PratoMiMuovo

Ipotesi di Specifica Tecnica Architetturale e Funzionale

Sistema di Smart Mobility per la città di Prato

Versione 1.0 — Aprile 2026

Progetto	#PratoMiMuovo
Tipologia	Progetto di Innovazione per la Mobilità Urbana
Città	Prato (PO) — Toscana, Italia
Autore	Matteo Tempestini
Stato	Ipotesi di Specifica Tecnica
Data	Aprile 2026

Indice

1. Executive Summary

#PratoMiMuovo è un progetto di innovazione per la mobilità urbana della città di Prato. L'obiettivo è trasformare la gestione del traffico da un modello statico — basato su cicli semaforici a tempo fisso, decisi a priori e indipendenti dalla situazione reale — a un sistema reattivo e intelligente, in grado di prendere decisioni in tempo reale sulla base di dati raccolti da una rete di sensori distribuiti sul territorio.

Il sistema si ispira alla metafora del corpo umano: la città necessita di Occhi (sensori per vedere la realtà), un Cervello (software di intelligenza artificiale per analizzare e decidere) e Muscoli (attuatori per agire sulla realtà stradale). L'architettura tecnologica è progettata su open standard internazionali per garantire indipendenza dai fornitori, interoperabilità tra sistemi e apertura dei dati alla comunità.

Il progetto qui riportato è da intendersi come spunto per un reale progetto urbano da realizzare secondo i protocolli di una pubblica amministrazione.

> L'obiettivo non è eliminare il traffico — che è impossibile — ma eliminare l'inefficienza e lo spreco di tempo causati da una gestione statica e cieca della viabilità.

Obiettivo	Metrica Target
Riduzione tempi medi di attesa ai semafori	−20% nelle ore di punta
Riduzione emissioni PM10 nei canyon urbani	−30% durante episodi critici
Recupero puntualità bus LAM	+25–40 secondi per corsa (−30% ritardo accumulato)
Riduzione incidenti agli incroci critici	Azzeramento impatti laterali da Dilemma Zone
Risparmio energetico illuminazione pubblica	−40% consumo nei tratti con sensori PIR

2. Contesto e Obiettivi

2.1 Situazione attuale

La rete semaforica di Prato opera attualmente con piani a ciclo fisso: le durate delle fasi verdi sono preimpostate in base a rilievi di traffico storici, aggiornati raramente. Questo approccio presenta criticità strutturali: i semafori sono 'ciechi', ovvero non percepiscono la situazione reale in tempo reale. Il risultato è che un conducente può ritrovarsi fermo a un rosso per 45 secondi con l'incrocio completamente vuoto, oppure che un bus LAM in ritardo subisca gli stessi tempi di attesa di un'auto privata.

Sul fronte ambientale, i dati ARPAT registrano regolarmente sforamenti delle soglie di PM10 e NO2 nelle vie a traffico intenso, in particolare nei 'canyon urbani' dove l'edificazione alta impedisce la dispersione degli inquinanti. La dinamica 'Stop & Go' — frena e riparte — è la principale causa di picchi emissivi: un veicolo in accelerazione da fermo emette il triplo degli inquinanti rispetto a un veicolo in marcia costante.

2.2 Visione del progetto

- Città Statica → Città Reattiva: passaggio da decisioni basate sul passato a decisioni basate sul tempo reale
- Sicurezza Attiva: la tecnologia corregge l'errore umano prima che diventi tragedia
- Sostenibilità Integrata: la qualità dell'aria diventa un parametro attivo nella gestione del traffico
- Priorità al Trasporto Pubblico: i bus della LAM guadagnano tempo reale sulle auto private
- Open Standard: nessun vendor lock-in, open data per sviluppatori e ricercatori locali

2.3 Perimetro del progetto

Il progetto copre l'intera rete semaforica della città di Prato, con un deployment progressivo pianificato in 3 fasi: (1) pilota su 5 incroci critici del centro, (2) estensione ai corridoi LAM principali, (3) copertura completa della rete. La presente specifica descrive l'architettura a regime completo.

3. Architettura del Sistema

3.1 Visione d'insieme

Il sistema è organizzato in 6 layer funzionali, ciascuno con responsabilità ben definita e interfacce standardizzate verso i layer adiacenti. La separazione in layer garantisce sostituibilità dei componenti senza impatto sull'intero sistema.

