

PETROUTILAJ

Manualul dispozitivului și API-ului telematic

HTTP publish/subscribe, digital twin, GPS, ușă, încuietoare, health și telemetrie flexibilă

Pentru cine este acest manual

Integratorii hardware, dezvoltatorii firmware și administratorii care configurează dispozitive asociate locomotivelor Petrouilaj.

Portal: <https://portal.petroutilaj.ro/>

Document operațional în limba română

MODEL

Un digital twin simplu, tip MQTT

Dispozitivul publică starea efectivă prin HTTP și citește periodic starea dorită. Nu este necesar un broker MQTT sau o conexiune permanentă.

- 1 Administratorul înregistrează dispozitivul pe o locomotivă. Acesta este creat dezactivat și primește un ID plus un secret afișat o singură dată.
- 2 Firmware-ul publică telemetrie, GPS, health și puncte flexibile. Mesajele au ID unic și timestamp de la dispozitiv.
- 3 Firmware-ul citește GET /twin la intervalul indicat de server și compară versiunea dorită cu ultima versiune aplicată.
- 4 Administratorul publică LOCKED sau UNLOCKED din portal. Dispozitivul acționează mecanismul, apoi raportează versiunea aplicată și starea fizică observată.
- 5 Portalul consideră comanda confirmată numai dacă versiunea și starea raportată corespund stării dorite.

Comportament sigur la pornire

Starea dorită inițială este NO_CHANGE, versiunea 0. Activarea accesului API nu generează automat o comandă de închidere sau deschidere.

ADMINISTRARE

Provisionare dezactivată implicit

Administratorul real poate gestiona dispozitivele flotei. Administratorul de test poate folosi același flux exclusiv pe locomotivele etichetate din setul său. Conturile ECM și chiriaș nu pot provisiona ori comanda dispozitive.

- 1 În portal, deschideți Dispozitive IoT → Înregistrează dispozitiv.
- 2 Alegeți locomotiva, denumirea și opțional codul dispozitivului.
- 3 Apăsați Creează dezactivat și salvați ID-ul plus secretul într-un secret store al dispozitivului.
- 4 Configurați URL-ul, acreditarea și ceasul UTC. Verificați local senzorii/actuatorul.
- 5 Administratorul apasă Activează numai după montare și validare. Dezactivarea ulterioară oprește imediat toate endpointurile dispozitivului.

Dispozitivul este creat oprit; secretul este afișat o singură dată după salvare.

STĂRI

Ciclul de viață și rezultatul API

Pagină / zonă	Butoane și controale	Ce faceți și când
DISABLED	Starea inițială sau starea după Dezactivează.	Acreditarea poate exista, dar toate rutele /api/device/v1/* răspund 403 DEVICE_DISABLED. Nu se acceptă date și nu se livrează starea dorită.
ENABLED	Administratorul a apăsă Activează.	Dispozitivul poate publica telemetrie/health/date și poate citi twin-ul. Comenzile LOCKED/UNLOCKED pot fi publicate din portal.
REVOKED	Administratorul a dezactivat și apoi a apăsă Revocă.	Secretul este șters. Autentificarea răspunde 401 și dispozitivul nu poate fi reactivat; trebuie provisionat unul nou.
Rotire secret	Rotește secretul în pagina de administrare.	Secretul anterior devine invalid imediat. Noul secret este afișat o singură dată și trebuie instalat pe dispozitiv înaintea următoarei cereri.

Activare controlată

Întrucât dispozitivul poate trimite locația și poate acționa încuietoearea, nu automatizați activarea la creare. Folosiți verificarea administrativă explicită.

