Adapter sprejema REST klice ('POST /api/v1/controller/{controller_id}/phase-call', 'POST .../phase-extension', 'GET .../spat') ali MQTT ukaze na temi 'tlc/cmd/{controller_id}', jih prevede v protokol naprave in posreduje krmilniku. V obratni smeri periodično poizveduje (angl. polling) stanje krmilnika, trenutno aktivne faze (SPaT), alarmne dogodke, stanje detektorjev, in rezultate objavlja nazaj na lokalni broker ('tlc/status/<controller_id>'). Istočasno iz prejetih SPaT podatkov sproži posodobitve semaforkega odštevalnika prek enotnega kanala (brez ločenega adapterja), kar zmanjšuje



kompleksnost in število komponent. Vsaka operacija je zabeležena v revizijski sledi z ISO 8601 časovnimi žigi, uporabnikom, starimi in novimi vrednostmi, kar zagotavlja sledljivost sprememb.

Minimalni nabor metod, ki jih mora vsak adapter implementirati:

- `POST /api/v1/controller/{controller_id}/phase-call` – sproži klic za zeleno fazo določene signalne skupine
- `POST /api/v1/controller/{controller_id}/phase-extension` – podaljša trenutno zeleno fazo
- `GET /api/v1/controller/{controller_id}/spat` – vrne trenutno stanje vseh signalov (zelena, rdeča, rumena, utripanje)

Ta minimalizem omogoča, da tudi preprosti krmilniki, ki ne nudijo naprednih funkcij (npr. adaptivnega krmiljenja ali popolnoma konfigurabilnih faz), lahko sodelujejo v sistemu, njihovi adapterji preprosto implementirajo osnovno funkcionalnost, medtem ko zmogljivejši krmilniki ponudijo širši API.

Četrta komponenta, Lokalni Most MQTT, je odgovorna za selektivno posredovanje lokalnih tem v Centralni Broker MQTT, ki deluje v CUP. Bridge ne posreduje vseh lokalnih dogodkov, če bi, bi centralni sistem prejel tisoče detekcij na sekundo, kar bi povzročilo preobremenitev, temveč filtrira, agregira in komprimira podatke. Na primer, posamezne detekcije prometa (`detection/B01/LANE_1_VEHICLE_*`) se združijo v “minutni agregat” (število vozil po razredih), ki se nato posreduje na centralno temo `its/data/B01/aggregates`. Status krmilnika, alarmi in zahteve za prioriteto (`priority/request/B01/*`) pa se posredujejo v realnem času, saj so kritični za odziv operaterjev na situacijo.

Lokalni Most MQTT deluje v načinu “store-and-forward”: če centralna povezava iz kateregakoli razloga prekine (izpad VPN, vzdrževanje omrežja, kratkotrajno preklapljanje), začne kopičiti dogodke v lokalnem shrambenem prostoru (angl. backlog), ki lahko sprejme vsaj 10.000 dogodkov ali 30 minut podatkov (odvisno kar nastopi prej). Ko se povezava obnovi, Lokalni Most MQTT dogodke postopoma sprosti (angl. flush) s hitrostjo, ki ne preplavi centralnega sistema (tipično 200 dogodkov na sekundo), kritični dogodki (npr. urgentno vozilo, huda napaka krmilnika) pa imajo prednost v vrsti.

Varnost je ključna, zato Lokalni Most MQTT komunicira s Centralni Broker MQTT prek mutual TLS (mTLS), kar pomeni, da obe končni točki, križiščni in centralni strežnik, preverita identiteto nasprotnika s certifikati. Ciljna latenca objave, to je sprejem v centralnem sistemu je 150 milisekund (95. percentil 200 ms), kar zagotavlja, da operaterji vidijo skoraj-realnočasovno situacijo na celotni mreži križišč.

Zadnja komponenta je Agent za monitoring naprav, storitev, ki periodično spremlja stanje (zdravje) vseh naprav na križišču (kamera, TLC, RSU, detektor pešcev) in objavlja agregirane metrike (`edge/health`) z informacijami o obremenitvi CPU, porabi RAM-a, zasedenosti diska, globini čakalne vrste Centralni Broker MQTT in latenci Lokalni Most MQTT. Če zazna degradacijo, na primer temperatura kamere presega varen prag, frekvenca kadrov (FPS) pade pod minimum, ali latenca do centralnega sistema skoči nad dopustno mejo, generira opozorilni dogodek `health_alert`, ki sproži alarm v nadzorni plošči CUP.

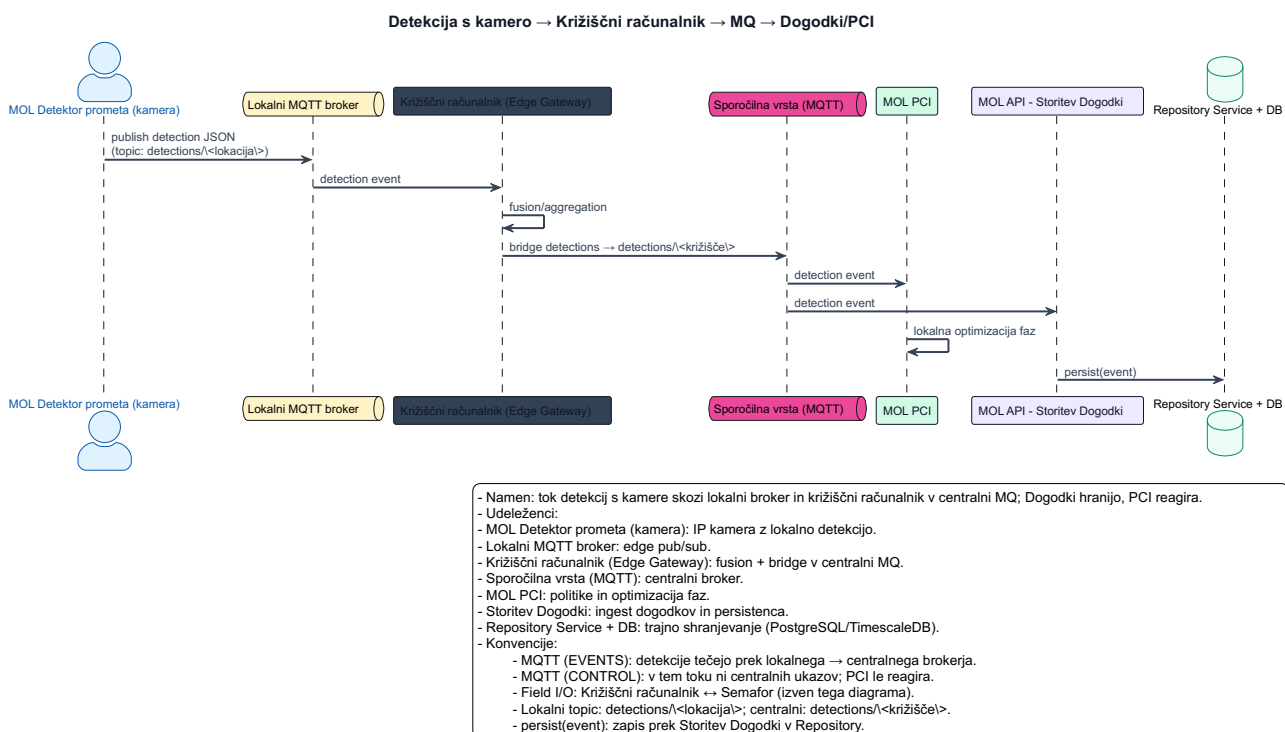




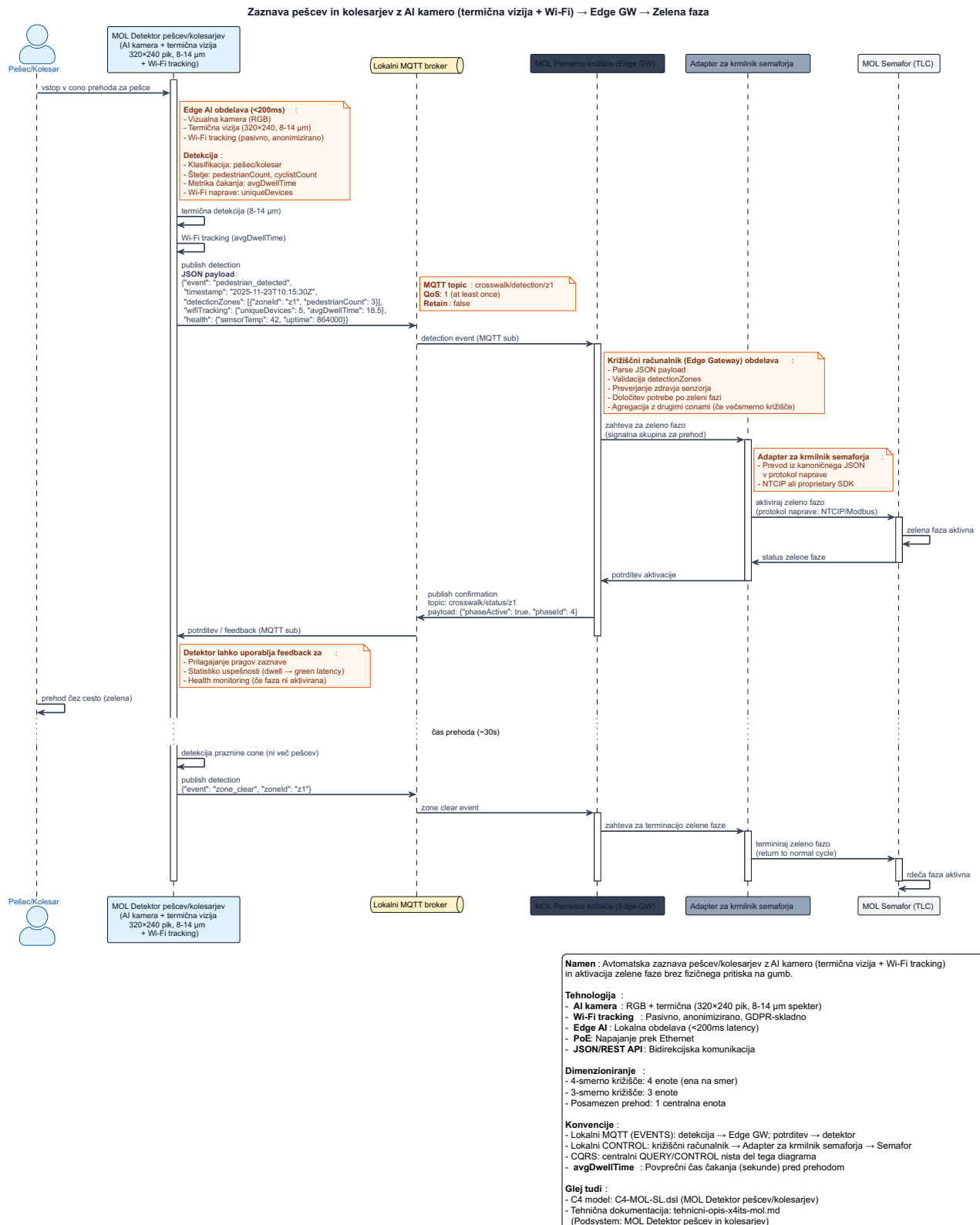
Agent je tudi odgovoren za posodobitve programske opreme na daljavo prek brezžične povezave (OTA – Over-The-Air), ki se izvedejo v dveh korakih: najprej prenese novo različico programske opreme, preveri integriteto (digitalni podpis + hash), jo postavi v pripravljeni režim (angl. staged activation) in po 24 urah brez kritičnih napak potrdi posodobitev (angl. commit). Če v tem obdobju sistem zazna težave, agent samodejno vrne prejšnjo različico (angl. rollback), s čimer se izogne situacijam, ko bi napačna posodobitev onespodobila celotno križišče. Poleg OTA nalaganja lahko operaterji prek ukaznega kanala (`edge/command/diagnostic`) sprožijo ad-hoc teste: preverjanje latence (latency probe), integriteto backlog-a, preverbo roka veljavnosti TLS certifikatov ali simulacijo obremenitve.

V nadaljevanju so prikazani sekvenčni prikazi ključnih kontrolnih in podatkovnih tokov med akterji in sistemi, usklajeni s predhodnimi diagrami. Vsak diagram jasno loči podatkovne (MQTT) ter kontrolne (HTTP/REST) povezave.

- Uporaba kamere za detekcijo udeležencev v prometu (Slika 10): kamera objavi agregirane anonimizirana števila kategorij udeležencev kot JSON po MQTT (topic `detections/<lokacija>`); MOL PCI lahko takoj optimizira faze, Storitev Analitika jih shrani prek Storitve Repozitorij
- Uporaba kamere za detekcijo pešcev in kolesarjev (Slika 11): prikazuje celoten tok dogodkov od zaznave pešca ali kolesarja na prehodu do aktivacije zelene luči brez fizičnega pritiska na gumb. Sistem temelji na AI kamerah z vizualno in termično vizijo (320×240 pik, 8–14 μm spekter) ter zaznavanjem Wi-Fi naprav pešcev / kolesarjev za merjenje povprečnega časa čakanja (avgDwellTime). Ko detektor zazna vstop v cono prehoda, lokalno obdela podatke z Edge AI (<200ms latenca) in pošlje strukturiran paket JSON prek lokalnega MQTT brokerja na Križiščni računalnik, ki validira dogodek, preveri stanje senzorja in prek TLC Adapterja sproži zeleno fazo na semaforju. Po prehodu pešcev sistem zazna praznino cone in samodejno prekine zeleno fazo, s čimer se vrne v normalen cikel. Diagram dokumentira tudi dvosmerno komunikacijo za ter vključuje dimenzioniranje (4-smerno križišče = 4 enote, 3-smerno = 3 enote, posamezen prehod = 1 enota)
- Prednost avtobusa (GNSS/AVL in CUP) (Slika 12): iz GNSS/AVL se izračuna ETA v CUP API storitve; CUP zahteva prednost prek MOL PCI, krmilnik izvede prilagoditev in vrne telemetrijo/status.
- RSU/GLOSA v C-ITS (Slika 13): CITS razpošlje SPaT/MAP proti RSU in vozilom (OBU), vozila periodično pošiljajo CAM; ob dogodkih se objavi DENM prek MQTT.