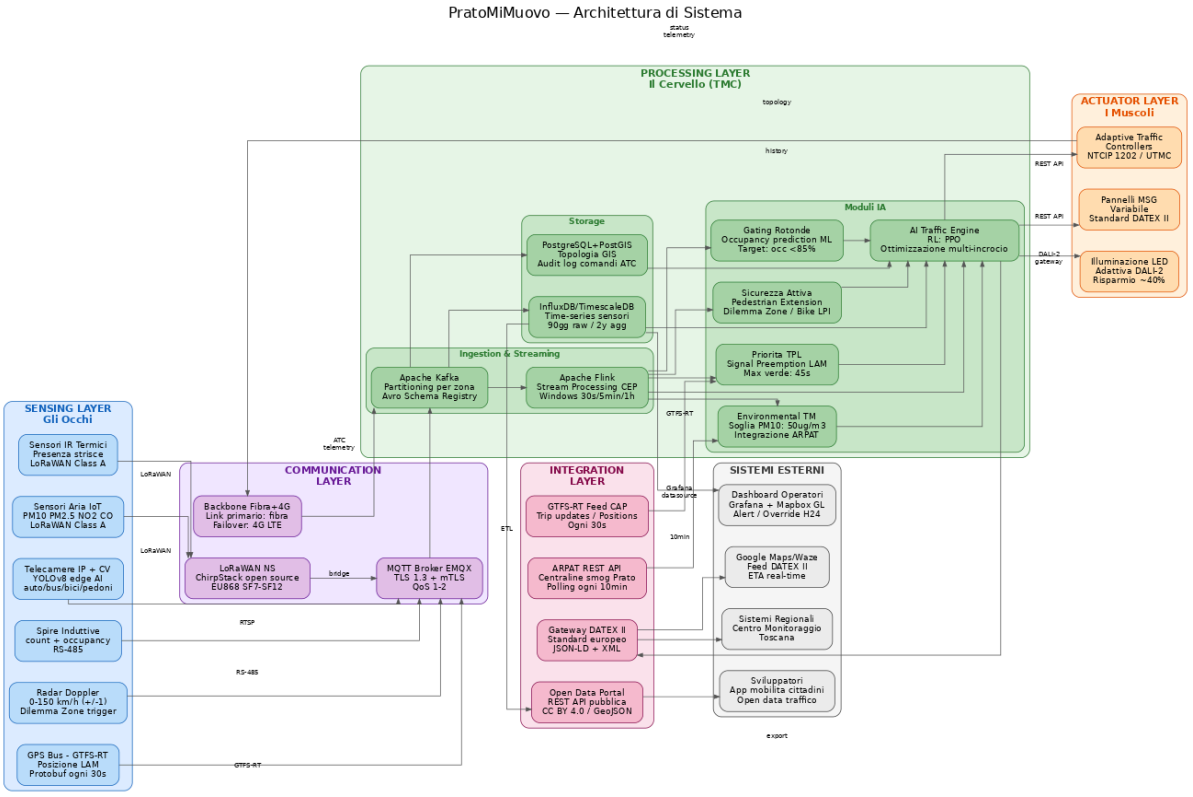

Figura 1 — Architettura del sistema PratoMiMuovo (6 layer)

Layer	Nome	Responsabilità
1	Sensing Layer	Raccolta dati dal campo: sensori di traffico, aria, posizione bus
2	Communication Layer	Trasporto dati: MQTT broker, LoRaWAN, backbone fibra/4G
3	Processing Layer (TMC)	Elaborazione, AI, moduli funzionali, storage time-series
4	Actuator Layer	Esecuzione comandi: semafori, PMV, illuminazione
5	Integration Layer	Interfacce esterne: ARPAT, DATEX II, GTFS-RT, Open Data
6	External Systems	Sistemi terzi: Google Maps, Sistemi Regionali, operatori

3.2 Strato Sensing — Gli Occhi

Il layer sensing comprende tutti i dispositivi fisici che raccolgono informazioni dalla rete stradale. I sensori sono progettati per la raccolta di dati aggregati e anonimizzati: nessun dispositivo legge targhe o identifica persone.

Dispositivo	Tecnologia	Output	Protocollo
Telecamere IP + CV	YOLOv8 on edge device	Conteggio e classificazione veicoli (auto/bus/bici/pedoni)	RTSP → MQTT
Spire Induttive	Loop elettromagnetico sotto asfalto	Conteggio passaggi, occupancy lane	RS-485 → MQTT
Radar Doppler	Radar a microonde 24 GHz	Velocità veicoli in arrivo, 0–150 km/h ±1 km/h	MQTT
Sensori IR Termici	PIR + termocamera	Presenza pedoni su strisce, posizione e stima velocità	LoRaWAN
GPS Bus (GTFS-RT)	GPS on-board + AVM (CAP)	Posizione in tempo reale LAM, trip_id, delay	Protobuf GTFS-RT
Sensori Aria IoT	Elettrochimici + ottici	PM10, PM2.5, NO2, CO, temperatura, umidità	LoRaWAN Class A

3.3 Strato Communication

LoRaWAN Network Server

I sensori a basso consumo (PIR, qualità aria) utilizzano LoRaWAN su banda EU868 con spreading factor SF7–SF12. Il Network Server è ChirpStack (open source), deployato su infrastruttura di proprietà comunale. I gateway LoRaWAN sono posizionati sui pali della pubblica illuminazione. Il duty cycle massimo per ogni sensore è dell'1%, sufficiente per polling ogni 10 minuti.

MQTT Broker

Tutti i flussi dati confluiscono su un MQTT Broker centralizzato (EMQX Enterprise). Le connessioni sono protette da TLS 1.3 con autenticazione mTLS per ogni dispositivo. Il Quality of Service è QoS 1 per dati non critici e QoS 2 per comandi agli attuatori. La gerarchia dei topic segue lo schema: /prato/{zona}/{incrocio}/{device_type}/{metric}.

Backbone Fibra + 4G/5G

I controller semaforici (ATC) comunicano con il TMC tramite backbone in fibra ottica con failover automatico su 4G LTE. La latenza target per i comandi agli ATC è inferiore a 50ms end-to-end. In caso di perdita del link, ogni ATC esegue autonomamente il piano fisso di backup preimpostato.

3.4 Strato Processing — Il Cervello (TMC)

Ingestion & Streaming

Il dato grezzo dei sensori viene ingerito tramite Apache Kafka, con partitioning per zona geografica per garantire locality e bassa latenza di processing. Lo Schema Registry Avro garantisce la compatibilità dei formati nel tempo. La retention è di 7 giorni per i dati raw, utile per debugging e replay in caso di malfunzionamenti.

Apache Flink gestisce lo stream processing in tempo reale con Complex Event Processing (CEP): rileva pattern complessi su sequenze di eventi (es. 'pedone lento + verde in scadenza') in finestre temporali sliding di 30 secondi, 5 minuti e 1 ora.

Storage

Database	Tecnologia	Contenuto	Retention
Time-Series DB	InfluxDB / TimescaleDB	Dati sensori, metriche traffico, qualità aria	90 giorni raw, 2 anni aggregati
Spatial DB	PostgreSQL + PostGIS	Topologia stradale, conf. incroci, audit log comandi ATC	Permanente

3.5 Strato Actuator — I Muscoli

Attuatore	Standard	Interfaccia	Failsafe
Adaptive Traffic Controllers (ATC)	NTCIP 1202 / UTMC	REST API + SNMP	Piano fisso locale autonomo
Pannelli a Messaggio Variabile (PMV)	DATEX II location ref.	REST API	Messaggio statico di default
Illuminazione Adattiva	DALI-2	Gateway DALI-2 → MQTT	Luminosità massima in failsafe

4. Specifiche Funzionali

4.1 AI Traffic Optimization Engine

Il motore centrale di ottimizzazione del traffico usa Reinforcement Learning con algoritmo PPO (Proximal Policy Optimization). Il reward è una funzione multi-obiettivo che minimizza contemporaneamente: ritardo cumulativo dei veicoli, numero di ripartenze da fermo (proxy per emissioni), e code nelle rotonde.

L'ottimizzazione è multi-incrocio: il sistema considera la rete come un grafo e ottimizza il flusso globale, non incrocio per incrocio. I moduli specializzati (Sicurezza, Environmental, Bus Priority, Gating) possono sovrascrivere le decisioni dell'AI Engine con priorità ben definite, descritte nella sezione 4.2.