AUTENTIFICARE

Antet Device pentru fiecare cerere

URL de bază: <https://portal.petroutilaj.ro/api/device/v1>. Nu trimiteți secretul în URL, query string, topic sau payload.

```
Authorization: Device DEVICE_ID.DEVICE_SECRET
Accept: application/json
Content-Type: application/json          # numai pentru POST
```

- ID-ul este UUID-ul primit la provisionare; secretul este tokenul afișat o singură dată.
- În baza de date este păstrată numai amprenta SHA-256 a secretului.
- Folosiți TLS și nu dezactivați verificarea certificatului serverului.
- Păstrați secretul într-o zonă protejată a dispozitivului. Nu îl includeți în loguri, dump-uri sau capturi.
- La 401 opriți retry-ul rapid și semnalați lipsa acreditării; la 403 dispozitivul este dezactivat administrativ.

ENDPOINTURI

Contractul HTTP_TWIN_V1

Metodă și adresă	Rol	Scop
GET /api/device/v1/twin	dispozitiv ← portal	Citește starea dorită LOCKED/UNLOCKED, versiunea, starea raportată și intervalul recomandat de polling.
POST /api/device/v1/telemetry	dispozitiv → portal	Publică starea ușii, starea încuietorii, versiunea dorită aplicată și/sau GPS.
POST /api/device/v1/health	dispozitiv → portal	Publică heartbeat, firmware, semnal, tensiune, temperatură, uptime, alimentare și eroare.
POST /api/device/v1/data	dispozitiv → portal	Publică un topic și un payload JSON arbitrar pentru alte puncte de telemetrie.

- Toate răspunsurile includ JSON și Cache-Control: no-store.
- Cererile POST sunt idempotente prin messageId per dispozitiv.
- Timpul este ISO 8601 UTC, de exemplu 2026-08-27T12:34:56.000Z.
- Dimensiune maximă: 16 KB pentru telemetry/health și 32 KB pentru data.

SUBSCRIBE

GET /twin și starea dorită

```
GET /api/device/v1/twin HTTP/1.1
Host: portal.petroutilaj.ro
Authorization: Device DEVICE_ID.DEVICE_SECRET
Accept: application/json
```

```
{
  "accepted": true,
  "deviceId": "DEVICE_ID",
  "vehicleId": "VEHICLE_ID",
  "protocolVersion": "HTTP_TWIN_V1",
  "serverTime": "2026-08-27T12:35:01.000Z",
  "nextPollSeconds": 15,
  "desired": {
    "lockState": "LOCKED",
    "version": 12,
    "changedAt": "2026-08-27T12:34:58.000Z"
  },
  "reported": {
    "doorState": "CLOSED",
    "lockState": "UNLOCKED",
    "desiredVersionApplied": 11,
    "telemetryAt": "2026-08-27T12:34:50.000Z"
  },
  "commandPending": true
}
```

Polling

Respectați nextPollSeconds (în prezent 15 s). Adăugați jitter și backoff exponențial la 5xx/rețea pentru a evita sincronizarea tuturor dispozitivelor.

PUBLISH

POST /telemetry pentru ușa, încuietoare și GPS

O cerere poate conține unul sau mai multe câmpuri. Cel puțin o stare, versiune aplicată sau poziție GPS este obligatorie.

```
POST /api/device/v1/telemetry HTTP/1.1
Authorization: Device DEVICE_ID.DEVICE_SECRET
Content-Type: application/json

{
  "messageId": "boot42-telemetry-000187",
  "timestamp": "2026-08-27T12:35:10.000Z",
  "doorState": "CLOSED",
  "lockState": "LOCKED",
  "desiredVersionApplied": 12,
  "gps": {
    "latitude": 44.94621,
    "longitude": 26.01234,
    "accuracyMeters": 8.5,
    "speedKph": 0,
    "headingDegrees": 181.2
  }
}
```

- doorState: OPEN, CLOSED sau UNKNOWN.
- lockState: LOCKED, UNLOCKED, JAMMED sau UNKNOWN.
- desiredVersionApplied: număr întreg între 0 și versiunea dorită curentă.
- GPS-ul valid creează și un eveniment de locație TELEMATICS în istoricul locomotivei.
- Nu raportați LOCKED doar pentru că a fost trimisă comanda; folosiți feedback-ul fizic al actuatorului/senzorului.