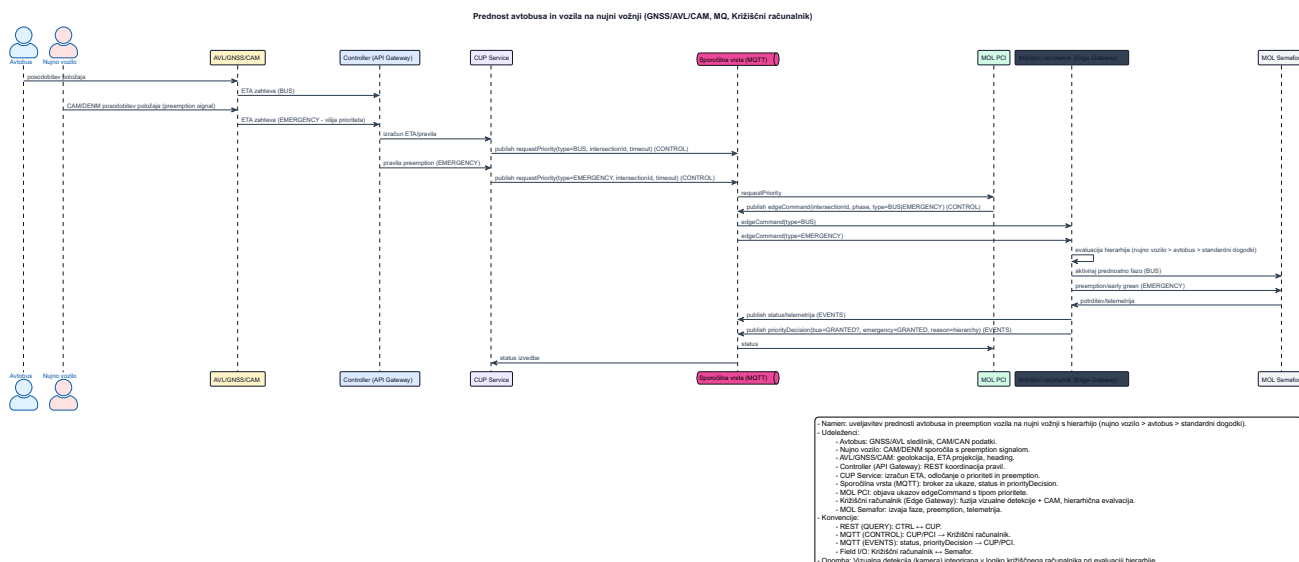


Slika 10. Sekvenčni diagram »Detekcija udeležencev prometu«



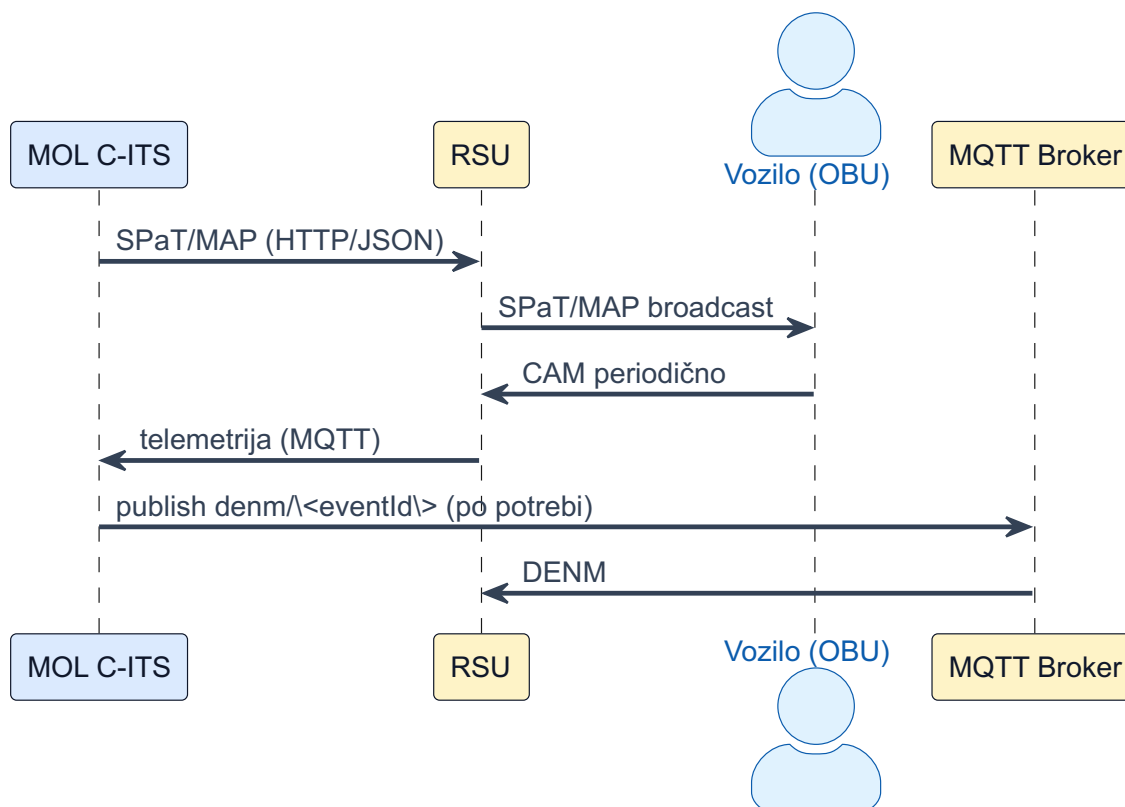
Slika 11. Sekvenčni diagram »Detekcija pešcev in kolesarjev«





Slika 12. Sekvenčni diagram »Prednost avtobusa in vozila na nujni vožnji«

Delovanje RSU/GLOSA in C-ITS



- Namen: GLOSA in varnostna opozorila (C-ITS) med MOL CUPs, RSU in vozili.
- Udeleženci:
 - MOL C-ITS: backoffice storitev C-ITS.
 - RSU: cestna enota na križišču.
 - Vozilo (OBU): enota v vozilu za sprejem/sporočanje.
 - MQTT Broker: posredovanje dogodkov in telemetrije.
- Konvencije:
 - SPaT/MAP: C-ITS → RSU (HTTP/JSON); RSU → OBU (broadcast).
 - CAM: OBU → RSU (periodično).
 - Telemetrija: RSU → C-ITS prek MQTT.
 - DENM: C-ITS → MQTT → RSU.

Slika 13. Sekvenčni diagram za »Delovanje sistema GLOSA in C-ITS«

3.2.6 Zahteve za posodobitev semaforских naprav

Zahtevana je tudi prenova semaforских krmilnih naprav. Obstoječe signalne naprave MSKE60, opremljene z moduli, namenjenimi krmiljenju klasičnih ali halogenskih signalnih luči (ne LED), predstavlja tehnološko zastarel sistem, ki ne ustreza sodobnim tehničnim in energetskim standardom.

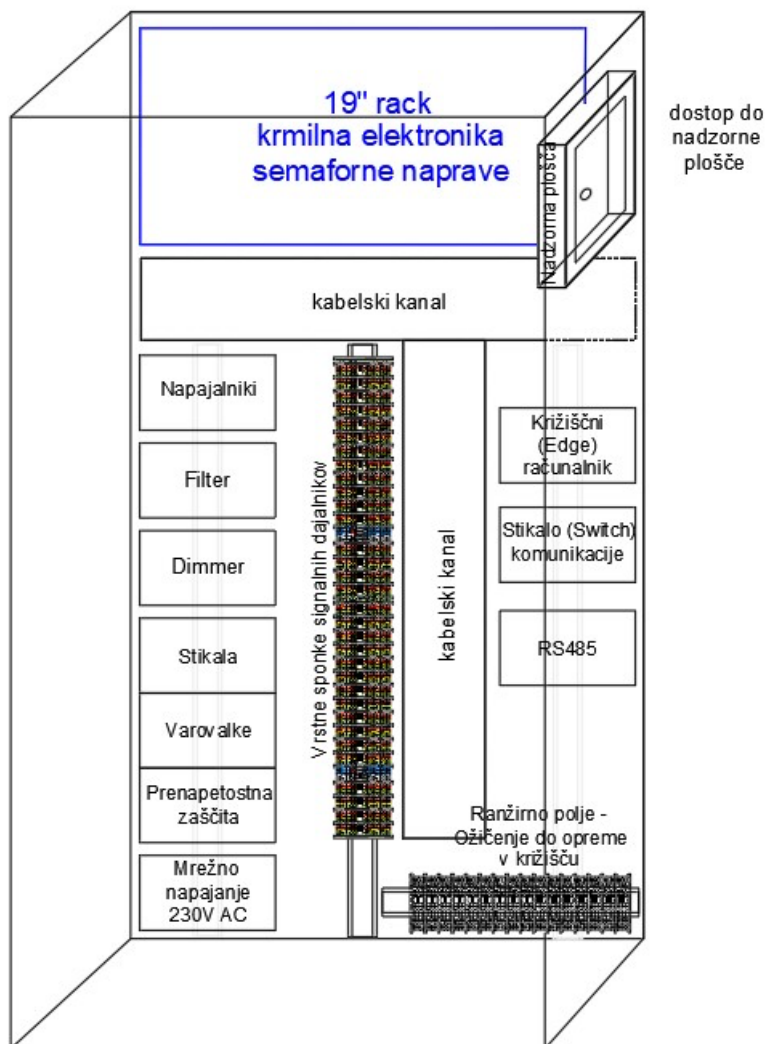


Čeprav je delna nadgradnja obstoječega sistema tehnično mogoča, na primer z zamenjavo modulov, tak poseg ni niti ekonomsko upravičen niti dolgoročno vzdržen. Stroški nadgradnje omenjenega sistema MSKE60 na sodobne standarde (LED signalizacija, integracija z naprednimi prometnimi sistemi, komunikacija s komponentami V2X/RSU) so nesorazmerni s preostalo življenjsko dobo naprave in omejenimi tehničnimi zmogljivostmi samega krmilnika. Poleg tega takšna nadgradnja zahteva dodatne prilagoditve napajanja, krmiljenje svetlobnega toka in morebitne spremembe komunikacijskih vmesnikov, kar še dodatno poveča skupne stroške in kompleksnost integracije.

Priporočilo je postopna zamenjava naprav MSKE60 s sodobnimi prometnimi krmilniki, ki v osnovi podpirajo LED tehnologijo, inteligentno upravljanje in spremljanje ter enostavno integracijo s prihajajočimi sistemi pametne mobilnosti.

Vendar je treba opozoriti, da je v primerih, ko naprava MSKE60 še vedno v celoti izpolnjuje tehnične in funkcionalne zahteve določenega projekta, tj. kadar ni predvidena implementacija naprednih funkcionalnosti in je sistem stabilen in vzdržen, njena ohranitev lahko upravičena. V takih primerih je treba izvesti oceno stroškov in koristi ter sprejeti odločitev na podlagi dejanskih potreb in možnosti nadaljnjega vzdrževanja.





Slika 14. Model semaforne omare v križišču.

3.2.7 Prihodnja razširitev: varnostna kamera PTZ in snemanje skorajšnjih nesreč

Razširitev lahko predvideva opsijsko varnostno kamero PTZ, ki se aktivira le ob dogodku tipa `near_accident_risk` (skorajšnja nesreča) ali `conflict_high_severity`, zaznanem z lokalno analitiko trajektorij. Cilj je omogočiti forenzični vpogled v nevarne prometne interakcije brez stalnega snemanja in brez vpliva na zasebnost udeležencev.

Potek aktivacije:

1. Detekcija konflikta: prometna kamera objavi dogodek `near_accident_risk` (trajektorije, območje konflikta, udeleženci).
2. Odločitev križišča: Križiščni računalnik preveri resnost (`severity=HIGH`, `probability=HIGH`) in sproži CONTROL ukaz `ROTATE_AND_RECORD` na interno temo `securityCam/command`.



3. PTZ rotacija: varnostna kamera takoj preklopi na preset (npr. `CONFLICT_ZONE_NW`) in začne snemanje (profil 1920×1080, ≥25 FPS, H.264/H.265).
4. Lokalna hramba: datoteka se šifrira (AES256), dobi `videoId` (UUID) in kriptografski `hashSha256`.
5. DENM generacija: Križiščni računalnik sestavi DENM z referenco na posnetek (časovno omejena podpisana URL povezava, $\text{exp} \leq 24 \text{ h}$) in objavi na `C-ITS/denm`.
6. Čiščenje: samodejni izbris posnetka po 30 dneh (`retentionDays=30`); revizijski dnevnik dostopov (RBAC: `CUP_OPERATOR`, `INVESTIGATION`).

Varnost/zasebnost:

- Snemanje samo ob dogodku visokega tveganja (ni stalnega nadzora).
- Šifrirano hranjenje, podpisane kratkotrajne URL povezave (`token`, `exp`).
- Revizija vsakega dostopa (čas, uporabnik, vloga, videoId).
- Brez biometrije; uporaba izključno za analizo varnosti in izboljšanje križišča.

Napake:

- `recordingStatus=FAILED` če rotacija ali snemanje ne uspe (DENM brez `videoUrl`).
- Generira se `edge_alert` (npr. `SEC_CAM_ROTATION_FAILURE`).

Razširitev dogodka detekcije (primer dodatnih polj):

```
{  
  "eventType": "near_accident_risk",  
  "severity": "HIGH",  
  "conflictZone": "NW_CORNER",  
  "participants": ["car", "cyclist"],  
  "minDistanceMeters": 1.8,  
  "timeToCollisionMs": 420,  
  "probability": "HIGH"  
}
```

Opomba (causeCode/subCauseCode): ETSI TS 102 8942 določa `causeCode` (npr. 6 = ACCIDENT). Za skorajšnjo nesrečo se lokalno uporabi `causeCode=6` + `subCauseCode=1` (predhodno opozorilo). Ob uvedbi uradne vrednosti se konfiguracija prilagodi brez spremembe logike. Primer DENM (JSON reprezentacija z lokalnimi razširitvami – dejanska produkcijska enkodiranje ASN.1 UPER):

```
{  
  "ts": "2025-11-24T07:40:12Z",  
  "messageType": "DENM",  
  "eventId": "denm-nearacc-2025-11-24-07-40-12-V05-001",  
  "publisherId": "edge-krizisce-V05",  
  "intersectionId": "V05",  
  "causeCode": 6,  
  "subCauseCode": 1,  
}
```





```
"causeDescription": "SKORAJŠNJA_NESREČA",
"location": {"lat": 46.035558, "lon": 14.461638, "radiusM": 35},
"vehiclesInvolvedApprox": 2,
"severity": "MEDIUM",
"probability": "HIGH",
"detectionSources": ["visual", "trajectory_analysis"],
"video": {
  "recordingStatus": "STARTED",
  "videoUrl": "https://edgegw-V05.local/video/denm-nearacc-2025-11-24-07-40-12-V05-001.mp4?token=ABCD1234&exp=2025-11-25T07:40:12Z",
  "retentionDays": 30,
  "startTime": "2025-11-24T07:40:12Z",
  "expectedPurge": "2025-12-24T07:40:12Z",
  "hashSha256": "9f3c4d7a1b2e...abc",
  "cameraPreset": "CONFLICT_ZONE_NW"
},
"lifecycle": {"validFrom": "2025-11-24T07:40:12Z", "validTo": "2025-11-24T07:45:12Z"},
"extensions": {
  "localPolicy": {"privacyMode": "EVENT_ONLY", "accessRole":
["CUP_OPERATOR", "INVESTIGATION"]},
  "recordingParams": {"resolution": "1920x1080", "fps": 25, "encoding": "H.264"}
},
"scope": "LOCAL"
}
```

Integracijske točke:

- CONTROL API (interno):

`POST /api/v1/security-camera/preset/{presetId}/record` (avtentikacija, podpis).

- MQTT CONTROL: tema `securityCam/command`

(`{"action": "ROTATE_AND_RECORD", "preset": "CONFLICT_ZONE_NW", "eventId": "..."}`).

- Telemetrija: `securityCam/health` (rotacija, zadnji posnetek, napake).

Vpliv na konfiguracijo Križiščnega računalnika: dodatno ≤ 5 GB/dan lokalne šifrirane hrambe (odvisno od pogostosti), minimalen CPU vpliv, kratkotrajni konični I/O ob zagonu snemanja. Modularni vtičnik omogoča uvedbo brez sprememb Križiščnega računalnika.

Funkcionalnost izboljša varnostno forenzično analitiko (identifikacija vzorcev tveganih manevrov, optimizacija faz, infrastrukturne prilagoditve) in ostaja skladna z načeli minimalnega snemanja, šifriranja ter strogega nadzora dostopa.

3.2.8 Ključni kazalniki uspešnosti

V splošnem bi lahko, glede na izkušnje iz objavljenih rezultatov podobnih projektov, dosegli naslednje kriterije uspešnosti:

- Natančnost detekcije pešcev: ≥ 92 -98% natančnost klasifikacije in detekcije prisotnosti pešcev¹
- Latenca odziva: ≤ 1 s latence detekcija \rightarrow ukrep za kritične dogodke





- Zmanjšanje čakalnih časov: –10–15% povprečni čakalni čas na križiščih; –5–12% potovalni čas²
- Prednost avtobusov³: +10 % povprečna hitrost avtobusov na koridorjih z uvedeno prednostjo;
- Razpoložljivost infrastrukture⁴: ≥ 99.5 % razpoložljivost RSU in kamer;
- GDPR skladnost⁵: 0 incidentov v zvezi z zasebnostjo (GDPR compliance).

3.3 Izvedba povezljivosti z Nacionalno točko dostopa

NAP je nacionalna dostopna točka Republike Slovenije za prometne in mobilnostne podatke. Deluje skladno z Direktivo 2010/40/EU (ITS) in delegiranimi uredbami ter zagotavlja enoten, standardiziran in varen način objave ter izmenjave podatkov. Povezljivost MOL z NAP.si je ključna zaradi skladnosti, interoperabilnosti in večje vidnosti mestnih podatkov na nacionalni in evropski ravni.