4.2 Modulo Sicurezza Attiva

Il Modulo Sicurezza Attiva ha priorità assoluta su tutti gli altri moduli. Le sue decisioni non possono essere sovrascritte dall'AI Engine o dal Modulo Bus Priority. L'unico override consentito è quello manuale da Dashboard Operatori H24.

4.2.1 Pedestrian Extension (Scudo Pedoni)

Quando un sensore IR termico rileva presenza sulle strisce pedonali e il modello di velocità stima che il pedone non terminerà l'attraversamento entro il verde pedonale residuo, il sistema estende automaticamente la fase verde pedonale (e mantiene il rosso per i veicoli) fino a liberazione dell'incrocio confermata da sensore.

Parametro	Valore
Velocità pedone 'lento'	< 0.8 m/s (anziani, bambini, persone con disabilità)
Estensione massima concessa	+15 secondi
Early release	Sì — il verde auto parte non appena l'incrocio è libero
Dual sensor requirement	PIR + telecamera (doppia conferma per ridurre falsi positivi)
Priorità	MASSIMA — non bypassabile da altri moduli

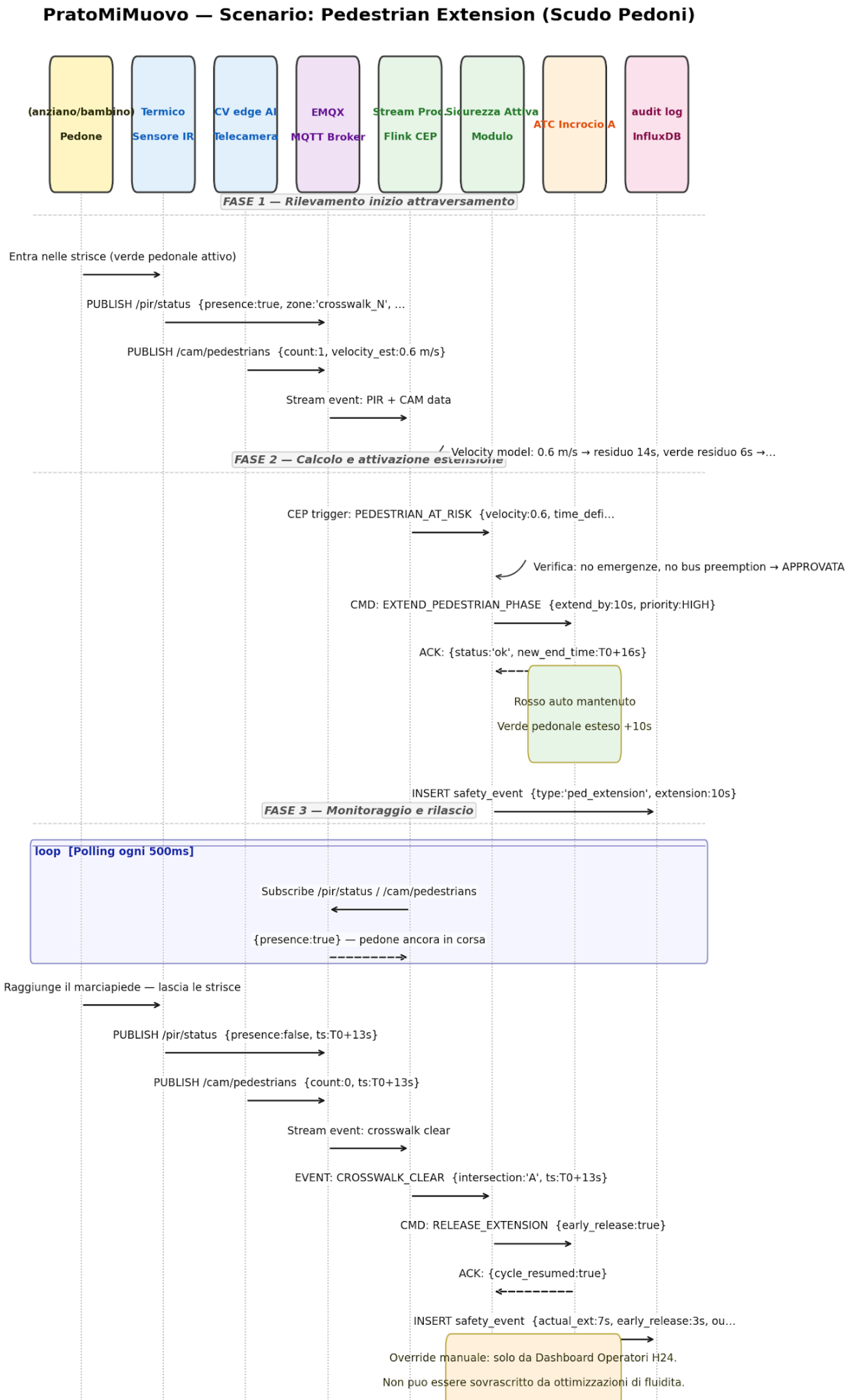
PratoMiMuovo — Scenario: Pedestrian Extension (Scudo Pedoni)
(anziano/bambino)
Pedone
Termico
Sensore IR
CV edge AI
Telecamera
EMQX
MQTT Broker
Stream Proc
Flink CEP
Sicurezza Attiva
Modulo
ATC Incrocio A
audit log
InfluxDB
FASE 1 — Rilevamento inizio attraversamento
Entra nelle strisce (verde pedonale attivo)
PUBLISH /pir/status {presence:true, zone:'crosswalk_N', ...
PUBLISH /cam/pedestrians {count:1, velocity_est:0.6 m/s}
Stream event: PIR + CAM data
Velocity model: 0.6 m/s → residuo 14s, verde residuo 6s →...
FASE 2 — Calcolo e attivazione estensione
CEP trigger: PEDESTRIAN_AT_RISK {velocity:0.6, time_defi...
Verifica: no emergenze, no bus preemption → APPROVATA
CMD: EXTEND_PEDESTRIAN_PHASE {extend_by:10s, priority:HIGH}
ACK: {status:'ok', new_end_time:T0+16s}
Rosso auto mantenuto
Verde pedonale esteso +10s
INSERT safety_event {type:'ped_extension', extension:10s}
FASE 3 — Monitoraggio e rilascio
loop [Polling ogni 500ms]
Subscribe /pir/status / /cam/pedestrians
{presence:true} — pedone ancora in corsa
Raggiunge il marciapiede — lascia le strisce
PUBLISH /pir/status {presence:false, ts:T0+13s}
PUBLISH /cam/pedestrians {count:0, ts:T0+13s}
Stream event: crosswalk clear
EVENT: CROSSWALK_CLEAR {intersection:'A', ts:T0+13s}
CMD: RELEASE_EXTENSION {early_release:true}
ACK: {cycle_resumed:true}
INSERT safety_event {actual_ext:7s, early_release:3s, ou...
Override manuale: solo da Dashboard Operatori H24.
Non puo essere sovrascritto da ottimizzazioni di fluidita.