COMANDĂ

Aplicarea sigură LOCKED / UNLOCKED

Starea dorită este schimbată de administrator în portal. Firmware-ul nu o setează și nu presupune că o comandă a reușit.

- 1 Citiți twin-ul și comparați `desired.version` cu versiunea memorată local.
- 2 Dacă `desired.lockState` este `NO_CHANGE` sau versiunea a fost deja procesată, nu acționați din nou.
- 3 Verificați interblocările locale: ușă, tensiune, actuator, temperatură, situație de urgență și orice condiție impusă de proiect.
- 4 Acționați mecanismul și citiți feedback-ul fizic. În caz de blocare, raportați `JAMMED` și un `health ERROR`.
- 5 Publicați telemetry cu `lockState` observat și `desiredVersionApplied` egal cu versiunea procesată.
- 6 Păstrați comanda local până la confirmarea răspunsului. Repetarea aceluiași mesaj este sigură și nu dublează evenimentul.

Confirmare în portal

Comanda rămâne «Așteaptă confirmarea» dacă versiunea raportată este mai veche sau dacă `lockState` nu coincide cu `desired.lockState`. `JAMMED` nu este afișat ca succes.

HEALTH

POST /health și heartbeat

```
POST /api/device/v1/health HTTP/1.1
Authorization: Device DEVICE_ID.DEVICE_SECRET
Content-Type: application/json
```

```
{
  "messageId": "boot42-health-000063",
  "timestamp": "2026-08-27T12:35:15.000Z",
  "status": "OK",
  "firmwareVersion": "1.4.2",
  "signalDbm": -71,
  "batteryVolts": 24.6,
  "temperatureC": 41.2,
  "uptimeSeconds": 9283,
  "powerSource": "VEHICLE",
  "errorCode": null,
  "errorMessage": null
}
```

- status: OK, DEGRADED, ERROR sau UNKNOWN.
- powerSource: MAINS, BATTERY, VEHICLE sau UNKNOWN.
- Câmpurile numerice sunt opționale; uptimeSeconds trebuie să fie întreg pozitiv.
- La eroare folosiți un cod stabil și o descriere scurtă, fără secrete sau date personale.
- Recomandare: heartbeat la 60 s în exploatare, cu interval mai mare numai dacă autonomia o cere; twin-ul rămâne la nextPollSeconds.

TELEMETRIE EXTENSIBILĂ

Snapshot motor LDE 2100 / DA681

Endpointul primește semnale suplimentare fără migrarea schemei. Platforma descoperă automat numerele, stările și unitățile și le afișează în istoricul locomotivei.

```
POST /api/device/v1/data HTTP/1.1
Authorization: Device DEVICE_ID.DEVICE_SECRET
Content-Type: application/json

{
  "messageId": "boot42-custom-000901",
  "timestamp": "2026-09-03T12:35:20.000Z",
  "topic": "engine.data.snapshot",
  "payload": {
    "Turatie MD": 750,
    "coolantTemperatureC": 82.3,
    "oilTemperatureC": 74.1,
    "oilPressure": 4.7,
    "airPressure": 8.2,
    "units": {
      "Turatie MD": "rpm",
      "coolantTemperatureC": "°C",
      "oilTemperatureC": "°C",
      "oilPressure": "bar",
      "airPressure": "bar"
    },
    "sensorQuality": {
      "Turatie MD": "OK",
      "coolantTemperatureC": "OK",
      "oilTemperatureC": "OK",
      "oilPressure": "OK",
      "airPressure": "OPEN_CIRCUIT"
    }
  }
}
```