Vloga NAP na nacionalni ravni je sledeča:

- Centralna točka za objavo in iskanje prometnih/mobilnostnih podatkov (odprti in regulirani nabori).
- Standardizacija prek DATEX II (cestni promet), NeTEx/SIRI (javni prevoz potnikov) in mobilityDCAT-AP (metapodatki/katalog).
- Čezmejna interoperabilnost (TENT, CRoads, SRTI) ter preglednost za ponudnike storitev in raziskovalce.
- Operativni nadzor nad kakovostjo in skladnostjo objav.

Sistem MOL C-ITS uporablja NAP kot uradni kanal za objavo standardiziranih mestnih naborov podatkov (zapore, prometni podatki, parkirišča) v nacionalni katalog. NAP omogoča delitev mestnih podatkov drugim akterjem in pripravo na storitve C-ITS storitve (sinhronizacija zapor, SRTI, koordinacija z NCUP/DARS). Skladnost z evropskimi profili DATEX II podpira prihodnje širjenje funkcionalnosti (GLOSA, hibridni C-ITS).

Tipični nabori podatkov (angl. datasets) na NAP so:

- Dela na cesti / planirani dogodki
- Nesreče / nevarne situacije (SRTI)
- Potovalni časi (RTTI)
- Vremenske razmere in razmere na cesti (RWIS)
- Razpoložljivost parkirišč
- Spremenljive prometne table/sporočilne table (VMS)

³ Študije TSP (Transit Signal Priority) kažejo 5-15% izboljšave hitrosti (TRB Transit Capacity Manual; projekti v Stockholmu, Seattlu).

⁴ ITS standardi za kritične aplikacije zahtevajo >99% uptime (ISO 21217; C-ITS deployment guidelines)

⁵ Zero-incident target je standard za javne ITS projekte (EU C-ITS Platform guidelines; Dutch C-ITS corridor experience).





- Hitrostne in druge omejitve

Objave so katalogizirane z mobilityDCAT-AP metapodatki (opis, licenca, osveževanje, kontakt) in večinoma temeljijo na profilih DATEX II.

3.3.1 Nabori podatkov MOL za objavo

Nabori podatkov (datasets), ki jih MOL C-ITS pošilja v NAP, morajo biti v javnem interesu in so:

- Dela na cesti / planirani dogodki: mestne zapore, preusmeritve, časovni intervali.
- Potovalni časi: čas potovanja po ključnih koridorjih, agregirane hitrosti, zastoji.
- Nesreče: potrjeni mestni prometni dogodki (brez osebnih podatkov) – nesreče, ovire.
- Parkirišča: zasedenost P+R in mestnih parkirišč (interval + eventdriven).
- Vremenske razmere za ceste: lokalne razmere (če na voljo – površinska temp., padavine).
- Spremenljive prometne table/sporočilne table: sporočila z mestnih cestnih površin, če vplivajo na širši promet.

3.3.2 Objava na NAP.si v okviru MOL C-ITS

V arhitekturi MOL C-ITS (Slika 3) objavo na NAP izvaja namenski integracijski vsebnik »NAP Adapter«. NAP Adapter je jasno ločen od aplikacijskega jedra in je povezan s CUP API skozi API Prehod (Controller) in preko sporočilnega sistema Centralni Broker MQTT. Navzven vzpostavlja varno povezavo do NAP.si prek HTTPS z vzajemno overitvijo certifikatov (mTLS), kar zagotavlja avtentičnost in celovitost prenosov. Controller orkestrira objave prek internega API-ja: sproži pripravo nabora podatkov, posodobi metapodatke in nadzira življenjski cikel (aktivacija, začasna ustavitev, upokožitev). NAP Adapter ob tem pridobi izvirne podatke, jih normalizira in preslika v ustrezeni profil DATEX II. Pred objavo izvede validacijo XSD in notranje kontrole (časovni žigi, geometrije, poslovna pravila), nato pa pripravljene pakete objavi na NAP preko mTLS kanala. Operativno adapter spremlja odzive NAP (ACK, status), meri telemetrijo (latenca, velikost, uspešnosti) in vzdržuje robustnost z nadzorovanim ponovnim poskusom ter čakalno vrsto »dead-letter«⁶ za sporne zapise. Pri dinamičnih naborih podatkov (npr. RTTI, parkirišča) izvaja kombinacijo periodičnih objav in dogodkovno vodenih posodobitev, pri statičnih ali planskih naborih (npr. zapore) pa objavlja ob spremembah in preklicih. Kataloški zapisi se usklajujejo z metapodatki mobilityDCAT-AP, tako da so nabori sledljivi in pravilno opisani.

Podrobnosti so v nadaljevanju in na sekvenčnem diagramu (Slika 15).

3.3.3 Vsebnik NAP Adapter (DATEX II)

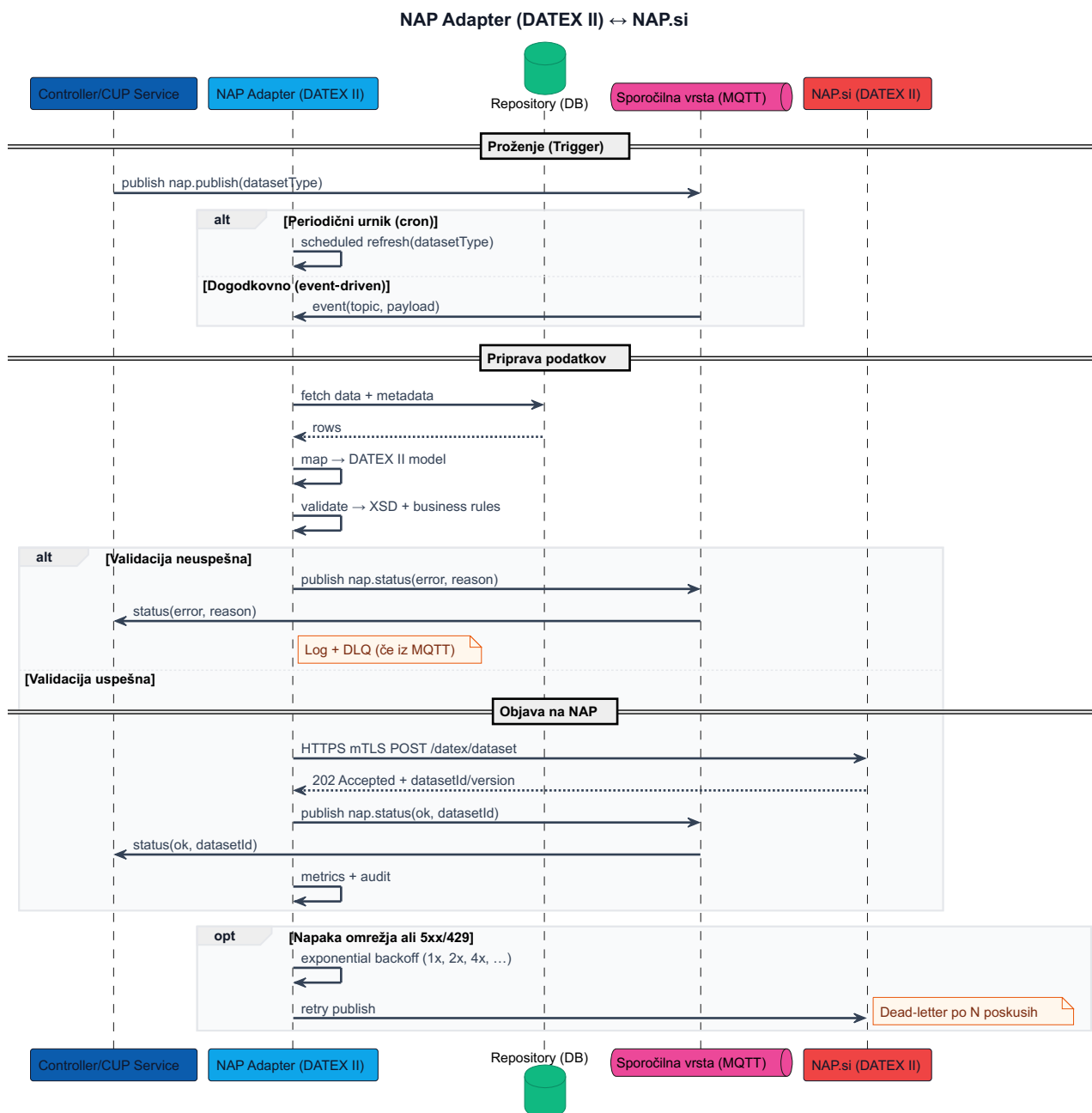
⁶ »Dead-letter queue« (DLQ) je varna čakalna vrsta za sporočila, ki jih po več neuspešnih poskusih ni mogoče uspešno obdelati ali dostaviti (npr. trajne napake: neveljavni podatki, kršitev sheme, manjkajoče reference, potek veljavnosti). Sporočila se tja premaknejo po konfiguriranem številu ponovitev/časovnem oknu in čakajo na ročni pregled, korekcijo in morebitno ponoven poskus obdelave. DLQ preprečuje blokado podatkovnega toka, omogoča forenzično analizo napak in ohranjanje zanesljivosti brez izgube sporočil.



V arhitekturi MOL C-ITS uvedemo namenski vsebnik »NAP Adapter (DATEX II)«, ki je specializiran integracijski vmesnik za NAP. Na diagramu (Slika 2) je vrisan kot lasten vsebnik in je povezan z:

- Storitvami CUP API (internal HTTP/JSON) za orkestracijo objav, sprožitev/preklic naborov podatkov in upravljanje metapodatkov,
- podatkovno bazo (Repository/DB) za branje izvornih podatkov in metapodatkov,
- sporočilno vrsto MQTT za asinhrono sprejemanje dogodkov, ki vplivajo na RTTI in druge dinamične nabore podatkov,
- NAP.si preko HTTPS/TLS z vzajemnim zaupanjem (PKI), kamor objavlja DATEX II vire.





- Namen: prikaz »publish« cikla do NAP.si (DATEX II) prek NAP Adapterja.
- Vhodi: interni REST (CTRL) ali MQTT dogodki; podatki iz Repository (DB).
- Obdelava: mapping v DATEX II + XSD/business validacija.
- Izhod: HTTPS/TLS z obojestransko avtentikacijo (PKI), 202 ack.
- Napake: retry z eksponentnim odstopanjem, DLQ po preseženi kvoti.
- Barvna legenda:
 - CTRL = #0B5CAD
 - NAP Adapter = #0EA5E9
 - DB = #10B981
 - Broker (MQTT) = #EC4899
 - NAP.si = #EF4444

Slika 15. Sekvenčni diagram objave iz MOL C-ITS na NAP.si



Na nivoju CUP API je NAP Adapter prikazan kot zunanji (integracijski) vsebnik, do katerega Controller dostopa prek internega API. S tem ločimo odgovornosti: CUP API orkestrira, NAP Adapter oblikuje in objavi standardizirana sporočila.

3.3.4 Podatkovni tokovi in nabori podatkov

Objava posameznega nabora podatkov sledi ponovljivemu poteku, ki se začne pri virih in konča z objavo standardiziranih sporočil na NAP. Vhodi prihajajo iz notranjih sistemov (npr. PCI, C-ITS, Analitika ter drugi sistemi MOL), bodisi prek dogodkov, ki jih objavljajo na MQTT, bodisi prek neposrednega dostopa do podatkov prek storitve Repository. NAP Adapter te podatke prevzame, jih normalizira in obogati: konsistentno doda geolokacijske attribute, preslika vrednosti v dogovorjene slovarje in poravna statusna polja ter časovne žige. Nato jih preslika v ustrezne razrede DATEX II, skladno s profilom za posamezni nabor.

Preden gre paket v objavo, poteka večstopenjska validacija. Najprej shematska (XSD za DATEX II), ki zagotovi skladnost strukture, nato še notranje poslovne kontrole, kot so veljavnost intervalov, prisotnost in pravilnost časovnih žigov ter geometrij (npr. veljavnost geometrij v PostGIS). Šele ob uspešni validaciji adapter pripravi končno predstavitev in jo prek varne povezave (HTTPS z mTLS) objavi na NAP.si.

Ritem objavljanja je odvisen od tipa nabora: pri zaporah in načrtovanih dogodkih se objava sproži ob nastanku, spremembi ali preklicu; pri parkiriščih teče kombinacija periodičnih objav (npr. vsakih 30–60 sekund) in dogodkovnih posodobitev ob spremembi zasedenosti; pri vremensko-cestnih razmerah se objave izvajajo periodično (npr. na 5–10 minut) ali ob alarmnih pragovih; pri RTTI pa tipično periodično (npr. na 1–5 minut) ter po pomembni spremembi stanja. Sočasno z vsebinskimi objavami adapter vzdržuje tudi metapodatke. Kataloške zapise usklajuje z mobilityDCAT-AP (opis, licenca, kontakt, frekvenca osveževanja), tako da so nabori na NAP.si pravilno opisani, sledljivi in dosledno različici.

3.3.5 Operativno delovanje

Operativno delovanje NAP Adapterja temelji na strogih ciljih storitev (SLA) z zahtevano razpoložljivostjo najmanj 99,5 % ter hitro obnovitvijo storitve v največ 15 minutah ob morebitnem izpadu objave podatkov. Ta visok standard zagotavlja neprekinjeno delovanje sistema in zanesljivost podatkovnih tokov proti nacionalni točki dostopa. Celoviti monitoring sistema vključuje kontinuirane preglede (angl. health checks) NAP Adapterja skupaj z detajlnim spremljanjem metrik objav, ki zajemajo število uspešnih in neuspešnih poskusov objave, latence komunikacije ter velikosti podatkovnih paketov. Ti parametri se v realnem času prikazujejo na nadzorni plošči z ustreznimi opozorilnimi alarmi, kar omogoča proaktivno ukrepanje ob morebitnih težavah.

Za zagotavljanje robustnosti sistema je implementiran napredni mehanizem ponovnih poskusov z eksponentno rastočimi intervali med poskusi ter specializirana »deadletter« čakalna vrsta za problematične zapise, ki jih sistem ne more uspešno objaviti. V takšnih primerih je mogoč tudi ročni ponoven poskus objave po odpravi vzroka težave.