Figura 2 — Sequence diagram: Pedestrian Extension

4.2.2 Dilemma Zone Protection (Anti-Furbetti del Giallo)

I sensori radar misurano la velocità di ogni veicolo che si avvicina a un incrocio. Se il sistema calcola che un veicolo, con la velocità rilevata, non riuscirà a fermarsi prima della linea di stop prima del rosso, attiva una fase All-Red: tutti i semafori dell'incrocio restano rossi per 2–4 secondi, congelando l'incrocio fino a che il veicolo transitante non lo ha liberato.

Parametro	Valore
Distanza di rilevamento	60–100 metri prima della linea di stop
Algoritmo	Kinematic model: d_stop = v² / (2·a), a = 3.5 m/s² (decel. media)
Durata fase All-Red	2–4 secondi (calibrabile per incrocio)
Falso positivo	Il sistema non interviene se il veicolo può fermarsi normalmente

4.2.3 Bike LPI Head Start

Gli incroci con alta frequenza ciclistica (rilevata da telecamere CV) ricevono una fase LPI (Leading Pedestrian Interval) per biciclette: il verde scatta 4–5 secondi prima per i ciclisti rispetto ai veicoli motorizzati. Questo consente alla bici di portarsi al centro dell'incrocio ed essere ben visibile prima che le auto in svolta si muovano.

4.3 Modulo Environmental Traffic Management

Il Modulo Environmental TM integra i dati di qualità dell'aria — provenienti dalle centraline ARPAT e dai sensori IoT locali — nella logica di controllo semaforica. Quando i valori di PM10 o NO2 superano le soglie definite in una zona, il sistema attiva automaticamente un piano di gating che riduce l'afflusso di veicoli verso quell'area.

Parametro	Valore
Soglia PM10 allerta	50 µg/m³ (valore limite giornaliero UE)
Soglia NO2 allerta	100 µg/m³ (valore limite orario WHO)
Fonte dati primaria	ARPAT REST API (polling ogni 10 minuti)
Fonte dati secondaria	Sensori IoT LoRaWAN in loco (ogni 10 minuti)
Isteresi	2 letture consecutive sotto soglia per rientro allerta
Azione	Riduzione verde verso zona critica: −40% flusso
Comunicazione	PMV + DATEX II → Google Maps / Waze con percorso alternativo
Integrazione con Stop & Go	Onda verde attivata per ridurre ripartenze da fermo

PratoMiMuovo — Scenario: Environmental Traffic Management (Canyon Urbano)

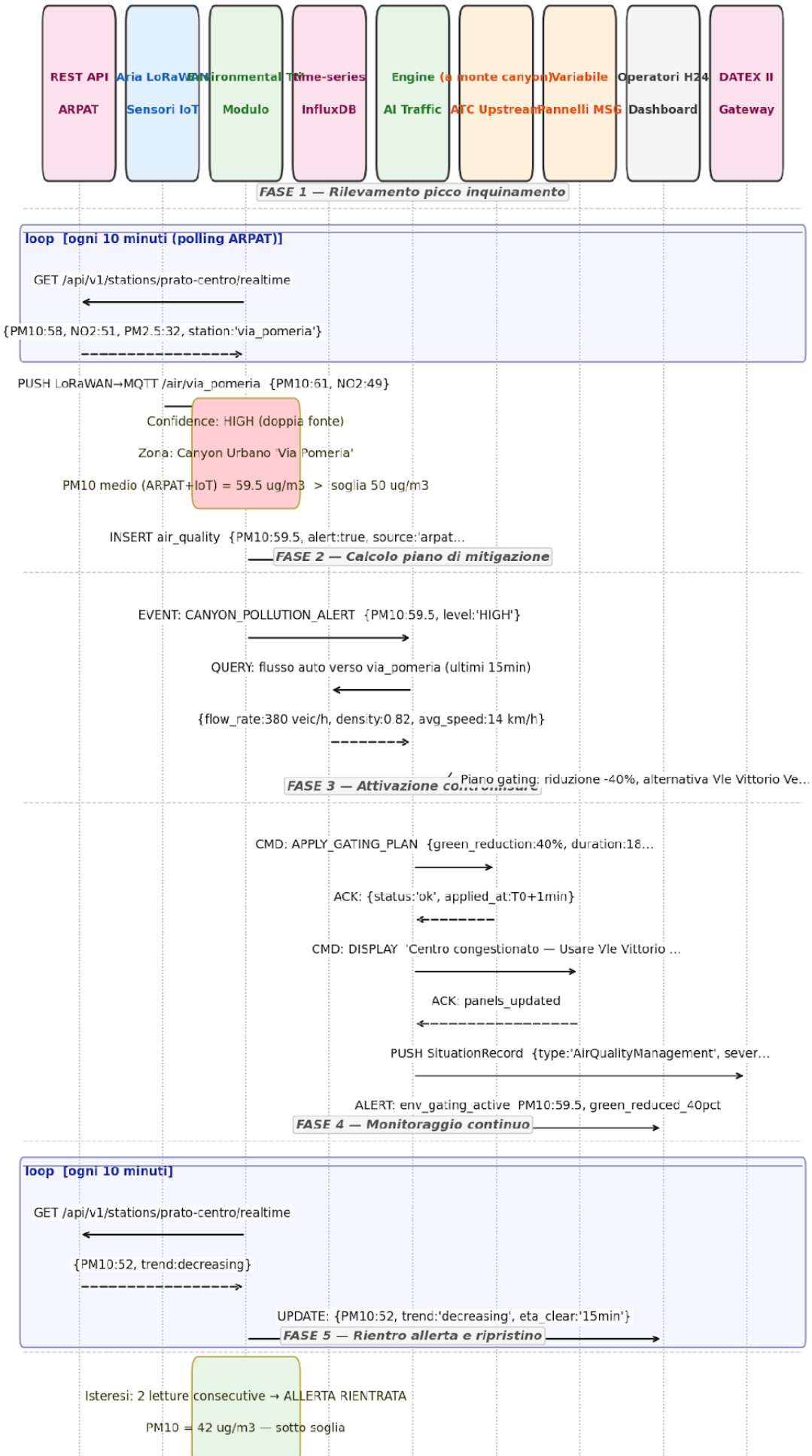

Figura 3 — Sequence diagram: Environmental Traffic Management

4.4 Modulo Priorità TPL — Bus Priority

Il Modulo Priorità TPL riceve i feed GTFS-RT dal CAP (azienda trasporti di Prato) e calcola in tempo reale la posizione e il ritardo di ogni bus LAM. Quando un bus supera la soglia di ritardo e si trova entro la finestra di preemption, il sistema richiede al Modulo Sicurezza Attiva il permesso di attivare la preemption semaforica.