- Turația este integer direct: valMDspeed=750 produce 750 rpm.
- Temperaturile și presiunile sunt întregi în zecimi în achiziția locală: 823 produce 82.3 °C, iar 47 produce 4.7 bar.
- Împărțirea la 10 se face o singură dată în firmware. Cloudul nu scalează din nou valorile primite.
- Pentru 4–20 mA transmiteți calitatea canalului: OK, UNDER_RANGE, OVER_RANGE, OPEN_CIRCUIT, SHORT_CIRCUIT, OUT_OF_RANGE sau UNAVAILABLE.
- Pentru turație se folosesc OK, OUT_OF_RANGE sau UNAVAILABLE; o valoare aflată în domeniu nu poate demonstra singură un defect de senzor.
- topic are 1–120 caractere și începe alfanumeric; sunt permise litere, cifre, punct, underscore, slash și cratimă.
- payload poate fi obiect, listă, text, număr, boolean sau null; întregul mesaj trebuie să rămână sub 32 KB.
- Nu duplicați GPS-ul ori starea încuietorii aici; endpointurile dedicate actualizează digital twin-ul și istoricul operațional.
- Portalul agregă mesajele după locomotivă și recomandă automat grafice linie, bare, circulare sau evenimente.

INTEGRARE FIRMWARE

Helper C gata de copiat

Fișierele `examples/engine_snapshot.h` și `examples/engine_snapshot.c` serializează exact contractul de mai sus, fără suport printf floating-point.

```
pu_engine_snapshot_t snapshot = {
    .engine_speed_rpm = valMDspeed,
    .coolant_temp_x10 = valMDtempApa,
    .oil_temp_x10 = valMDtempUlei,
    .oil_pressure_x10 = valMDpresUlei,
    .air_pressure_x10 = valMDpresAerAlim,
    .speed_quality = PU_SENSOR_OK,
    .coolant_quality = PU_SENSOR_OK,
    .oil_temp_quality = PU_SENSOR_OK,
    .oil_pressure_quality = PU_SENSOR_OK,
    .air_pressure_quality = PU_SENSOR_OPEN_CIRCUIT
};

pu_err_t result = pu_engine_snapshot_publish(&snapshot);
if (result == PU_ERR_QUEUE_FULL) {
    /* fault local; reincearca dupa golirea cozii */
}
```

- Apelați helperul dintr-un task, nu din ISR sau callbackul ADC/DMA.
- Pragurile electrice pentru defect 4–20 mA aparțin driverului traductorului/modulului și trebuie configurate din fișa tehnică reală.
- Mesajul este persistent și idempotent: la timeout se retransmite același mesaj.
- `PU_ERR_QUEUE_FULL` nu se ignoră și nu justifică pierderea silențioasă a măsurării.
- Testul automat verifică inclusiv 823 -> 82.3, 47 -> 4.7 și -5 -> -0.5.

Separare corectă

Acest snapshot este telemetrie motor. Fișele din arhiva Revizii sunt documente de mentenanță executată și trebuie completate în dosarul ferestrei, cu operator, instrument, regulă și rezultat.

FIABILITATE

messageld, timp, retry și erori

messageld este cheia de idempotență per dispozitiv pentru toate mesajele publicate.

Pagină / zonă	Butoane și controale	Ce faceți și când
200	Mesaj acceptat sau duplicat acceptat.	Când duplicate=true, serverul nu inserează a doua copie. Folosiți twin-ul din răspuns ca stare curentă.
400	Payload, stare, GPS, timestamp sau messageld invalid.	Nu repetați identic la infinit. Corectați datele și generați un ID nou numai pentru un eveniment nou/corectat.
401	DEVICE_AUTHENTICATION_REQUIRED.	Acreditare lipsă/greșită/revocată. Opriti bucla rapidă și cereți reprovisionare sau rotire administrativă.
403	DEVICE_DISABLED.	Dispozitivul este oprit administrativ. Nu publicați și nu încercați să citiți comenzi până la activare.
5xx / rețea	Eroare tranzitorie.	Păstrați același messageld, repetați cu backoff și jitter, apoi continuați coada în ordinea timestamp-ului.