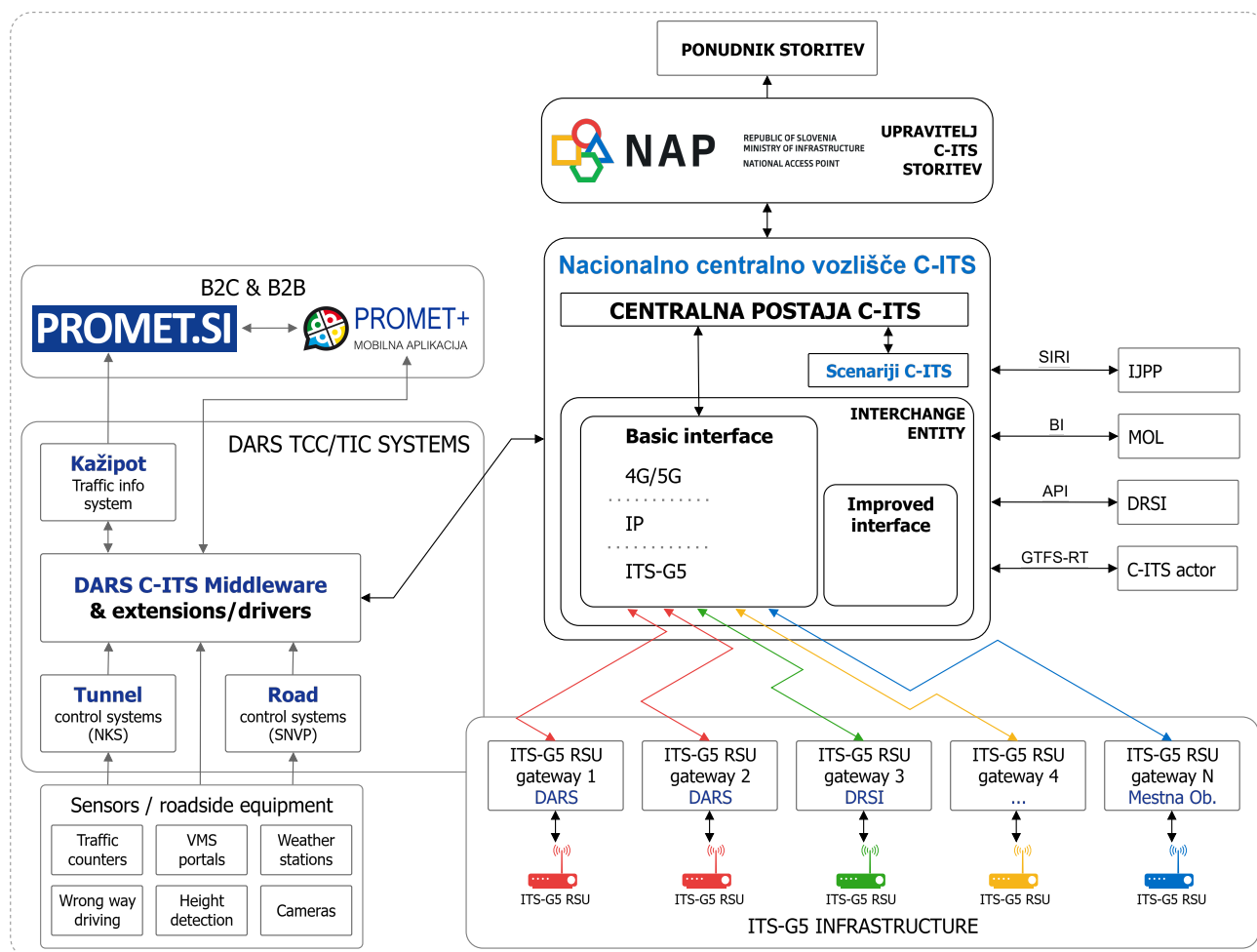
Upravljanje različic sistema zagotavlja kontinuirano kompatibilnost pri prehajanju na nove profile DATEX II standarda preko strukturiranega postopka preizkušanja (staging) pred produkcijsko uporabo, kar minimizira tveganja pri posodobitvah in zagotavlja gladke prehode med različicami.



3.4 Izvedba poveztljivosti z nacionalnim sistemom C-ITS

3.4.1 Nacionalni sistem C-ITS⁷

Slika 16 prikazuje pričakovano strukturo C-ITS, ki jo gradi Slovenija. Prikazano je nacionalno centralno vozlišče C-ITS (angl. National central C-ITS node). Vozlišče bo integrirano v informacijski sistem NCUP. Na ta del se lahko povezujejo različni ponudniki (C-ITS actor), ki na dogovorjen način posredujejo informacije v informacijski sistem NCUP. Na shemi je podrobneje prikazan trenutno aktiven akter C-ITS, to je DARS, ki s svojimi sistemi že ustvarja sporočila C-ITS skladna s specifikacijami C-Roads.



Slika 16. Shema sistema C-ITS v Sloveniji

Vsi nazivi, ki se v shemi uporabljajo za poimenovanje komponent Nacionalnega centralnega vozlišča C-ITS, so povzeti in skladni z definicijami projekta C-Roads in jih je na ta način potrebno tudi razumeti

⁷ Povzeto po dokumentu Tehnična specifikacija »Sistemi za delovanje ITS in C-ITS rešitev, SKLOP 1:

Nacionalno centralno vozlišče C-ITS», NCUP, Maj, 2025



(glej harmoniziran komunikacijski profil C-Roads⁸). Nazivi komponent sistema DARS so povzeti po specifikacijah DARS. Zunanji ponudniki storitev, ki svoje storitve gradijo na toku C-ITS sporočil, ki se pretaka skozi nacionalno vozlišče, se z vozliščem povezujejo preko Nacionalne točke dostopa (NAP), preko katere dostopajo do aplikacije za registracijo in konfiguriranje naročanja na informacijske vsebine C-ITS (Upravitelj C-ITS storitev za NAP). Na NAP se ustvari personalizirana točka dostopa, kjer ponudnik storitve nato prejema tok C-ITS sporočil preko IP omrežja. Poseben primer zunanjih storitev so vmesniki, ki C-ITS sporočila, ki jih prejmejo iz nacionalnega vozlišča C-ITS, preko mobilnih operaterjev 4G/LTE/5G posredujejo do končnih uporabnikov v IP omrežju. Na ta način se omogoči hibridni način delovanja C-ITS sistema, torej ob C-ITS g5 (na obcestnih postajah RSU) lahko poteka tudi distribucija C-ITS sporočil preko omrežij 4G/LTE/5G.

Nacionalno centralno vozlišče C-ITS zajema centralno postajo C-ITS (angl. *Central C-ITS Station*) ter izmenjevalno vozlišče, v skladu s specifikacijami C-Roads (WG2/TF4 – delovna skupina 2, podskupina 4 za hibridno komunikacijo). Centralna postaja C-ITS oblikuje vsebino sporočil C-ITS za potrebe storitev in scenarijev C-ITS. Podatke o stanju v prometnem sistemu in zahteve za C-ITS sporočila centralna postaja C-ITS dobi od podsistema za implementacijo C-ITS storitev (na sliki prikazan kot Scenariji C-ITS). Pripravljena C-ITS sporočila posreduje izmenjevalnemu vozlišču, kjer deluje t.i. *Basic Interface* (BI), ki opremi vsebino sporočila z meta podatki, potrebnimi za filtriranje in izmenjavo sporočil med akterji in vozlišči sistema skladno s standardi ETSI⁹ ter posreduje sporočila v omrežje. Sestavni del izmenjevalnega vozlišča mora biti tudi t.i. *Improved Interface* (II), ki je namenjen nadzoru pretoka informacij med akterji, še posebej v mednarodnem prostoru. Preko II se akterji med seboj na zaupanja vreden način sporazumevajo glede registracije in konfiguracije naročanja na informacijske vsebine in si izmenjujejo informacije o razpoložljivih vsebinah in zmožnostih sistema. Zgoraj naveden Upravitelj C-ITS storitev za svoje delovanje uporablja storitve II.

3.4.2 Zahteve za vzpostavitev sistema C-ITS v MOL

Opisana je implementacija mestnega sistema C-ITS v MOL in njegova povezava z nacionalnim vozliščem C-ITS (NCUP). Rešitev omogoča izmenjavo standardiziranih sporočil, hibridno komunikacijo (ITS-G5 in IP prek mobilnih omrežij) ter usklajeno delovanje z nadzornim centrom za upravljanje prometa (CUP).

Cilje in zahteve so naslednje:

- Prednostna signalizacija za vozila javnega prevoza (JPP) in vozila s prednostjo v realnem času.
- Opozorila voznikom o razmerah na cesti (nenadni zastoji, nesreče, spolzke površine, zapore).
- Optimizacija upravljanja semaforiziranih križišč na podlagi podatkov o dohodnem prometnem toku.
- Prenos priporočene hitrosti za optimiran prehod skozi zeleno luč (GLOSA).
- Povezava s centraliziranim sistemom za upravljanje prometa (CUP) za sinhronizacijo lokalnih in regionalnih odločitev.

⁸ dostopno na <https://releases.c-roads.eu>

⁹ seznam referenčnih standardov ETSI, C-ITS Message Profiles, C-RRoads Platform, WG2, V 2.0.5, str. 98





3.4.3 Sistemska arhitektura C-ITS Vozlišče

Mestni sistem C-ITS temelji na obcestnih enotah (RSU), ki so nameščene na prioritetnih križiščih in koridorjih pilotnega področja. Enote RSU oddajajo in sprejemajo sporočila C-ITS ter objavljajo SPATEM/MAPEM za potrebe GLOSA in drugih storitev. Krmilniki semaforjev posredujejo status signalov in programov (SPaT) ter geometrijo križišč (MAP) prek standardnih vmesnikov neposredno do RSU ali posredno skozi CUP, kar omogoča usklajene spremembe programov in varno centralno upravljanje.

MAPEM (MAP Extended Message) predstavlja digitalni opis križišča in pripadajočih dovozov: geometrijo pasov, topologijo povezav, dovoljene manevre in attribute (npr. omejitve po razredih vozil). Vsak pas in gibanje imata stabilne identifikatorje. SPATEM (Signal Phase And Time Extended Message) pa prenaša stanja signalov za posamezne dovoze/premike skupaj s časom do spremembe in zanesljivostjo. Skupaj tvorita par: MAPEM pove, kako je križišče zgrajeno, SPATEM pa, kaj luči počnejo zdaj in kdaj se bodo spremenile. V MOL ju oddajajo RSU prek ITSG5 in po potrebi zrcalijo prek IP kanala skozi NCUP; MAPEM se menja redkeje (ob spremembi topologije/programa ali periodično zaradi svežine), SPATEM pa pogosto in kontinuirano. Sporočila so podpisana v skladu z ETSI C-ITS PKI, IP povezave pa zavarovane z mTLS.

Za podpisovanje/validacijo ETSI ITS sporočil in zaupanja vredno izmenjavo prek nacionalnega vozlišča morajo C-ITS enote (npr. RSU, mestni C-ITS Gateway/centralna postaja in integracijski BI vmesniki) uporabljati veljavna PKI potrdila in pripadajoče ključke. V praksi to vključuje vpisno (ang. *enrollment*) potrdilo za registracijo enote v varnostno infrastrukturo C-ITS (CCMS/PKI), avtorizacijska potrdila (ang. *authorization tickets*) za konkretne profile storitev/sporočil (npr. CAM/DENM/SPATEM/MAPEM) ter posodabljan »trust list« korenskih overiteljev za preverjanje podpisov. Potrdila se pridobijo po postopku registracije pri upravljavcu nacionalne C-ITS PKI/CCMS v okviru nacionalnega sistema C-ITS (NCUP) oziroma pri pristojnem nacionalnem organu C-ITS organu; naročnik/izvajalec mora zagotoviti varno generiranje in hrambo ključev (npr. HSM ali varovan *keystore*), namestitev potrdil ter njihov življenjski cikel (rotacija/preklic). Za razvoj in integracijske teste se uporablja ločena testna (staging) PKI infrastruktura, produkcijska potrdila pa se uporabijo ob prehodu v produkcijo.

Vozila javnega prevoza in vozila s prednostjo se vključujejo bodisi z OBU napravami (ITSG5), bodisi prek GNSS telemetrije in aplikacij, ki preko CUP sprožajo zahteve za prednost; pri tem se uporabljajo sporočila SREM/SSEM ali ustrezni klici internega APIja.

SREM (Signal Request Message) je sporočilo, s katerim vozilo ali nadzorni sistem zaprosi za prednost na križišču. Vsebuje identifikator zahteve, klasifikacijo/prioritetni razred (npr. JPP, vozilo na nujni vožnji), predviden čas prihoda in potek (pristopni pas ter željeni manever) ter dodatne attribute za usklajevanje in varnost. SSEM (Signal Status Extended Message) je povratno sporočilo z odgovorom in stanjem obravnave zahtevka: potrjeno/zavrnjeno/čakanje, morebiten čas storitve (npr. ocenjen začetek zelene), povezava na konkretni premik/lanes in razlogi za odločitev. Skupaj tvorita zaprt krog: SREM sproži zahtevo za prednost, SSEM pa zagotavlja nadzorovano potrjevanje in sledljivost. V MOL se SREM lahko pošlje neposredno z OBU prek ITSG5, ali posredno prek CUP (GNSS/aplikacija), SSEM pa se vrne po isti poti; vse zahteve so časovno in prostorsko omejene (geofencing), podpisane





prek ETSI C-ITS PKI, z možnostjo povratnega preklopa na varne privzete režime ob izpadu radijske poti (fallback prek CUP).

V središču stoji mestni C-ITS Gateway, ki notranje dogodke pretvarja v ETSI sporočila (CAM, DENM, SPATEM, MAPEM, IVIM, SREM/SSEM), jih kriptografsko zaščiti in objavi, hkrati pa sprejema vsebine iz nacionalnega vozlišča in jih usklajuje z lokalnimi politikami. Integracija s CUP poteka prek dvosmernega internega APIja in zajema orkestracijo ukrepov, nadzor nad signalnimi programi, beleženje revizijskih sledi in telemetrije ter postopke povrnitve po izrednih stanjih.

Namen in funkcionalnost – C-ITS RSU (angl. Road Side Unit):

- dvosmerna komunikacija med infrastrukturo in vozili (V2I/I2V),
- podpora razširitvi v smeri V2N (angl. Vehicle-to-Network) in integracijo s centralnimi ITS sistemi,
- lokalno izvajanje logike C-ITS aplikacij in filtriranje podatkov (edge processing),
- varno in sledljivo delovanje v skladu z evropskimi C-ITS smernicami in standardi ETSI.

Namen in funkcionalnost – C-ITS OBU (angl. On-Board Unit):

- sprejem in oddaja C-ITS sporočil (CAM, DENM, SPaT, MAP, IVI),
- obveščanje voznika ali voznških sistemov o prometnih razmerah, nevarnostih in signalnih fazah,
- podpora aplikacijam, kot so:
 - GLOSA (angl. Green Light Optimal Speed Advisory),
 - opozarjanje na nevarne situacije,
 - prioritetna obravnava javnega potniškega prometa in intervencijskih vozil,
- integracija s sistemi vozil (CAN, GNSS, HMI).

3.4.4 Izmenjava z nacionalnim vozliščem (NCUP)

Povezljivost z nacionalnim vozliščem poteka preko dveh komplementarnih vmesnikov. »Basic Interface (BI)« skrbi za prenos vsebin, torej za distribucijo in sprejem C-ITS sporočil, medtem ko »Improved Interface (II)« upravlja registracije akterjev, konfiguracijo naročil na vsebine ter vzpostavlja zaupanje med sistemi v skladu s smernicami C-Roads in ETSI. Vsa sporočila so podpisana in preverjena z javnoključnim PKI po ETSI (npr. TS 103 097), IP povezave pa so dodatno zaščitene z vzajemno TLS overitvijo. Na ravni distribucije se uporablja geografsko filtriranje in naročanje po storitvah, tako da do uporabnikov pridejo le vsebine, ki so zanje relevantne v prostoru in času. MOL praviloma objavlja DENM za incidente in nevarnosti (vključno s SRTI), SPATEM/MAPEM za lokalne statusne informacije križišč (GLOSA) ter IVIM za regulativne informacije; po potrebi tudi agregirane CAM podatke. Iz NCUP prejema regionalne DENM/IVIM in usklajevalne ukrepe, ki lahko vplivajo





na lokalne politike in signalne programe. Rešitev podpira hibridno delovanje: istočasno oddajanje prek ITSG5 z RSU v vozila in prek IP kanala skozi NCUP do ponudnikov storitev.

3.4.5 Funkcionalni scenariji

3.4.5.1 Prednostna signalizacija (JPP in vozila s prednostjo)

Vozilo z OBU (ali aplikacijo prek GNSS) pošlje zahtevek za prednost (SREM) z napovedjo prihoda in smerjo prevoza (Slika 12). RSU sprejme SREM, odgovori s SSEM ter, kjer je primerno, sproži lokalno prilagoditev faz prek Križišnega računalnika in TLC Adapterja (ne neposredno), skladno z definiranimi pravili in varnostnimi omejitvami. V posrednem scenariju (GNSS/aplikacija) CUP objavi zahtevek za prednost na Sporočilno vrsto (MQTT, CONTROL tema); PCI ga prevede v ukaz za rob ("edgeCommand"), ki ga izvede Križišni računalnik. Potrditve in odgovori (SSEM/status) se objavijo na MQTT in, kjer je relevantno, tudi prek ITS-G5/IP. Vsi zahtevki so časovno omejeni, geografsko pogojeni in revizijsko zabeleženi. Ob izpadu radijske poti ali IP povezave se uporabi fallback prek CUP → MQTT.