Parametro	Valore
Soglia ritardo per preemption	> 120 secondi (2 minuti)
Finestra di attivazione	200 metri prima dell'incrocio
Verde esteso massimo	45 secondi
Look-ahead	2 incroci (coordinamento corridoio verde)
Arbiter sicurezza	Il Modulo Sicurezza Attiva ha veto assoluto
Preemption condizionata	Se pedoni attivi → attende clearance strisce pedonali
Max preemption per incrocio	1 bus simultaneamente
Update GTFS-RT dopo preemption	Aggiornamento delay stimato inviato al backend CAP

PratoMiMuovo — Scenario: Bus Priority / Signal Preemption (LAM)

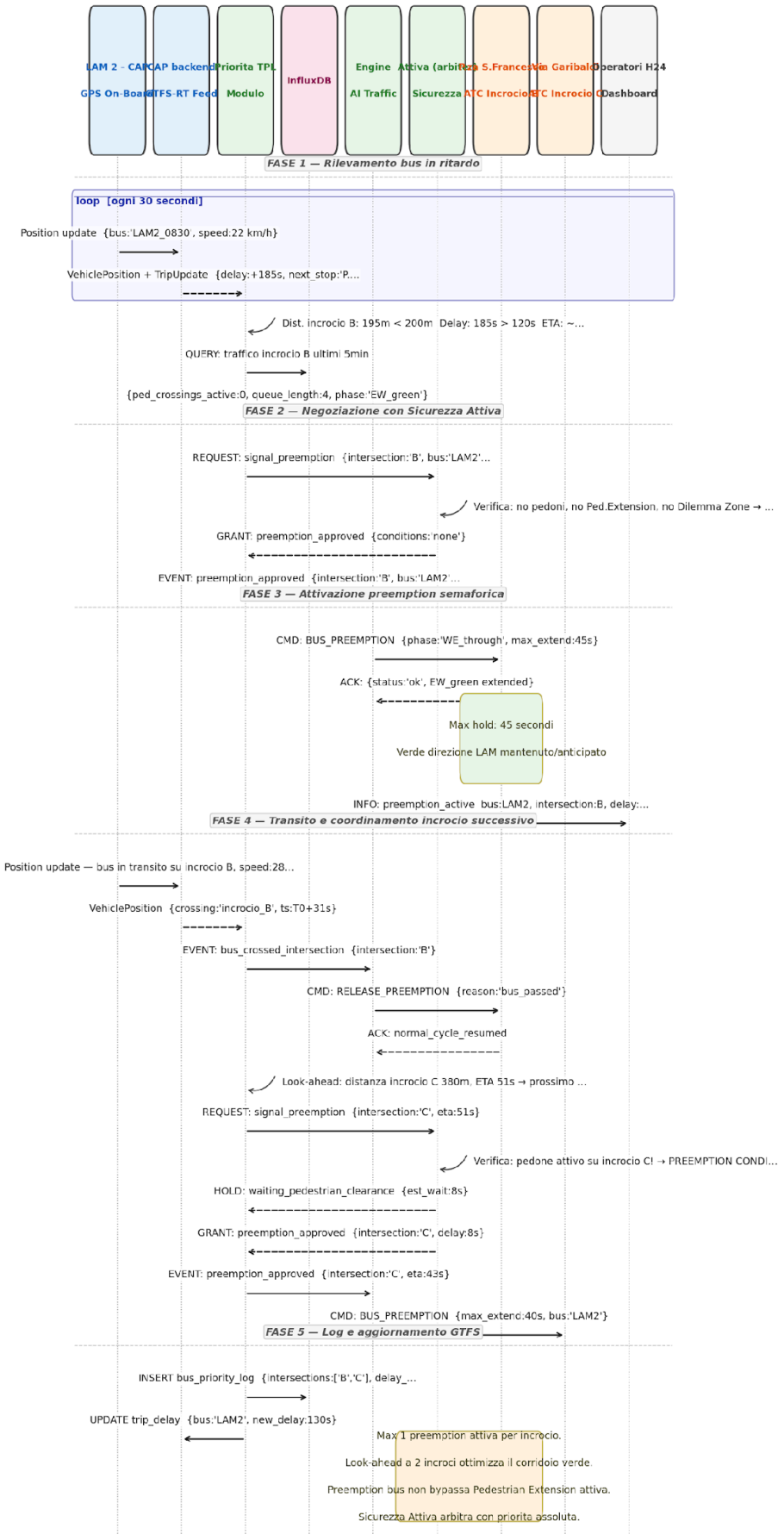

Figura 4 — Sequence diagram: Bus Priority / Signal Preemption

4.5 Modulo Gating Rotonde

Le principali rotonde di Prato (es. Piazza San Marco, Piazza Mercato Nuovo) tendono a saturarsi nei periodi di punta, creando situazioni di gridlock che si propagano a ritroso sulle strade afferenti. Il Modulo Gating Rotonde previene questo scenario intercettando il traffico a monte, prima che le auto entrino nella rotonda satura.