- messageld: 8–128 caractere din A–Z, a–z, 0–9, punct, underscore, două puncte sau cratimă.
- timestamp-ul nu poate fi cu peste 10 minute în viitor și nu poate fi mai vechi de 30 de zile.
- Sincronizați periodic ceasul. Pentru funcționare offline, păstrați evenimentele și ID-urile până la confirmarea 200.

BUCLĂ FIRMWARE

Implementare recomandată

```
la pornire:
  încarcă DEVICE_ID, secretul și ultima versiune procesată
  inițializează senzori, actuator, ceas și coada persistentă

la fiecare 15 secunde (+ jitter):
  GET /twin
  dacă 401: oprește retry rapid; semnalizează reprovisionare
  dacă 403: intră în mod administrativ dezactivat
  dacă desired.version este nouă:
    validează interblocările; acționează; citește feedback-ul
    POST /telemetry cu versiunea aplicată și starea observată

la schimbarea ușii, încuietorii sau GPS-ului:
  adaugă mesaj persistent cu messageId unic; POST /telemetry

periodic:
  POST /health
  golește coada cu același messageId până la răspuns 200
```

Persistență

Memorați ultima versiune procesată și coada de mesaje în memorie nevolatilă. Un restart nu trebuie să reaplice orbește o comandă veche și nici să piardă confirmarea fizică.

VERIFICARE FINALĂ

Checklist înainte de activare

- Dispozitivul este asociat locomotivei și codului corect; secretul nu apare în loguri.
- TLS, DNS și ceasul UTC funcționează; retry-ul folosește backoff și jitter.
- Senzorul ușii distinge OPEN/CLOSED/UNKNOWN și actuatorul distinge LOCKED/UNLOCKED/JAMMED/UNKNOWN.
- Comanda nu este marcată aplicată înainte de feedback-ul fizic; interblocările locale rămân autoritatea de siguranță.
- GPS-ul respectă coordonatele WGS84 și raportează acuratețea; health-ul semnalează lipsa senzorilor sau erorile.
- messageld persistă între retry-uri, iar coada supraviețuiește restartului.
- Testați DISABLED (403), ENABLED (200), rotirea secretului (401 pentru secretul vechi) și REVOKED (401).

PT

Petroutilaj
Portal locomotive

LA

1

Dispozitive IoT

2

Locații feroviare

3

Verificări mentenanță

4

Sarcini mentenanță

Calendar mentenanță

Rapoarte PDF

C

Secretul se afișează numai la creare sau rotire. Dezactivarea oprește imediat toate endpointurile dispozitivului.

DISPOZITIV

Dispozitiv exemplu manual

MANUAL-SCREEN-001

HTTP_TWIN_V1 · 0 mesaje flexibile

LOCOMOTIVĂ

LDE 2100 · LOCAL-1787828455594

92 53 1787828455594

ACCES

● Dezactivat

Endpoint oprit

UȘĂ / ÎNCUIETOARE

Neraportată / Neraportată

—

STARE DORITĂ

Nicio comandă

● Necomandată

versiunea 0

GPS

Neraportat

SĂNĂTATE

● Fără heartbeat

—

ACȚIUNI

Activează

Rotește secretul

Revocă

Integrare HTTP tin publish/subscribe

Administratorul verifică starea, ultima telemetrie, comanda, GPS-ul, health-ul și acțiunile dispozitivului.

SUPPORT

Ce transmiteți pentru diagnostic

Nu transmiteți niciodată secretul dispozitivului.

- Cod dispozitiv, ID dispozitiv și locomotivă asociată.
- Endpoint, metodă, status HTTP, error code JSON și moment UTC.
- messageld, firmwareVersion și ultimele valori fără date sensibile.
- Pașii de reproducere: dezactivat/activat, versiunea dorită, starea fizică și versiunea raportată.
- Contact operațional: mentenanta@petroutilaj.ro.

Separarea responsabilităților

Portalul publică intenția și păstrează trasabilitatea. Firmware-ul și instalația locală trebuie să aplice interblocările, feedback-ul fizic și cerințele de siguranță ale proiectului.