3.4.5.2 Opozorila voznikom o razmerah

Senzorji, analitika ali CUP ustvarijo DENM ob zaznavi nevarnosti (nesreča, nenaden zastoj, spolzka vozišča, zapora). DENM se objavi lokalno prek RSU (ITSG5) in hkrati prek NCUP do ponudnikov storitev. Uporabljajo se SRTI kategorije, čas veljavnosti in preklici; redundanca z VMS sporočili ostaja možna.

3.4.5.3 Optimizacija upravljanja semaforjev

Agregati CAM, lokalne detekcije in meritve zasedenosti pasov napajajo optimizacijske algoritme v CUP. Rezultati (npr. spremembe zelenih valov, offsetov, minimalnih/ maksimalnih faz) se uskladijo s signalnimi programi krmilnikov. SPATEM/MAPEM se posodabljata skladno s spremembami, da ostane GLOSA točna.

3.4.5.4 GLOSA – priporočena hitrost

RSU in/ali CUP objavljata SPATEM/MAPEM. GLOSA (Green Light Optimal Speed Advisory) storitev na strani MOL izračuna priporočeno hitrost za prihajajoče faze na podlagi geometrije križišča, trenutnega stanja in predikcije faz. Priporočilo je na voljo aplikacijam/vozilom prek IP (prek NCUP) ali neposredno prek ITSG5; po potrebi se objavi tudi kot IVIM (regulativne/napotitvene informacije). IVIM (In-Vehicle Information Message) je standardizirano sporočilo C-ITS za posredovanje trajnih, začasnih ali dinamičnih prometnih informacij, ki jih morajo ali naj bi upoštevali vozniki in vozila med vožnjo. Gre za digitalno obliko prometnih znakov, omejitev, priporočil in opozoril, dostavljeno neposredno v vozilo (prek ITSG5 ali IP) namesto (ali poleg) fizične signalizacije. Za podporo sistemu GLOSA bodo na ključnih križiščih (na vstopno/izstopnih točkah koridorjev za vzpostavitev zelenega vala – skupno 5 takšnih koridorjev) dodatno nameščeni dinamični LED-zaslони, ki voznikom brez opreme V2X vizualno prikazujejo priporočeno hitrost. Zaslони so dvo- ali tričrkovno sestavljeni, najpogostejše velikosti 90x90 cm, s fiksnim besedilnim poljem, označenim nad ali pod numeričnim prikazom (npr. »PRIPOROČENA HITROST«).





Slika 17. LED prikazovalnik za priporočeno hitrost.

3.4.5.5 Povezava s CUP in regionalno usklajevanje

CUP ostaja centralni orkestrator lokalnih ukrepov (prioritete, spremembe programov, VMS sporočila). Prek dvosmerne integracije z NCUP se lokalne odločitve upoštevajo v regionalnem kontekstu, regionalna opozorila/ukrepi pa vplivajo nazaj na lokalno delovanje (npr. znižanje hitrosti, preusmeritve). Vsi ukrepi so sledljivi, s politiko izrednih stanj in postopki povrnitve.

3.5 Izvedba prototipne rešitve na testnem območju

3.5.1 Obstoječe stanje

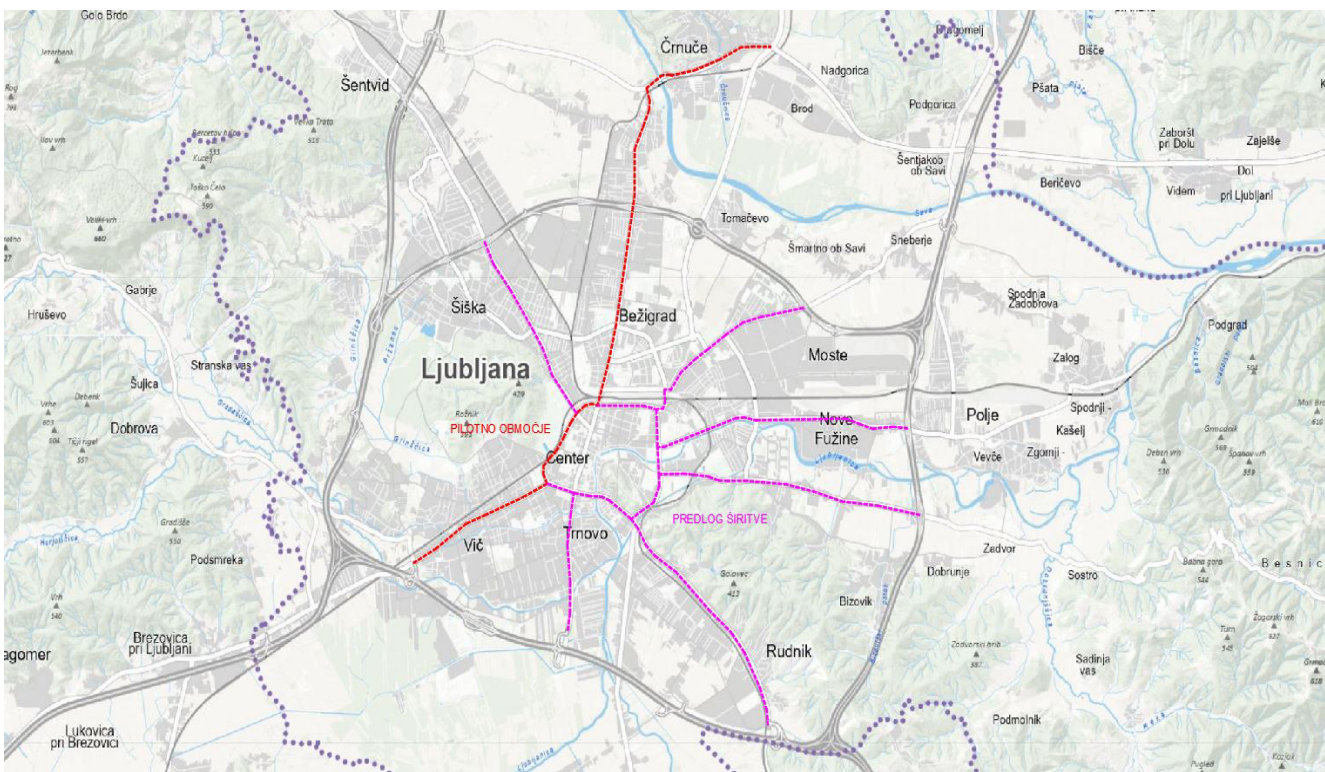
Na področju MOL je trenutno 292 semaforiziranih križišč, od tega 58 semaforiziranih prehodov za pešce in kolesarje. Križišča so različno opremljena in različnih topologij. Obstoječi sistem načeloma dobro deluje, vendar trenutna infrastruktura ne omogoča dinamičnega krmiljenja semaforizacije - enostavnega in hitrega prilagajanja trenutnim prometnim razmeram (vse željene spremembe delovanj posameznih krmilnih naprav (krmilni programi,...) je sedaj potrebno ročno vnašati na mestu samem), kot tudi ne omogoča konkretne analitike prometa v realnem času (potrebno štetje prometa in podobno).

Vse te nadgradnje ni mogoče izvesti brez celovitega posega v infrastrukturo, tako na križiščih, kot, še posebej pomembno, v nadgradnjo in modernizacijo nadzornega centra za vodenje in upravljanje prometa - CUP (kapacitete obstoječega CUP so omejene (tako tehnično, kot tudi kadrovske), zato študija predvideva celovito prenovo).

Za nadgradnjo se identificira manjkajočo ali ne dovolj zmogljivo opremo na cesti ter v CUP ter izdelava popis vseh potrebnih elementov (naprave, programska oprema, kabelske povezave, omrežne povezave, stikala, pretvorniki, itd.) in del za nadgradnjo.

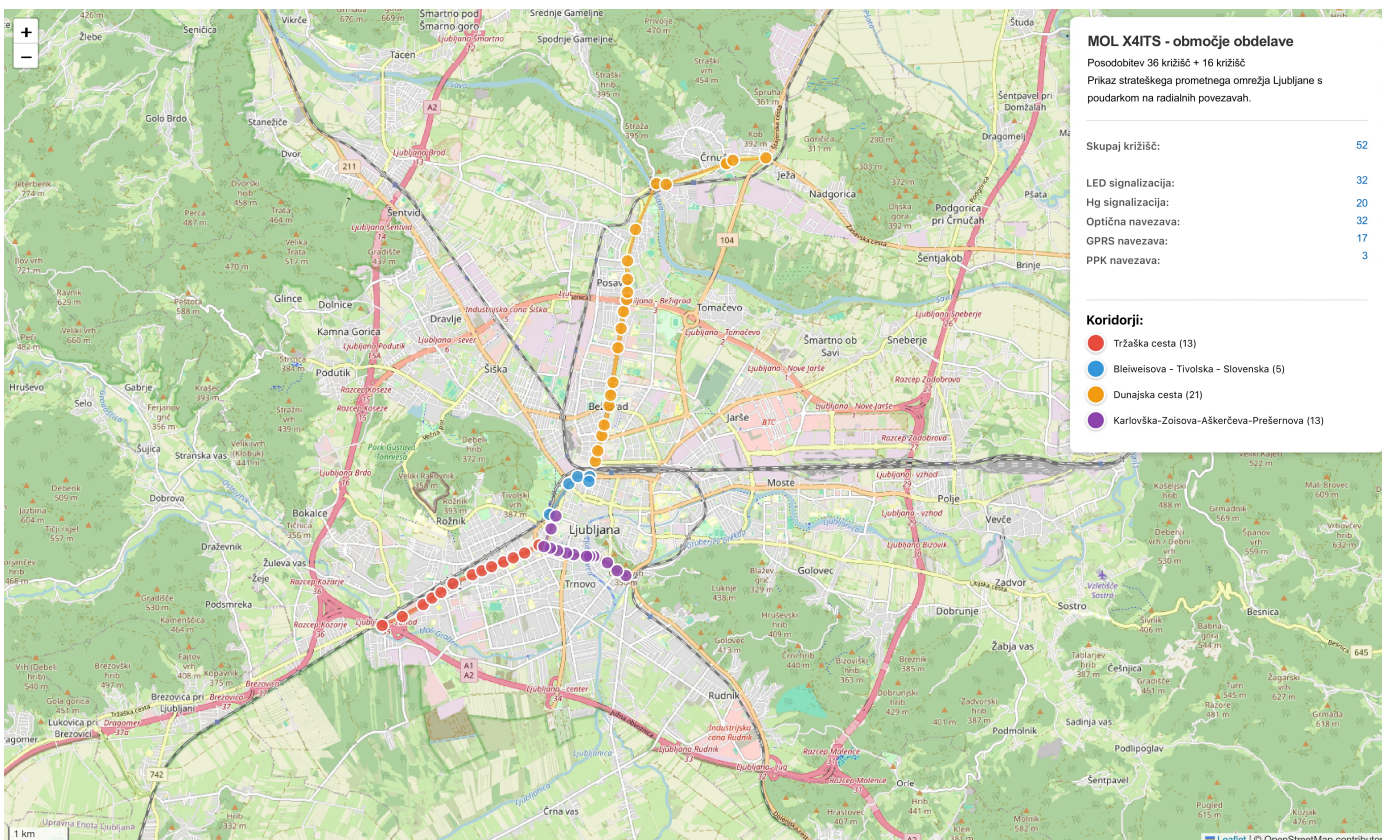
3.5.2 Obseg predvidenega območja za prototipno rešitev

Slika 18 prikazuje cestne povezave MOL, ki se radialno povezujejo z avtocestnim obročem, na katerih so bila analizirana križišča.



Slika 18 Cestne povezave MOL z radialno navezavo na AC obroč

V okviru te študije so bili, s strani naročnika, izbrani naslednji koridorji, katerih križišča in prehodi bodo kot del pilotnega območja vključeni v projekt X4ITS : Tržaška, Bleiweisova - Tivolska – Slovenska, Dunajska cesta, Karlovska - Zoisova - Aškerčeva – Prešernova (Slika 19). Gre za pilotno območje po osnovni PN (36 križišč) ter dodatnih 16 križišč. Gre za ceste strateškega pomena za radialni prometni sistem Ljubljane in predstavljajo hrbtenico povezav z regionalno cestno infrastrukturo.



Slika 19: Celotno območje s prikazom koridorjev ter pripadajočih križišč in prehodov

V nadaljevanju je prikazan tabelarični pregled pilotnega ter razširjenega območja, vključno z opisom trenutne tehnologije po posameznih križiščih.

Zap. št.	ID križišča	Opis / imena cest in ulic	Obst. tip semaforjev	Obst. tip SEM KN	Letnik obst. SEM KN	Obst. komunikacijska povezava
1.	B01	Dunajska cesta - Linhartova cesta - Bežigrad	LED	MSKE 60	2021	OPTIKA
2.	B01A	Dunajska cesta - Einspielerjeva ulica - Kržičeva ulica	LED	MSKE 60	2021	OPTIKA
3.	B02	Dunajska cesta - Samova ulica - Topniška ulica	Hg	MSKE 60	2007	GPRS
4.	B02A	Dunajska cesta - Ptujška ulica	Hg	vezan na B02		vezan na B02
5.	B03	Dunajska cesta - Posavskega ulica - Dimičeva ulica	LED	MSKE 60	2010	GPRS



6.	B04	Dunajska cesta - Tolstojeva ulica - Baragova ulica	Hg	MSKE 60	2008	OPTIKA
7.	B05	Dunajska cesta - Cesta Janeza Porente - Bevkova cesta-Štukljeva cesta	LED	MSKE 60	2009	OPTIKA
8.	B05A	Dunajska cesta - Ogrinčeva ulica	LED	MSKE 60	2010	PPK3
9.	B05B	Dunajska cesta - Ulica padlih borcev - Stoženska ulica	LED	MSKE 60	2010	PPK3
10.	B06	Dunajska cesta - Ulica 7. septembra	Hg	MSKE 60	2005	GPRS
11.	B06A	Dunajska cesta - priključek BS4	Hg	MSKE 60	2000	PPK3
12.	B07	Dunajska cesta - Cesta Ceneta Štuparja - Stare Črnuče	Hg	MSKE 60	2015	OPTIKA
13.	B08	Dunajska cesta - Cesta Ceneta Štuparja	Hg	MSKE 60	2015	OPTIKA
14.	B08A	Dunajska cesta - Lovrenčičeva	Hg	vezan na B08		vezan na B08
15.	B09	Dunajska cesta - Štajerska cesta - Zasavska cesta	Hg	MSKE 60	2009	OPTIKA
16.	B25	Dunajska cesta - Turnerjeva ulica - Kadilnikova ulica	Hg	MSKE 60	1996	GPRS
17.	B33	Dunajska cesta - Mala ulica	LED	MSKE 60	2010	GPRS
18.	B34	Dunajska cesta - Gameljska cesta	LED	MSKE 60	2009	GPRS
19.	B34A	Dunajska cesta - Izletniška ulica	LED	vezan na B34		vezan na B34
20.	C01	Bleiweisova - Celovška - Tivolska	Hg	MSKE 60	2011	GPRS
21.	C01B	Tivolska - Vošnjakova	Hg	MSKE 60	1999	GPRS
22.	C02	Bleiweisova - Šubičeva	LED	MSKE 60	2003	GPRS
23.	C04	Tržaška - Trg MDB - Bleiweisova	LED	MSKE 60	2021	OPTIKA
24.	C10	Tivolska - Slovenska - Dunajska cesta - Trg OF	Hg	MSKE 60	2002	GPRS
25.	C10A	Dunajska cesta - Vilharjeva cesta	LED	MSKE 60	2016	OPTIKA
26.	C10B	Dunajska cesta - prehod pri Gospodarskem razstavišču	LED	vezan na C10A		vezan na C10A



27.	C04A	Aškerčeva cesta - Prešernova cesta				
28.	C05	Aškerčeva cesta - Slovenska cesta				
29.	C27	Aškerčeva cesta - Snežniška ulica				
30.	C27A	Aškerčeva cesta - Murnikova ulica				
31.	C05A	Zoisova cesta-Emonska cesta-Hieronimova ulica				
32.	V01	Tržaška - Šestova - Jadranska	LED	MSKE 60	2021	OPTIKA
33.	V01A	Tržaška - Vrhovnikova	LED	vezan na V01		vezan na V01
34.	V02	Tržaška - Gregorinova	LED	MSKE 60	2006	OPTIKA
35.	V02A	Tržaška - Kogejeva	LED	MSKE 60	2021	OPTIKA
36.	V03	Tržaška - Tbilisijska - Fajfarjeva	LED	MSKE 60	2021	OPTIKA
37.	V03A	Tržaška - prehod pri poslovnem objektu	LED	vezan na V03		vezan na V03
38.	V04	Tržaška - Pot rdečega križa	LED	MSKE 60	2016	OPTIKA
39.	V13	Tržaška - Viška cesta	LED	MSKE 60	2003	OPTIKA
40.	V15	Tržaška - Oražnova - Langusova	LED	MSKE 60	2005	OPTIKA
41.	V15A	Tržaška - prehod pri FE	LED	vezan na V15		vezan na V15

Tabela 1. Pregledna tabela križišč za pilotno območje (41 križišč)

3.5.3 Pristop k nadgradnji obstoječe prometne infrastrukture

Implementacija sistema pametne prometne infrastrukture na 41 zahteva sistematičen pristop, ki uravnoteži stroškovno učinkovitost, minimalno motenje prometa in postopno uvedbo naprednih funkcionalnosti. Nadgradnja obstoječih semaforских sistemov predstavlja kompleksen inženirski izziv, saj mora zagotoviti interoperabilnost med različnimi generacijami opreme in proizvajalci ter hkrati omogočiti postopni prehod k komunikaciji C-ITS.