Parametro	Valore
Sensore di occupancy rotonda	Spire induttive + telecamere CV
Soglia di attivazione gating	Occupancy > 85%
Meccanismo	Riduzione verde semafori upstream verso la rotonda
Vantaggio per il conducente	30s di attesa al semaforo vs. 10+ minuti fermi in rotonda
Comunicazione PMV	'Rotonda satura — Usare percorso alternativo [nome]'

5. Specifiche Non Funzionali

5.1 Latenza e Tempo di Risposta

Scenario	Latenza Target	Latenza Max Accettabile
Pedestrian Extension (comando ATC)	< 200ms end-to-end	500ms
Dilemma Zone Protection (All-Red)	< 100ms da rilevamento radar	200ms
Bus Preemption (comando ATC)	< 500ms da trigger	1 secondo
Environmental gating (riduzione verde)	< 60 secondi da superamento soglia	3 minuti
Aggiornamento dashboard operatori	< 5 secondi	30 secondi
Feed DATEX II verso navigatori	< 2 minuti da cambio situazione	5 minuti

5.2 Disponibilità e Resilienza

- Disponibilità target sistema TMC: 99.5% (downtime massimo ~44 ore/anno)
- Ogni ATC opera autonomamente con piano fisso in caso di perdita connessione TMC
- Il Modulo Sicurezza Attiva è l'ultimo a cedere: mantiene le funzioni salvavita anche in degraded mode
- Kafka: replica factor 3, nessun single point of failure nel processing
- InfluxDB / TimescaleDB: backup incrementale ogni 15 minuti, replica su nodo secondario
- Failover 4G automatico entro 30 secondi su link fibra primario

5.3 Conformità Privacy e GDPR

Privacy by Design e Privacy by Default (GDPR Art. 25): il sistema è progettato per non raccogliere dati personali. Le telecamere eseguono il riconoscimento oggetti sull'edge device e trasmettono esclusivamente conteggi aggregati anonimi. Nessuna immagine, volto, targa o dato identificativo viene trasmesso, archiviato o analizzato al di fuori dell'edge processor. Il sistema è conforme al Regolamento (UE) 2016/679 (GDPR) per design.

5.3.1 Base Giuridica del Trattamento

Ai sensi dell'Art. 6 GDPR, il trattamento dei dati tecnici aggregati prodotti dal sistema si fonda sul legittimo interesse pubblico (Art. 6 comma 1 lettera e) — esercizio di pubblici poteri — e sull'adempimento di obblighi derivanti dalla normativa europea ITS (Direttiva 2010/40/UE e atti delegati). Poiché il sistema è progettato per non trattare dati personali, la maggior parte del trattamento non ricade sotto l'ambito di applicazione GDPR.

5.3.2 Registro dei Trattamenti (Art. 30 GDPR)

Il Comune di Prato, in qualità di Titolare del Trattamento, mantiene il Registro ex Art. 30 per i trattamenti residuali del sistema PratoMiMuovo. Le attività di trattamento identificate sono:

Categoria Dato	Raccolta	Trasmissione	Conservazione	Base Giuridica
Immagini telecamere (raw)	Edge device locale — elaborazione real-time	NON trasmesse — elaborazione locale	NON conservate — cancellazione immediata dopo inferenza	N/A — non esce dall'edge
Conteggio veicoli per tipo	Edge device — solo aggregati	Solo valori numerici anonimi via MQTT	90 giorni raw / 2 anni aggregati su InfluxDB	Art. 6(1)(e) — interesse pubblico
Velocità veicoli (radar)	Valore numerico istantaneo	Solo se sopra soglia Dilemma Zone (log evento)	Log eventi per 30 giorni su TSDB	Art. 6(1)(e) — sicurezza stradale
Posizione bus LAM (GPS)	GPS on-board CAP / feed GTFS-RT	Feed GTFS-RT: trip_id anonimo + coordinate	7 giorni su TSDB (trip history)	Art. 6(1)(e) — TPL / Direttiva 2010/40/UE
Qualità aria (PM10, NO2, CO)	Sensore IoT — valori fisici	Valore numerico + timestamp + location	2 anni aggregati / 5 anni per ARPAT	Art. 6(1)(e) — D.Lgs. 155/2010
Audit log comandi ATC	PostgreSQL append-only — azioni operatori	Non trasmesso — solo su DB interno	5 anni (obblighi normativi PA)	Art. 6(1)(c) — obbligo legale PA

5.3.3 Valutazione d'Impatto (DPIA — Art. 35 GDPR)

Il sistema PratoMiMuovo non rientra nelle categorie per cui la DPIA è obbligatoria ai sensi dell'Art. 35 GDPR, poiché: (a) non esegue profilazione sistematica di persone fisiche; (b) non tratta categorie particolari di dati (Art. 9); (c) non effettua sorveglianza sistematica di aree pubbliche in senso proprio — le immagini non lasciano mai l'edge device. Tuttavia, per trasparenza e best practice, è prevista una pre-DPIA volontaria prima del deployment della fase telecamere (Fase 2), con consultazione del Garante se ritenuto opportuno.

> Misura tecnica chiave per la DPIA: l'edge device esegue inferenza YOLOv8 su frame video e distrugge il frame subito dopo. L'output è esclusivamente un contatore (es. {car:3, bus:1, bike:2, ped:0}) senza alcun dato biometrico, di targa o identificativo associato.

5.3.4 Diritti degli Interessati (Artt. 15–22 GDPR)

Poiché il sistema non associa dati a persone fisiche identificabili, i diritti di accesso, rettifica, cancellazione e portabilità (Artt. 15–20) non sono esercitabili in senso tecnico sulle serie storiche di traffico, che sono dati aggregati anonimi. Il Comune pubblica comunque un'Informativa Privacy cittadini ai sensi dell'Art. 13 GDPR, disponibile online e su pannelli informativi nei pressi degli incroci monitorati, che specifica:

- Quali dati NON sono raccolti: immagini, targhe, volti, dati biometrici
- Quali dati sono raccolti: conteggi aggregati di flusso veicolare per categoria
- Chi è il Titolare del Trattamento: Comune di Prato — Ufficio Mobilità
- Chi è il DPO (Data Protection Officer) designato ex Art. 37 GDPR

- Come esercitare i diritti residuali: email DPO, tempi di risposta (max 30 giorni ex Art. 12)

5.3.5 Data Protection Officer (Art. 37 GDPR)

Il Comune di Prato ha l'obbligo di designare un DPO ai sensi dell'Art. 37(1)(a) GDPR (autorità pubblica). Il DPO deve essere coinvolto fin dalla fase di progettazione di PratoMiMuovo (Art. 38) per validare le scelte architetturali in termini di privacy. Il DPO deve ricevere notifica dei seguenti eventi operativi: deployment di nuovi sensori, variazioni nei periodi di retention, eventuali data breach (notifica entro 72h ex Art. 33), e richieste di accesso ai dati da parte di soggetti terzi (forze dell'ordine, ecc.).