3.5.3.1 Analiza obstoječega stanja in kategorizacija križišč

Pregled predvidenih 41 križišč razkriva heterogeno infrastrukturo z opremo različnih starosti (od 1994 do 2024) in tehnologij.

Ključna razdelitev:





- križišča z LED signalno opremo ter z optičnimi komunikacijskimi povezavami (2016-2021): predstavljajo najboljšo osnovo za hitro nadgradnjo, saj že imajo digitalno infrastrukturo in sodobno komunikacijo.
- Starejša križišča z LED signalno opremo ter z GPRS komunikacijskimi povezavami (2003-2016): potrebujejo nadgradnjo komunikacijskih povezav na optiko.
- križišča s signalno opremo v Hg izvedbi ter z GPRS komunikacijskimi povezavami (1997-2011): zahtevajo celovito prenovo signalne opreme na LED tehnologijo in modernizacijo krmilne opreme.

3.5.3.2 Fazni pristop k nadgradnji:

- Faza 1 -- Terenska inventarizacija in priprava lokacij (M1-M2; DP2)
 - popis tipov križišč (LED optika / LED GPRS / Hg GPRS), krmilnikov in detektorjev
 - pregled povezljivosti in izvedljivosti (optika, LTE/5G, napajanje, omare)
 - izbor prioriternih križišč za pilotno zaporedje nadgradnje
- Faza 2 -- Povezljivost in osnovna varna komunikacija do terena (M1-M4; DP3 + del DP6)
 - nadgradnja/utrjevanje komunikacij (zamenjava GPRS, kjer je izvedljivo prehod na optiko)
 - uvedba redundantnih LTE/5G povezav za kritična križišča
 - vzpostavitev VPN in osnovnega nadzora/belženja za terenske naprave
- Faza 3 -- Namestitev križiščnega računalnika in telemetrija križišč (M3-M6; DP6)
 - namestitev križiščnega računalnika (lokalni MQTT + most do centralnega sistema)
 - standardizirana telemetrija (zdravje/stanje), alarmiranje in oddaljeno upravljanje
 - priprava tem MQTT za krmiljenje (CONTROL) in telemetrijo (DATA)
- Faza 4 -- Senzorika in integracija s krmilniki (M4-M9; DP6)
 - integracija prometnih kamer (zaznavanje z AI) in detektorjev pešcev/kolesarjev
 - TLC adapter in prioritetne logike (JPP/izredna vozila) ter terenska kalibracija
 - postopna širitev na dodatna križišča po potrjenih konfiguracijskih vzorcih
- Faza 5 -- C-ITS oprema na terenu (RSU/OBU) in V2X tokovi (M6-M8; DP5; OBU pilot M6-M7; DP5.5)
 - namestitev in konfiguracija RSU na izbranih lokacijah
 - aktivacija V2X tokov (SPaT/MAP/IVI) in preverjanje skladnosti (PKI/mTLS)





- integracija OBU na pilotnih vozilih ter terenska validacija scenarijev (npr. GLOSA)
- Faza 6 -- Pilotna izvedba, stabilizacija in priprava na razširitev (M7-M12; DP9/DP10)
 - pilotsko obratovanje na izbranem naboru križišč, odprava napak in optimizacije
 - potrjevanje postopkov vzdrževanja/operativnega odziva za terenske komponente
 - priprava na širitev (uvajanje) na razširjeno območje in prehod v produkcijo

3.5.3.3 Tehnični pristop k posameznim tipom križišč:

Za križišča z LED signalno opremo in z optiko:

Ti sistemi potrebujejo predvsem programsko nadgradnjo krmilnikov in dodajanje modulov C-ITS.

Pristop vključuje:

- Namestitev križiščnega računalnika (Pametno križišče) za lokalni MQTT broker, fusion/aggregator
- Razvoj programskega modula Adapter za krmilnik semaforja po Specifikaciji Adapterja za krmilnik semaforja
- Namestitev prometnih kamer (Detektor prometa) za AI detekcijo vozil, JPP, vrst in incidentov
- Namestitev detektorjev pešcev/kolesarjev (Detektor pešcev/kolesarjev) z vizualno in termično kamero
- Testiranje kompatibilnosti s centralnimi sistemi preko staging okolja

Za križišča z LED signalno opremo in z GPRS:

Potrebna je nadgradnja komunikacijske infrastrukture ob ohranitvi obstoječe signalne opreme:

- Nadgradnja komunikacijskih povezav: namestitev optičnih povezav
- Namestitev križiščnega računalnika (Pametno križišče) za lokalni MQTT broker, fusion/aggregator
- Razvoj programskega modula Adapter za krmilnik semaforja po Specifikaciji Adapterja za krmilnik semaforja
- Namestitev prometnih kamer (Detektor prometa) za AI detekcijo vozil, JPP, vrst in incidentov
- Namestitev detektorjev pešcev/kolesarjev (Detektor pešcev/kolesarjev) z vizualno in termično kamero
- Testiranje kompatibilnosti s centralnimi sistemi preko staging okolja

Za križišča s Hg signalno opremo in z GPRS:





Potrebna je celovita prenova s popolno zamenjavo svetlobne in krmilne opreme:

- Zamenjava živosrebrnih svetilk z LED moduli z zmanjšano porabo energije
- Nadgradnja komunikacijskih povezav: namestitev optičnih povezav ali LTE/5G modulov
- Namestitev križišnega računalnika (Pametno križišče) za lokalni MQTT broker, fusion/aggregator
- Razvoj programskega modula Adapter za krmilnik semaforja po Specifikaciji Adapterja za krmilnik semaforja
- Namestitev prometnih kamer (Detektor prometa) za AI detekcijo vozil, JPP, vrst in incidentov
- Namestitev detektorjev pešcev/kolesarjev (Detektor pešcev/kolesarjev) z vizualno in termično kamero
- Testiranje kompatibilnosti s centralnimi sistemi preko staging okolja





4 Projektni načrt za implementacijo MOL-ITS sistema

4.1 Pregled projekta

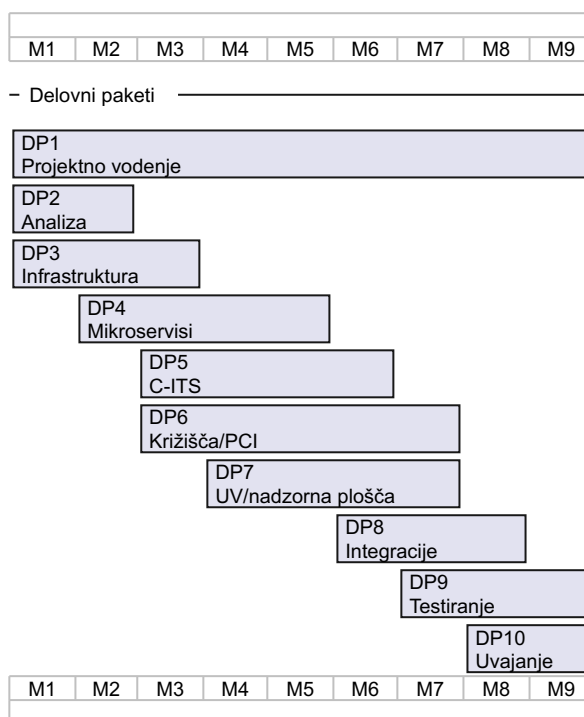
Trajanje: 9 mesecev

Začetek: M1 (T0 = datum podpisa pogodbe)

Zaključek: M9 (T0 + 9 mesecev)

4.2 Časovni načrt projekta

Projektni načrt za MOL-ITS - Informacijski sistem za upravljanje prometa v CUP



Slika 20. Časovni potek projekta

4.3 Struktura delovnih paketov

4.3.1 DP1: Projektno vodenje in upravljanje

Trajanje: Celotno obdobje projekta (9 mesecev)

Odgovorna oseba: Projektni vodja

4.3.1.1 Aktivnosti:

- **DP1.1** Vzpostavitev projektne pisarne
 - Definiranje projektne organizacije





- Vzpostavitev komunikacijskih kanalov
 - Priprava projektne dokumentacije
 - Trajanje: 0.5 meseca
 - Viri: 1 PM, pisarna, IT oprema
- **DP1.2** Redno projektno vodenje
 - Tedenski sestanki projektne skupine
 - Mesečno poročanje naročniku
 - Upravljanje tveganj in sprememb
 - Trajanje: 8.5 mesecev
 - Viri: 1 PM, projektna skupina
- **DP1.3** Kontrola kakovosti in standardi
 - Definiranje standardov razvoja
 - Procesi pregleda kode (angl. code review)
 - Testiranje in validacija
 - Trajanje: Celotno obdobje
 - Viri: QA specialist, arhitekt

4.3.2 DP2: Analiza in načrtovanje sistema

Trajanje: 2 meseca (M1-M2)

Odgovorna oseba: Sistemski arhitekt

4.3.2.1 Aktivnosti:

- **DP2.1** Analiza obstoječe infrastrukture
 - Inventarizacija obstoječih sistemov
 - Analiza prometnih tokov
 - Identificiranje integracijskih točk
 - Trajanje: 0.5 meseca
 - Viri: Sistemski analitik, prometni strokovnjak
- **DP2.2** Detajlno načrtovanje IT arhitekture
 - Detajliranje kontekstnega diagrama
 - Detajliranje vsebniških pogledov
 - Specifikacija komponentnih pogledov
 - Načrtovanje podatkovnih modelov
 - Trajanje: 1 mesec
 - Viri: Arhitekt, analitik, strokovnjak C-ITS
- **DP2.3** Tehnični zahtevki in specifikacije
 - Funkcijske specifikacije mikroservisov
 - API dokumentacija
 - Varnostne zahteve





- Zahteve glede zmogljivosti
 - **Trajanje:** 0.75 meseca
 - **Viri:** Arhitekt, varnostni strokovnjak
- **DP2.4** Prototipiranje ključnih komponent
 - Potrditev koncepta za dogodkovno arhitekturo (MQTT pub/sub, CQRS)
 - Potrditev koncepta za procese C-ITS (CAM/SPaT/MAP/DENM) in BI adapter
 - Prototip križiščnega računalnika (lokalni broker + bridge + detekcije kamer)
 - Trajanje: 0.75 meseca (paralelno z 2.3)
 - Viri: razvijalec senior, IoT strokovnjak

4.3.3 DP3: Infrastruktura in platforme

Trajanje: 3 mesece (M1-M3)

Odgovorna oseba: DevOps arhitekt

4.3.3.1 Aktivnosti:

- **DP3.1** Priprava razvojnega okolja
 - Vzpostavitev sistema za avtomatizirano upravljanje, razporejanje in skaliranje vsebnških aplikacij
 - Cevovod za CI/CD
 - Struktura repozitorija Git
 - Razvojna orodja
 - Trajanje: 1 mesec
 - Viri: DevOps inženir, sistemski administrator
- **DP3.2** Produkcijska infrastruktura
 - Arhitektura »Cloud/on-premise«
 - PostgreSQL grozd (JSON/PostGIS/TimescaleDB)
 - MQTT broker grozd
 - Uravnoveževalniki obremenitve in povratni posrednik (angl. reverse proxy)
 - Trajanje: 1.5 meseca
 - Viri: Infrastrukturni arhitekt, DBA
- **DP3.3** Varnostna infrastruktura
 - PKI certifikati za C-ITS (test/produkcija, proces pridobivanja)
 - VPN povezave za kamere
 - Upravljanje identitet in dostopov (IAM)
 - Varnostni nadzor (angl. security monitoring)
 - Trajanje: 1.5 meseca
 - Viri: Varnostni strokovnjak, sistemski administrator
- **DP3.4** Nadzor in beleženje (angl. monitoring in logging)
 - Centralizirano beleženje (ELK stack)





- Nadzor aplikacij (angl. application monitoring)
- Nadzor infrastrukture (angl. infrastructure monitoring)
- Alarmiranje (angl. alerting)
- Trajanje: 1 mesec
- Viri: specialist za monitoring, specialist za zanesljivo delovanje spletnega mesta

4.3.4 DP4: Razvoj osnovnih mikroservisov

Trajanje: 4 mesece (M2-M5)

Odgovorna oseba: vodja razvoja (angl. lead developer)

4.3.4.1 Aktivnosti:

- **DP4.1** Storitev Repozitorij
 - PostgreSQL ORM implementacija
 - PostGIS prostorske funkcije
 - TimescaleDB časovne vrste
 - CRUD API vmesniki
 - Trajanje: 1.5 meseca
 - Viri: 2 backend razvijalca, DBA
- **DP4.2** API Prehod (Controller) (angl. API Gateway)
 - Usmerjanje (angl. routing) in uravnoteženje bremena (angl. load balancing)
 - Avtentikacija in avtorizacija
 - Omejevanje hitrosti zahtevkov (angl. rate limiting)
 - API dokumentacija (OpenAPI ali Swagger)
 - Trajanje: 1 mesec
 - Viri: 2 backend razvijalca, arhitekt
- **DP4.3** Storitev Dogodki (zajem dogodkov)
 - Naročanje na centralni MQTT (C-ITS, detekcije kamer, telemetrija RSU)
 - Validacija in normalizacija dogodkovnih bremen (JSON)
 - Persistenca v podatkovnem Repozitoriju (angl. write model)
 - Trajanje: 1.5 meseca
 - Viri: 2 razvijalca zalednega sistema
- **DP4.4** Storitev Analitika
 - KPI metrike (zgodovinski trendi, agregacije, poročila)
 - Poizvedbe (angl. read model) prek podatkovnega Repozitorija
 - Osnovni modeli (npr. zastoje, obremenitve, SLA)
 - Trajanje: 2 meseca
 - Viri: 2 backend razvijalca, specialist za podatke
- **DP4.5** Storitev Pametna cestna infrastruktura (PCI) – del CUP API
 - Konfiguracija križišč/naprav (kamer, detektorjev) in signalnih planov





- Objavljanje ukazov prek centralnega MQTT (brez neposrednih klicev do naprav)
- Upravljanje tem (its/control//..., edge/config//...)
- Trajanje: 2 meseca (paralelno z 4.3/4.4)
- Viri: 2 backend razvijalca, IoT arhitekt

4.3.5 DP5: C-ITS integracija

Trajanje: 4 mesece (M3-M6)