5.4 Conformità Cybersecurity

5.4.1 Inquadramento Normativo

Il sistema PratoMiMuovo gestisce infrastrutture critiche per la mobilità urbana. Il framework normativo di riferimento è composto da: Direttiva NIS2 (UE 2022/2555), recepita in Italia con D.Lgs. 138/2024, che classifica i sistemi ITS comunali come soggetti importanti nel settore trasporti; ISO/IEC 27001:2022 per il sistema di gestione della sicurezza delle informazioni (ISMS); IEC 62443 per la cybersecurity dei sistemi di controllo industriale e ITS; NIST Cybersecurity Framework 2.0 come riferimento metodologico.

Classificazione NIS2: il Comune di Prato come gestore di infrastrutture ITS urbane rientra nel perimetro NIS2 (Allegato II, settore trasporti — infrastrutture stradali). Obbligo di registrazione ad ACN (Agenzia per la Cybersicurezza Nazionale) e notifica degli incidenti significativi entro 24h (early warning) / 72h (notifica completa).

5.4.2 Requisiti NIS2 (D.Lgs. 138/2024)

Obbligo NIS2	Articolo	Implementazione in PratoMiMuovo
Misure di gestione del rischio cyber	Art. 21	Risk assessment annuale ISMS, vulnerability scanning trimestrale, patch management documentato per tutti i componenti (Kafka, EMQX, OS)
Sicurezza della supply chain	Art. 21(2)(d)	Requisiti security nei capitolati di gara per ATC, sensori e gateway. Verifica certificazioni fornitori (ISO 27001 o equivalente)
Crittografia e gestione chiavi	Art. 21(2)(h)	TLS 1.3 obbligatorio su tutti i canali. PKI interna per certificati mTLS dispositivi IoT. Rotazione chiavi annuale
Continuità operativa	Art. 21(2)(c)	RTO 30s per failover 4G. RPO 15min per backup TSDB. Piano di Business Continuity documentato
Notifica incidenti significativi	Art. 23	Procedura documentata: early warning 24h ad ACN, notifica completa 72h, relazione finale 30 giorni
Formazione del personale	Art. 21(2)(g)	Training annuale obbligatorio su cybersecurity per operatori TMC e amministratori di sistema
Autenticazione multi-fattore	Art. 21(2)(j)	MFA obbligatorio per accesso dashboard operatori H24 e per accesso amministrativo ai server TMC

5.4.3 IEC 62443 — Sicurezza Sistemi di Controllo Industriale / ITS

La norma IEC 62443 (Industrial Automation and Control Systems Security) è applicata alla componente di controllo semaforico (ATC — Adaptive Traffic Controller), che costituisce il sottosistema di Operational Technology (OT) del progetto. Il Security Level target per il sistema ATC è SL-2 (protezione contro attaccanti con risorse moderate e motivazione specifica).

Requisito IEC 62443	Security Level	Implementazione
Segmentazione di rete OT/IT	SL-2 (SR 5.1)	Rete ATC isolata da rete IT TMC tramite firewall industriale (es. Fortinet o equivalente). DMZ dedicata per interfaccia REST API ATC
Controllo accessi ai dispositivi di campo	SL-2 (SR 1.1)	Accesso SSH ai gateway solo da IP TMC autorizzati. Autenticazione basata su certificato. Nessun accesso diretto da rete pubblica
Integrità dei comandi semaforici	SL-2 (SR 3.1)	Firma digitale su tutti i comandi CMD trasmessi agli ATC. Verifica integrità lato ATC prima dell'esecuzione
Failsafe e risposta ad anomalie	SL-2 (SR 6.2)	Piano fisso locale su ogni ATC. Ripristino automatico entro 30s da perdita connessione TMC. Watchdog hardware indipendente
Audit trail dei comandi OT	SL-2 (SR 2.8)	Log append-only su PostgreSQL di tutti i comandi inviati agli ATC: timestamp, comando, operatore/sistema sorgente, risposta ATC
Patch e vulnerability management	SL-2 (SR 7.6)	Finestra di manutenzione notturna (02:00–04:00) per aggiornamenti firmware ATC. Test su ambiente staging prima del deploy in produzione

5.4.4 Architettura di Sicurezza — Requisiti Implementativi

Layer	Componente	Requisito di Sicurezza
Sensing Layer	Sensori IoT / Gateway LoRaWAN	mTLS per ogni dispositivo — certificato X.509 univoco per device. Join OTAA LoRaWAN con AppKey a 128 bit AES. Disabilitazione ABP (Activation By Personalization)
Communication Layer	MQTT Broker EMQX	TLS 1.3 obbligatorio. ACL per topic: ogni dispositivo pubblica solo sui propri topic /prato/{zone}/{device}/#. Audit log di autenticazione attivato
Processing Layer	Apache Kafka	Autenticazione SASL/SCRAM-SHA-512 tra producer e broker. Cifratura a riposo dei topic contenenti dati operativi. Network policy Kubernetes: solo pod autorizzati accedono al broker
Processing Layer	TMC Server / API	Zero Trust: no implicit trust. Ogni chiamata API autenticata con JWT + mTLS. Rate limiting per prevenire DoS. WAF (Web Application Firewall) davanti alle API REST pubbliche
Actuator Layer	ATC — Controller Semaforici	Rete OT segregata (IEC 62443). Firma digitale comandi. Piano fisso locale come failsafe. Watchdog hardware
Integration Layer	ARPAT API / GTFS-RT / DATEX II	Validazione schema di tutti i feed in ingresso. Sandbox di elaborazione per feed esterni. Timeout e circuit breaker per API esterne
Dashboard / Operatori	Grafana + Mapbox GL	MFA obbligatorio (TOTP o FIDO2). RBAC: 3 ruoli (Operatore / Supervisore / Amministratore). Session timeout 30 minuti. IP allowlist per accesso amministrativo

5.4.5 Gestione Vulnerabilità e Penetration Testing

Il piano di vulnerability management prevede le seguenti attività ricorrenti:

- Vulnerability scanning automatico (es. Nessus / OpenVAS) su tutti i componenti TMC — frequenza: settimanale
- Penetration test esterno (VAPT) obbligatorio prima di ogni fase di deployment su rete produzione — frequenza: prima di Fase 1, Fase 2, Fase 3
- Revisione dipendenze software (npm audit, pip-audit, trivy per container) — frequenza: ad ogni build CI/CD
- Red team exercise annuale focalizzato su scenario di attacco al sistema di controllo semaforico
- Responsible disclosure policy pubblicata: canale di segnalazione vulnerabilità per ricercatori di sicurezza esterni

5.4.6 Incident Response — Piano di Risposta agli Incidenti

In conformità con NIS2 Art. 23 e le best practice NIST CSF (Respond/Recover), il piano di Incident Response di PratoMiMuovo definisce le seguenti fasi:

Fase	Azioni	Tempi	Responsabile
Rilevamento (Identify)	Alert automatico da SIEM. Analisi log EMQX, Kafka, ATC. Classificazione severità (P1–P4)	< 15 minuti	NOC / Sistema automatico
Contenimento (Protect)	Isolamento componente compromesso. Attivazione piano fisso su ATC interessati. Blocco credenziali sospette	< 30 minuti	Amministratore TMC
Notifica Early Warning	Notifica ad ACN (Agenzia Cybersicurezza Nazionale) per incidenti significativi	< 24 ore	CISO / DPO Comune
Notifica Completa	Rapporto dettagliato ad ACN. Eventuale comunicazione al Garante se coinvolti dati personali (GDPR Art. 33)	< 72 ore	CISO Comune
Eradicazione e Ripristino (Recover)	Patch / remediation. Restore da backup validato. Test regressione. Rientro in produzione	< 4 ore (RTO)	Team Tecnico
Post-Incident Review	Root cause analysis. Aggiornamento ISMS. Lessons learned. Rapporto finale ad ACN	< 30 giorni	CISO + Team Tecnico

6. Standard e Protocolli

La scelta degli open standard è una decisione strategica fondamentale: il Comune non deve diventare ostaggio di un singolo fornitore. Tutti i protocolli adottati sono standard internazionali aperti, che garantiscono la possibilità di sostituire qualsiasi componente senza dover rifare l'intera infrastruttura.

Standard / Protocollo	Ambito	Perché è stato scelto
DATEX II	Scambio dati traffico	Standard europeo obbligatorio per sistemi ITS. Compatibile con Google Maps, Waze, sistemi regionali Toscana.
GTFS / GTFS-RT	Dati trasporto pubblico	Standard de facto mondiale per TPL. Usato da tutti i principali navigatori.
LoRaWAN (EU868)	Sensori IoT a lungo raggio	Basso consumo, lungo raggio (>1km in area urbana), rete di proprietà comunale a costo operativo zero.
MQTT v5	Messaggistica IoT real-time	Standard OASIS per IoT. Leggero, veloce, QoS configurabile.
NTCIP 1202	Controller semaforici	Standard NEMA/AASHTO per ATC. Supportato da tutti i principali produttori.
INSPIRE / OGC SOS	Dati ambientali	Standard europeo per dati ARPAT e sensori ambientali.
Apache Kafka (Avro)	Streaming interno	De facto standard per event streaming ad alta scalabilità.
OpenStreetMap / PostGIS	Dati geografici	Open data geografici con supporto GIS completo.

7. Requisiti Hardware di Campo

7.1 Sensori per Incrocio (Configurazione Standard)

Componente	Specifiche Minime	Qtà / Incrocio
Telecamera IP edge-AI	4K, IP67, edge processor NPU ≥ 2 TOPS, YOLOv8 ottimizzato	2–4
Radar Doppler	24 GHz FMCW, range 5–150m, ±1 km/h, IP67	1–2 (corsie critiche)
Sensore IR Termico (PIR)	PIR + termocamera 8x8, LoRaWAN Class A, IP65, batteria 5+ anni	1–2 (strisce pedonali)
Spire Induttive	Doppia spira per corsia, interfaccia RS-485, IP68	2–8 (per corsia)
Gateway LoRaWAN	EU868, 8 canali, IP67, montaggio palo, connessione fibra/4G	1 ogni 10 incroci

7.2 Adaptive Traffic Controller (ATC)

Requisito	Specifica
Standard di comunicazione	NTCIP 1202 v3 obbligatorio, UTMC consigliato
Interfaccia di controllo	REST API documentata (OpenAPI 3.0) o SNMP v3
Piano fisso locale	Storage locale per almeno 8 piani di ciclo di backup
Watchdog	Ripristino automatico piano fisso entro 30s da perdita connessione TMC
Protezione ambientale	IP54 minimo per armadio stradale
Alimentazione	220V AC con UPS integrato (30 min autonomia)

Analisi dei Rischi

Rischio	Probabilità	Impatto	Mitigazione
Vendor lock-in su piattaforma TMC	Media	Alto	Open standard obbligatori nel capitolato. Separazione contrattuale hardware/software.
Cybersecurity: attacco al sistema semaforico	Bassa	Critico	Zero trust, mTLS, audit log. Failsafe fisico ATC indipendente da TMC.
Falso positivo Pedestrian Extension (rallentamento eccessivo)	Media	Medio	Dual sensor (PIR + CV). Limite estensione massima. Monitoraggio KPI su dashboard.
Interferenza LoRaWAN in ambiente urbano	Media	Basso	Adaptive Data Rate, ridondanza gateway. Sensori critici su MQTT via fibra.
Resistenza culturale dei cittadini (percezione sorveglianza)	Alta	Medio	Comunicazione proattiva: nessuna immagine raccolta, solo conteggi anonimi. Certificazione GDPR.
Mancata integrazione ARPAT (API non disponibile)	Bassa	Basso	Sensori IoT locali come fonte primaria alternativa. ARPAT come fonte secondaria di validazione.

Glossario

Termine	Definizione
ATC	Adaptive Traffic Controller — controller semaforico intelligente
CAP	Centro Autobus Prato — azienda del trasporto pubblico locale
CEP	Complex Event Processing — rilevamento di pattern su stream di eventi in tempo reale
DATEX II	Standard europeo per lo scambio di informazioni sul traffico stradale
Dilemma Zone	Zona in cui un conducente non può né fermarsi né passare in sicurezza al cambio di fase semaforica
GTFS-RT	General Transit Feed Specification Real Time — standard per dati TPL in tempo reale
LAM	Linea Alta Mobilità — linee bus rapide di Prato (LAM 1, LAM 2, ecc.)
LPI	Leading Pedestrian/Cyclist Interval — anticipo del verde per pedoni/ciclisti
LoRaWAN	Long Range Wide Area Network — protocollo IoT a lungo raggio e basso consumo
MQTT	Message Queuing Telemetry Transport — protocollo di messaggistica IoT leggero
NTCIP	National Transportation Communications for ITS Protocol — standard per ATC
PMV	Pannello a Messaggio Variabile — segnaletica elettronica variabile
PPO	Proximal Policy Optimization — algoritmo di Reinforcement Learning
TMC	Traffic Management Center — centro di controllo del traffico
TPL	Trasporto Pubblico Locale