Odgovorna oseba: C-ITS strokovnjak

4.3.5.1 Aktivnosti:

- **DP5.1** C-ITS vozlišče (centralno)
 - Generiranje/validacija SPaT/MAP/DENM/CAM
 - Integracija z ITS DB (arhiv) prek dogodkovnega toka
 - PKI/mTLS in upravljanje seznamov zaupanja (angl. trust list) (test/produkcija)
 - Trajanje: 2.5 meseca
 - Viri: C-ITS razvijalec, varnostni strokovnjak
- **DP5.2** C-ITS BI Adapter (AMQP 1.0)
 - Transformacija notranjih C-ITS tokov ↔ nacionalni BI (C-Roads)
 - Geo-filtriranje in podpis/validacija (JWS/PKI)
 - Operativni nadzor
 - Trajanje: 1.5 meseca
 - Viri: C-ITS razvijalec, sistemski integrator
- **DP5.3** RSU upravljanje in tokovi za V2X
 - RSU komunikacijski protokoli
 - V2X sporočila (ITS-G5/cellular V2X)
 - Telemetrija in nadzor
 - Trajanje: 1.5 meseca
 - Viri: IoT razvijalec, C-ITS strokovnjak
- **DP5.4** MQTT integracija (C-ITS ↔ CUP)
 - Definicija tem za DATA/CONTROL/PRIORITY in QoS
 - Serializacija/deserializacija (shema JSON)
 - Obvladovanje napak (angl. error handling), retry logika, vzorci obravnave nedostavljivih sporočil (angl. dead-letter patterns)
 - Trajanje: 1 mesec (paralelno)
 - Viri: backend razvijalec, IoT strokovnjak
- **DP5.5** OBU implementacija in pilot vozila
 - Integracija OBU z RSU (sprejem SPaT/MAP/DENM, pošiljanje CAM)
 - Konfiguracija certifikatov (ETSI C-ITS PKI) in varnostnih profilov
 - Testni scenariji (GLOSA, opozorila, bus/emergency priority) in validacija na terenu





- Trajanje: 1.5 meseca (M5-M6, delno paralelno)
- Viri: C-ITS razvijalec, inženir na terenu, varnostni strokovnjak

4.3.6 DP6: Pametna cestna infrastruktura

Trajanje: 5 mesecev (M3-M7)

Odgovorna oseba: IoT arhitekt

4.3.6.1 Aktivnosti:

- **DP6.1** PCI Service implementacija
 - Modeliranje konfiguracije križišč (cone, detekcije, signalni plani)
 - Konfiguracija naprav prek MQTT tem (brez direktnih klicev)
 - Upravljanje konfiguracij in revizijskih sledi (angl. audit trail)
 - Trajanje: 1.5 meseca
 - Viri: IoT razvijalec, IoT arhitekt
- **DP6.2** Pametno križišče (križiščni računalnik)
 - Lokalni MQTT broker + lokalni most (bridge) do centralnega brokerja
 - Upravljalnik dogodkov in pravil (korelacija CAM + vizualna detekcija; podpisani manifesti pravil)
 - Agent za nadzor naprav (health/status, alarmi, konfiguracijske posodobitve)
 - Trajanje: 2.5 meseca
 - Viri: IoT razvijalec, senior razvijalec
- **DP6.3** AI kamera integracija
 - Edge AI algoritmi
 - VPN konfiguracija
 - Klasifikacija udeležencev
 - Trajanje: 2 meseca
 - Viri: IoT/AI razvijalec
- **DP6.4** TLC adapter + adaptivna semaforizacija
 - Adapter za krmilnik semaforja (referenčni JSON → lastniški (angl. vendor-specific) protokol)
 - Dinamično podaljšanje zelene faze v realnem času (prioriteta avtobusa in interventnih vozil)
 - Integracija s signalnimi plani in obstoječimi TLC sistemi
 - Trajanje: 2.5 meseca
 - Viri: prometni inženir, IoT razvijalec
- **DP6.5** Detektor pešcev/kolesarjev + semaforski odštevalnik
 - Integracija detektorja pešcev/kolesarjev (dogodki MQTT/REST)
 - Tokovi SPaT (timeToChange) in prikazovalnik odštevanja (MQTT/RS-485)
 - Terenska kalibracija, cone zaznave, testiranje





- Trajanje: 1.5 meseca
 - Viri: IoT razvijalec, terenski inženir
- **DP6.6** MQTT telemetrija in spremljanje (križišča)
 - Standardizacija tem (its/data//...)
 - Pretok (angl. streaming) detekcij in nadzor zdravja/statusa
 - Alarmiranje in nadzorne plošče (SRE/operator)
 - Trajanje: 1 mesec (paralelno)
 - Viri: IoT razvijalec

4.3.7 DP7: Uporabniški vmesnik in nadzorna plošča

Trajanje: 4 mesece (M4-M7)

Odgovorna oseba: Frontend arhitekt

4.3.7.1 Aktivnosti:

- **DP7.1** Implementacija spletne nadzorne plošče
 - SPA (angl. Single Page Application) aplikacija (npr. React/Angular)
 - Real-time prometni podatki
 - Interaktivni zemljevidi
 - Prijazno mobilnim napravam (»responsive design« za pametne telefone in tablice)
 - Trajanje: 3 mesece
 - Viri: 2 frontend razvijalca, oblikovalec UX
- **DP7.2** Operatorski vmesniki
 - Upravljanje prometnih dogodkov
 - Konfiguracija sistemov
 - Nadzor in alarmiranje
 - Trajanje: 2 meseca
 - Viri: frontend razvijalec, oblikovalec UX

4.3.8 DP8: Integracije z zunanjimi sistemi

Trajanje: 3 mesece (M6-M8)

Odgovorna oseba: Integracijski arhitekt

4.3.8.1 Aktivnosti:

- **DP8.1** NAP.si integracija
 - REST API implementacija
 - Objava odprtih podatkov
 - Priprava podatkov





- Trajanje: 1 mesec
 - Viri: backend razvijalec, podatkovni specialist
- **DP8.2** Obstoječi sistemi MOL
 - Integracije obstoječih sistemov (če obstajajo)
 - Migracija podatkov
 - Trajanje: 2 meseca
 - Viri: Sistemski integrator
- **DP8.3** Integracija zunanjih API-jev
 - Vremenske napovedi
 - Prometne informacije
 - Sistem za organizacijo prireditev (če obstaja)
 - Trajanje: 1 mesec
 - Viri: backend razvijalec

4.3.9 DP9: Testiranje in validacija

Trajanje: 3 mesece (M7-M9)

Odgovorna oseba: vodja testiranja (QA)

4.3.9.1 Aktivnosti:

- **DP9.1** Enotski in integracijski testi
 - Avtomatizirano testiranje
 - Pokritost testiranja (angl. test coverage) > 80%
 - Integracija v CI/CD
 - Trajanje: Celotno obdobje razvoja
 - Viri: QA inženirji, razvijalci
- **DP9.2** Sistemsko testiranje
 - Scenariji »End-to-end«
 - Testiranje zmogljivosti (angl. performance)
 - Varnostno testiranje
 - Trajanje: 1.5 meseca
 - Viri: QA ekipa, specialist za zmogljivosti
- **DP9.3** Uporabniško testiranje (UAT)
 - Scenariji z uporabniki
 - Operatersko testiranje
 - Implementacija/popravki na osnovi povratnih informacij
 - Trajanje: 1 mesec
 - Viri: vodja testiranja (QA), ključni uporabniki, projektni vodja
- **DP9.4** Pilot implementacija





- Testno okolje v produkciji
- Omejena funkcionalnost (C-ITS RSU/OBU, PCI detekcije, prioritete logike)
- Nadzor in optimizacija
- Trajanje: 1.5 meseca
- Viri: Celotna projektna skupina

4.3.10 DP10: Uvajanje v produkcijo

Trajanje: 2 meseca (M8-M9)

Odgovorna oseba: vodja uvajanja

4.3.10.1 Aktivnosti:

- **DP10.1** Producerska namestitvev
 - »Blue-Green« uvajanje (blue – trenutno aktivno producersko okolje, green – novo verzijo, pripravljeno v ozadju)
 - Migracija podatkovne baze
 - Preklop DNS
 - Trajanje: 1 mesec
 - Viri: DevOps ekipa, DBA
- **DP10.2** Usposabljanje uporabnikov
 - Operatorski tečaji
 - Dokumentacija
 - Tehnična podpora
 - Trajanje: 0.75 meseca
 - Viri: trener, ekipa podpore
- **DP10.3** Podpora ob zagonu v produkcijo
 - Nadzor 24/7
 - Hitro reševanje težav
 - Optimizacija zmogljivosti (angl. performance tuning)
 - Trajanje: 1 mesec
 - Viri: ekipa podpore, razvijalci
- **DP10.4** Zaključek projekta
 - Predaja sistema
 - Dokumentacija
 - Trajanje: 0.25 meseca
 - Viri: PM, arhitekt

4.4 Ključni mejniki

Ključni mejniki (časovnica)





Mejnik	Datum	Opis
M1	M2	Zaključena analiza in IT arhitektura
M2	M3	Infrastruktura pripravljena (DB + centralni MQTT + CI/CD)
M3	M5	Osnovne storitve (Repozitorij, Dogodki, Analitika, API Prehod)
M4	M9	Križišča/PCI + C-ITS integracija (RSU/OBU, križiščni računalnik)
M5	M8	Integracije (NAP.si, nacionalni C-ITS)
M6	M8	Pilot uspešno izveden
M7	M9	Zagon v produkcijo in zaključek projekta

4.5 Kvalitativni kriteriji

4.5.1 Funkcijski kriteriji

- Vsi mikroservisi implementirani po specifikaciji
- Integracija C-ITS v skladu z ETSI standardi
- Realno-časovna obdelava prometnih podatkov
- 99.9% neprekinjen čas delovanja

4.5.2 Nefunkcijski kriteriji

- Odzivni čas < 200 ms za API klice
- Pretočnost > 1000 zahtev/s
- Skalabilnost do 10x trenutne obremenitve
- Varnost brez kritičnih ranljivosti





5 Repozitorij izvirne kode in dokumentacija

Vsa dokumentacija mora biti napisana v slovenskem jeziku.

5.1 Repozitorij in predaja izvirne kode

Izvajalec mora naročniku (oz. pooblaščenemu nadzoru) med razvojem zagotavljati ustrezen dostop do repozitorija za sprotni pregled izvirne kode z namenom izvajanja sprotnega zagotavljanja kakovosti.

Izvajalec naročniku preda celotno izvirno kodo z vsemi potrebnimi knjižnicami, da je mogoče neodvisno vzpostaviti delujoče razvojno okolje. Izvirno kodo je potrebno predati v obliki repozitorija, skladnega s splošno sprejetimi načini dela v industriji razvoja programske opreme (Github organizacija katerega naslov bo podal naročnik). Izvorna koda mora biti smiselno opremljena s komentarji.

Vse kasnejše nadgradnje in popravke izvirne kode je potrebno predati v isti repozitorij naročnika, tako da repozitorij vedno vsebuje zadnjo delujočo verzijo sistema ter po potrebi tudi testne verzije (module za test enot).

Za dele sistema, ki jih ni mogoče predati (npr. zaradi omejitev licenc), je potrebno natančno opisati, kako je mogoče manjkajoče dele sistema pridobiti in povezati s predano programsko kodo.

5.2 Tehnična dokumentacija

Izvajalec mora v okviru razvoja pripraviti tehnično dokumentacijo, ki vsebuje:

- opis zasnove in zgradbe sistema,
- opis vseh funkcionalnosti sistema z opisom delovanja,
- nabor in način integracije sistema z drugimi sistemi,
- opis protokolov za komunikacijo s sistemom z zahtevami glede varnosti in nadzora dostopa,
- opis protokolov za komunikacijo sistema z drugimi povezanimi sistemi s primeri.

Izvajalec mora izdelati podrobna navodila za instalacijo in konfiguriranje celotnega sistema, opisati vse parametre za konfiguracijo predane programske opreme ter potrebne nastavitve podatkovnih baz,

pripravo podatkov in drugih sistemskih nastavitev. Prav tako mora izdelati navodila za nameščanje posodobitev. Navodila naj zajemajo opis vzpostavitve testnega in produkcijskega okolja ter navodila za prehod iz testnega v produkcijsko okolje.

5.3 Uporabniška dokumentacija

Izvajalec mora izdelati navodila/priročnik za uporabnike in administratorje. Dokumentacija mora vsebovati vsaj:

- opis namena sistema in njegove glavne funkcionalnosti,
- vrste uporabnikov, ki jim je dokumentacija namenjena,





- varnostna navodila z osnovnimi smernicami za varno uporabo sistema, digitalnih potrdil, varovanje gesel in podatkov,
- podrobna navodila za uporabo vseh funkcij sistema.

Navodila za uporabo morajo vsebovati podroben opis uporabe aplikacij zaposamezna vsebinska področja in postopke.

Uporabniška dokumentacija mora uporabljati izrazoslovje poslovnega področja naročnika.

Za vsak postopek so pripravljena podrobna navodila, kako naj uporabnik uporablja aplikacije. Navodila obsegajo celotno izvedbo postopka od prijave v sistem, zagona, izvedbe in zaključka procesa, do odjave iz sistema. Pri tem se naj navodila neposredno nanašajo (tudi grafično) na uporabniški vmesnik sistema (nadzorna plošča).

Poleg glavnega toka skozi proces mora dokumentacija pokriti tudi stranske tokove. Podani naj bodo razumljivi opisi vzrokov za vsa opozorila in napake, ki jih povzročajo uporabniške in/ali systemske funkcije.

Podana naj bodo podrobna navodila za programske vmesnike in konfiguracijo dostopa do sistema z uporabo programskih rešitev (API vmesniki).

V uporabniški dokumentaciji je potrebno navesti kontaktno osebo ali naslov za pomoč pri morebitnih nejasnostih glede uporabe sistema. Pri popravkih in nadgradnjah je potrebno zagotoviti posodabljanje vseh delov tehnične in uporabniške dokumentacije, ki morata ostati skladni s produkcijsko verzijo sistema.





6 PRILOGA 1: Mikroservisi in REST API metode MOL-ITS

Podrobna specifikacija mikroservisne arhitekture, komunikacijskih vzorcev in REST API metod je zapisana v ločenem dokumentu Mikroservisi-in-REST-API-metode-MOL-ITS.pdf.





7 PRILOGA 2: Specifikacija adapterja za krmilnik semaforja

Generični vmesnik za komunikacijo med križiščnim računalnikom (Pametno križišče / Križiščni računalnik) in prometnimi svetlobnimi kontrolerji (Semafor / krmilnik) različnih proizvajalcev.

Vsak dobavitelj krmilnika semaforjev mora razviti programski Adapter za krmilnik semaforja, ki implementira ta vmesnik in prevaja standardne JSON ukaze/poizvedbe v lastniški protokol (NTCIP/SNMP, ASCII, drugo).

Arhitekturni kontekst vsebuje:

- križiščni računalnik: lokalno odločanje, pretvorba in filtriranje dogodkov
- adapter za krmilnik semaforja: pretvorba referenčnih zapisov (JSON) krmilnih programov križišč (semaforjev) v lastniške protokole proizvajalca, stanje in diagnoza, pretvorba signalnih programov MOL ITS v zapisu JSON v format proizvajalca
- krmilnik semaforja: izvršuje časovne programe, upravlja s signalnimi glavami, poroča o statusu in ga lahko lahko ponazorimo takole:

[Pametna cestna infrastruktura / Pametno križišče]

↓ JSON/REST ali MQTT

[Adapter za krmilnik semaforja]

↓ protokol naprave (NTCIP, ASCII, lastniški)

[krmilnik semaforja – fizična naprava]

Specifikacija minimalnega aplikacijskega vmesnika je opisana v ločenem dokumentu Specifikacija adapterja za krmilnik semaforja.pdf, skupaj z referencami na referenčno shemo JSON modela križišča (intersection-controller_schema.json) in primera B01.yaml skladnega s shemo.





8 PRILOGA 3: Konfiguracije krmilnih programov križišč (semaforjev) v referenčnem zapisu JSON

Za potrebe projekta je bila izvedena prometna analiza za pilotno območje in predstavlja osnovo za krmilne programe na ravni posameznih križišč, koridorjev in con.

Krmilni programi določajo ključne parametre za consko upravljanje prometa: dolžino cikla, fazne delitve in odmike. Ti parametri so osnovna orodja za koordinirano upravljanje semaforizacije na širšem prometnem območju.

Prometna analiza vključuje tudi diagrame poti/časa z izračunanimi zelenimi valovi, na podlagi katerih se določa priporočena hitrost vozila.

Ker se cikli, delitve in odmiki lahko spreminjajo načrtovano ali dinamično (na podlagi sprotne meritve prometnega toka), se ustrezno spremeni tudi priporočena hitrost. Sistem zato samodejno posreduje novo vrednost prek GLOSA in/ali prikazovalnikov, kar zagotavlja pravočasno in jasno obveščanje udeležencev v prometu.

Prometna analiza je referenčni okvir, vendar programi v obratovanju niso statični. Sistem neprekinjeno obdeluje meritve (število in tip vozil, doline čakalnih vrst, čakalni časi, obremenitve pristopov) ter adaptivno prilagaja parametre semaforizacije. Tako se osnovna matrika upravljanja dinamično prilagaja realnim razmeram na osnovi posameznega križišča.

Za pilotno območje so se za vsa križišča izdelali načrti v programu LISA+. Rezultati so dostopni kot izvozi v datoteke PDF in so vključeni v prilogi.

Priloga vsebuje tehnično dokumentacijo za križišča in predstavlja referenčni sklop podatkov za načrtovanje, izvedbo in preverjanje integracije križišča v sistem MOL-ITS. Namen priloge je zagotoviti enotno podlago za razumevanje geometrije križišča, signalne opreme, logike krmiljenja ter povezave s križiščnim računalnikom in centralnim delom sistema. Vsebina je organizirana v tri vsebinske sklope:

- konfiguracija krmilnega programa (mapa KKP) v strojno berljivi obliki (YAML/JSON),
- kartografski prikaz križišča (mapa Karta), ter
- PDF izvoz tehničnih diagramov in signalnih planov krmilnika izdelanih v programu LISA+ (mapa LISA).

Dokumentacija omogoča sledljivost med obstoječim stanjem na terenu in ciljnimi podatkovnim modelom, ki se uporablja za konfiguracijo krmilnika križišča (semaforjev), validacijo signalnih planov ter pripravo testnih in operativnih postopkov.



9 PRILOGA 4: Specifikacija računalniške in strojne opreme za CUP

9.1.1 Infrastruktura strojne opreme nadzornega centra CUP

Center za upravljanje prometa (CUP) zahteva robustno strojno infrastrukturo, ki lahko v realnem času obdeluje velike količine podatkov iz skupno 36 pametnih križišč v prvi fazi. Sistem mora zagotavljati neprekinjeno delovanje 24/7, hitro odzivanje na dogodke, varno hrambo kritičnih podatkov ter skalabilnost za prihodnje razširitve. Obstoječa arhitektura je zasnovana modularno in omogoča postopno razširitev. Za podporo do 250 križišč je potrebna nadgradnja: podvojitev glavnega computing clustra (12 vozlišč), razširitev kapacitet za koordinacijo križiščnih računalnikov (6-7 vozlišč), dodatni strežniki za podatkovno bazo (5 vozlišč), ter izboljšana omrežna infrastruktura. Modularna zasnova omogoča fazirano nadgrajevanje brez prekinitve delovanja.

9.1.2 Arhitektura podatkovnega centra

9.1.2.1 Primarna lokacija CUP

Glavna strežniška infrastruktura, nameščena v varovanem podatkovnem centru z nadzorom dostopa, sistemom za preprečevanje požara, klimatizacijo in neprekinjeno napajanje:

- Strežniški prostor: kabineti ohišja 42U z redundantnim napajanjem in hlajenjem
- Varnostni sistemi: biometrijski dostop, video nadzor, alarmni sistemi
- Okoljski nadzor: temperatura 18-22°C, relativna vlažnost 40-60%, prisilno prezračevanje
- Požarna varnost: FM200 sistem za gašenje brez vode, zgodnje zaznavanje dima
- Neprekinjeno napajanje: UPS sistemi z 15-minutno avtonomijo + dizelski generator za daljše izpade

9.1.2.2 Sekundarna lokacija

Geografsko ločen center za kontinuiteto delovanja sistema v kritičnih situacijah:

- Oddaljenost ≥ 15 km od primarne lokacije za izogibanje regionalnim motnjam
- Sinhronizacija podatkov v realnem času preko optičnih povezav
- Zmožnost prevzema celotnega prometa v 15 minutah ($RTO \leq 15$ min, $RPO \leq 5$ min)

Opcija izvedbe: Kolokacija v zunanjem podatkovnem centru (priporočeno) ali lastna investicija. Kolokacija omogoča fleksibilnost, profesionalno upravljanje infrastrukture ter nižje začetne stroške (prostor rack + napajanje + povezljivost), medtem ko lastna investicija zahteva investicijo za prostor, hlajenje, UPS in varnostne sisteme.

Vzpostavitev sekundarne lokacije ni naloga izvajalca. Za izvajalca je to informacija, ki jo mora upoštevati pri vseh razvojnih aktivnostih v tem dokumentu (npr. virtualizacija, zahteva po vsebnikih).

9.1.2.3 Strežniška infrastruktura

Visokozanesljivi glavni strežniški grozd za procesiranje komunikacije C-ITS in prometno analitiko:





9.1.2.3.1 Specifikacije računalniškega grozda

Konfiguracija vozlišča:

- CPU: 2x Intel Xeon Gold 6354 (18 core/36 thread @ 3.0GHz)
- RAM: 256GB DDR4-3200 ECC (razširljivo do 512GB)
- Shramba: 2x 1.92TB NVMe SSD (RAID 1) + 4x 7.68TB SAS SSD
- Omrežje: 4x 25GbE + 2x 100GbE QSFP28
- Redundanca: dvojni PSU, komponente z vročo zamenjavo

Velikost grozda: 6 vozlišč (4 aktivna + 2 v pripravljenosti)

Skupna zmogljivost:

- Računska zmogljivost: 216 jeder (vsa vozlišča), 144 jeder (aktivna)
- Delovni pomnilnik: 1.5TB RAM (vsa vozlišča), 1.0TB RAM (aktivna)
- Shramba: ~100TB uporabnega SSD (aktivna), ~92TB po rezervi
- Hipervizor: VMware vSphere 8.0 z HA/DRS
- Orkestracija: gruča Kubernetes za mikroservise
- Razširljivost: razširljivo do 12 vozlišč za 250+ križišč

9.1.2.4 Specializirani strežniki za posebne naloge

9.1.2.4.1 C-ITS strežniki (2 + 1 v pripravljenosti)

Specializirani za obdelavo ETSI C-ITS sporočil in PKI operacije:

- CPU: Intel Xeon Silver 4316 (20 core @ 2.3GHz) z AES-NI
- RAM: 128GB ECC za predpomnjenje PKI certifikatov
- Shramba: 960GB NVMe za hiter dostop do kriptografskih ključev
- Omrežje: 4x 10GbE + hardware security module (HSM) za PKI
- Specializacija: namenske kartice za kriptografsko pospeševanje ETSI TS 103 097

9.1.2.4.2 Koordinacijski strežniki za pametno cestno infrastrukturo (3 vozlišča, razširljivo na 7 vozlišč)

Sistemi za upravljanje in koordinacijo porazdeljenih naprav za detekcijo prometa na križiščih:

- CPU: Intel Xeon Silver 4316 (20 core @ 2.3GHz)
- RAM: 128GB ECC za koordinacijo analitike naprav v križišču
- Shramba: 3.84TB NVMe za agregacijo podatkov iz terena
- Omrežje: 4x 25GbE za komunikacijo z napravami v križišču
- Funkcionalnost: orkestrator delovanja naprav v križišču, agregator analitičnih rezultatov





- Kapaciteta: 3 vozlišča → 36-105 križišč (trenutna ciljna postavitev: 36; razširitev: 52+); 7 vozlišč → 250+ križišč (okvirno ~35-40 lokacij na vozlišče, odvisno od obremenitve)

9.1.2.4.3 Podatkovni strežniki (2 + 1 v pripravljenosti, razširljivo na 5 vozlišč)

Visokozanesljivi sistem za prometne podatke in konfiguracijo:

- CPU: Intel Xeon Platinum 8358 (32 core @ 2.6GHz)
- RAM: 1TB ECC za operacije podatkovne baze v pomnilniku
- Shramba: 8x 3.84TB NVMe SSD s strojnim RAID krmilnikom
- Omrežje: 4x 25GbE z LACP združevanjem povezav
- Podatkovna baza: gruča PostgreSQL s pretočno replikacijo
- Razširljivost: dodatna vozlišča za 250+ križišč (grupiranje po po koridorjih)

9.1.2.5 Infrastruktura v križiščih

Računalniki na 36 pilotnih lokacijah tvorijo sistem porazdeljenih računalniških enot (križiščnih računalnikov) za agregacijo podatkov iz detekcijskih kamer, fuzijo detekcij in koordinacijo križišča.

9.1.2.5.1 Specifikacija Križiščnega računalnika (izboljšani industrijski računalnik):

Strojna platforma: industrijski PC (razred ~€8.000)

- CPU: Intel Core i7-12700K / Xeon W-1370 (8-16 cores @ 3.6GHz)
- GPU: NVIDIA RTX A4000 (6144 CUDA jeder) + integrirana grafika (za prihodnjo PTZ koordinacijo)
- RAM: 64GB DDR4 ECC (razširljivo do 128GB)
- Shramba: 2TB NVMe SSD za MQTT medpomnilnik + lokalno predpomnjenje dogodkov + PTZ video posnetki incidentov (opcija)
- Omrežje: 4x GbE + Wi-Fi 6E + opsijski 5G modem
- Poraba: 200W (z možnostjo UPS rezervnega napajanja)
- Operacijski sistem: Ubuntu 22.04 LTS / Windows IoT Enterprise
- Izvedba ohišja: robustna zasnova brez ventilatorja, razred IP65

Funkcije za križiščni računalnik:

- Fuzija agregatnih podatkov iz 4x prometnih kamer + 1-4x detektorjev pešcev/kolesarjev
- Korelacija detekcij preko več pogledov kamer
- Fuzija CAM + vizualne detekcije za prioriteto avtobusov/nujna vozila
- TLC protokolarni adapter (kanonični JSON → vendor-specifični)
- Lokalni MQTT broker + most do centralnega sistema (Lokalni Most MQTT)
- Opcijsko:
 - PTZ kamera koordinacija (opcijsko: kontrolni ukazi + sprejem video posnetkov)





- PTZ snemanje incidentov (shranjevanje kratkih video posnetkov ob nesrečah/incidentih)
- Sinhronizacija večih kamer za koordinirane detekcijske cone

PTZ koordinacijske zmogljivosti (opcijsko):

- Generiranje kontrolnih ukazov PTZ na podlagi agregatnih detekcij
- Koordinirano pozicioniranje PTZ preko več kamer
- Upravljanje prednastavitev za samodejne nadzorne vzorce
- Z dogodki sprožene PTZ akcije (npr. povečava na lokacijo incidenta)
- Video snemanje ob incidentih (shranjevanje 30-60s posnetkov ob zaznavi skorajšnje nesreče)
- Lokalni medpomnilnik za posnetke incidentov (2TB zadostuje za ~500-1000 incidentov)

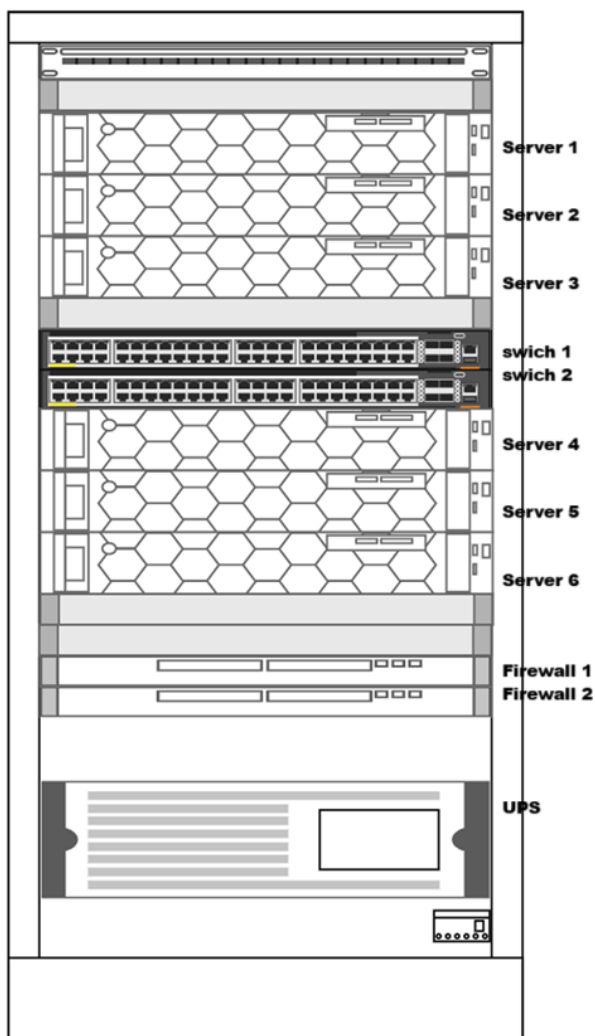
Komunikacija:

- MQTT za dogodke v realnem času do centralnega sistema
- REST API za konfiguracijo in status
- Šifriran prenos podatkov (TLS 1.3)
- Monitoring (angl. heartbeat) in oddaljena diagnostika
- Opcijsko: kontrolni protokoli PTZ (ONVIF, Pelco-D/P, Sony VISCA)

9.1.3 Specifikacija strežniške omare

Strežniška omara 42U je standardno ohišje polne višine, zasnovano za namestitev IT infrastrukture, vključno s strežniki, stikali, razdelilniki in drugo 19-palčno opremo, ki jo je mogoče namestiti v omaro. Z robustno konstrukcijo in optimiziranim upravljanjem pretoka zraka je primerna za podatkovne centre, strežniške sobe in omrežna distribucijska vozlišča.





Slika 21: Princip omare strežnika

Tehnične zahteve:

- Standardno ohišje: 42U (1U = 1,75 palca / 44,45 mm)
- Dimenzije (V x Š x G): približno 2000 × 600 × 1000 mm (lahko se nekoliko razlikuje glede na proizvajalca)
- Širina stojala: Standardni 19-palčni zaslon, skladen z EIA-310
- Nosilnost: Statična obremenitev do 1000 kg (odvisno od modela)
- Ohišje: Hladno valjani jekleni okvir z ojačanimi montažnimi tirnicami in odstranljivimi stranskimi ploščami
- Vrata:
 - Vhodna vrata: Perforirano jeklo ali steklo (kaljeno), možnost zaklepa
 - Zadnja vrata: Perforirano jeklo za izboljššan pretok zraka, možnost zaklepa
- Stranske plošče: Snemljivo z možnostjo zaklepanja, opcijsko brez orodja
- Podpira pretok zraka od spredaj proti zadaj za optimalno upravljanje toplote
- Neobvezno:



- Zgornji pladenj ventilatorjev (4 ali 6 ventilatorjev)
 - Spodnji kabelski vhod s krtačnimi ploščami
- Predhodno izvrtane prezračevalne odprtine za pasivno hlajenje
- Zgornja in spodnja dostopna točka za kabelski vhod
- Navpični organizatorji kablov (neobvezno)
- Krtačni trakovi za zmanjšanje prahu in ohranjanje ločevanja
- Združljivo z navpičnimi in vodoravnimi PDU-ji (enotami za distribucijo energije)
- Ozemljitvena letev vključena ali opcijsko
- Skladno z EN 60950 in drugimi ustreznimi varnostnimi standardi
- Nastavljive navpične montažne letve (prilagodljivost globine)
- Oznaka U na tirnicah za enostavno poravnavo opreme
- Kolesca in nivelirne nogice za mobilnost in stabilnost
- Dostop zadaj za upravljanje kablov in vzdrževanje

