TELEMATICS & REMOTE ACCESS

CZ Mobility IoT Gateway

Secure remote programming, online diagnostics and CAN-to-cloud data for mobile machinery — over 4G, Wi-Fi or Ethernet.

Construction | Agricultural | Material handling | Municipal & utility | Special-purpose vehicles



4G · Wi-Fi · LAN
Flexible uplink options

GPS
Live tracking & geofencing

CANopen → MQTT
Machine data to the cloud

–20…+60 °C
12–24 V DC, metal housing

The **CZ Mobility IoT Gateway** is a compact, rugged telematics and remote-access unit for off-highway and mobile machinery. It links the vehicle's CAN network to service engineers and cloud applications, so controllers, displays and other devices can be reprogrammed over CAN, Ethernet or Wi-Fi, faults diagnosed and machines monitored — without a site visit.

Combined with the **AMP access-management server** and the **Linker** client, the gateway forms a complete, auditable remote-service system: every session is authorised, encrypted over port 443 and logged. In parallel, CANopen data and GPS position are published via encrypted **MQTT** to the RMC cloud or your own private platform.

Remote programming & updates
Program and update controllers, displays and HMIs of any brand over CAN, Ethernet or Wi-Fi — from anywhere, without travelling to the machine.

Online troubleshooting
Read and write live CAN bus data from a web browser. Diagnose and clear faults before a technician is dispatched.

CAN data collection
Dedicated CAN channel with CANopen support for continuous acquisition of machine operating data and status.

MQTT cloud connectivity
Encrypted MQTT 3.1 / 5.0 uplink to the RMC cloud or a customer-specific private cloud and dashboard.

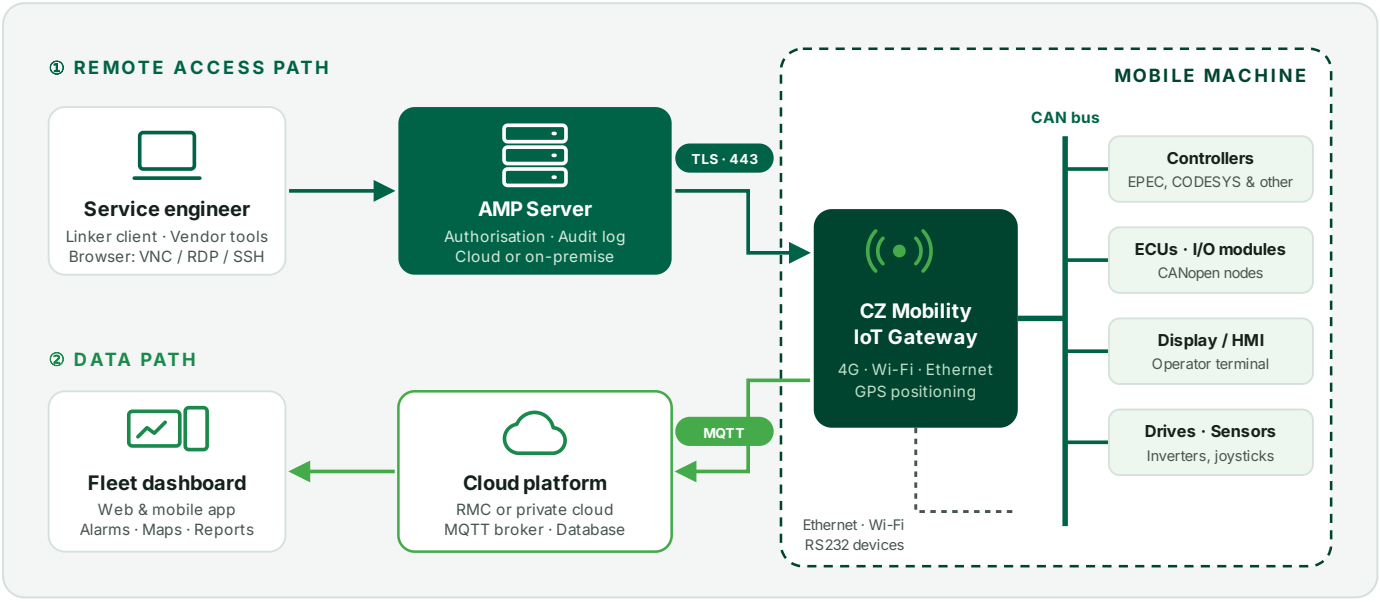
GPS tracking & geofencing
Integrated GPS for live location, trip history playback, geofence alarms and fleet dispatching.

Access management & audit
Zero-trust design aligned with IEC 62443, role-based permissions, operation logs and session screen recording.

HOW IT WORKS

One gateway, two data paths

Remote-access sessions are brokered by the AMP server over an outbound, encrypted connection on port 443 — firewall-friendly, with no inbound connections to the machine. Machine data travels independently via MQTT to the cloud platform.



Remote access

- **2 remote-access channels** for simultaneous sessions to different devices
- **All controller brands** — program, update and diagnose controllers, PLCs, displays/HMIs and drives
- **CAN, Ethernet (LAN), Wi-Fi & RS232** — every on-board interface is reachable through the same secure tunnel
- **CODESYS over CAN** — e.g. remote download to EPEC controllers (CODESYS V2.3)
- **Web access** — browser-based VNC, RDP and SSH, no client install needed
- **Layer 2 networking** — add devices by MAC address
- **Firewall-friendly** — outbound port 443 only; stable cross-border connections

Data collection & cloud

- **1 × CAN bus** dedicated to data acquisition
- **CANopen** protocol support for machine parameters and status
- **Encrypted MQTT 3.1 / 5.0** uplink to the cloud
- **RMC cloud platform** ready; customised private-cloud integration available
- **GPS** position for live tracking, trip history and geofencing
- **Analytics** — dashboards, alarms, work orders and historical trend analysis

01
Remote software deployment
Roll out new controller applications and parameter sets to machines in the field.

02
Remote diagnostics
Connect to a stopped machine, read fault codes live and guide the operator back to work.

03
Fleet monitoring
Track operating hours, load and alarms across the fleet for data-driven maintenance.

04
Location & geofencing
Know where every machine is, replay trajectories and get alerts on unauthorised movement.

OT SECURITY & COMPLIANCE

Full-process control over who reaches your machines

Remote access to a machine controller is a safety-relevant action. The gateway, AMP server and Linker client together enforce authorisation, encryption and traceability for every session.

Secure encryption

Zero-trust architecture; IEC 62443-compliant design. The client–server–gateway chain is protected against man-in-the-middle attacks.

Access control

Fine-grained, role-based authorisation per user, gateway and device channel — grant exactly the access each service partner needs.

Monitoring & audit

Operation logs and session screen recording provide full traceability of who accessed which machine, when and what was changed.

Firewall-friendly communication

Minimal firewall requirements and easy deployment. Each controller brand gets an independent device channel; the gateway has a built-in firewall.

Traceable communication records

Access time, destination, source, duration and resource usage are recorded for every domain, account, gateway and channel.

Tree-based management console

Organise customers, fleets and machines in domains. Drag-and-drop management, query tracing and delegated authorisation.

Automatic port management

Only the ports defined by the device channel are opened during a session; all unused ports stay closed.

Fine-grained permission management

Different permissions per account, supporting many-to-many, one-to-many and many-to-one remote-access scenarios.

No subnet IP conflicts

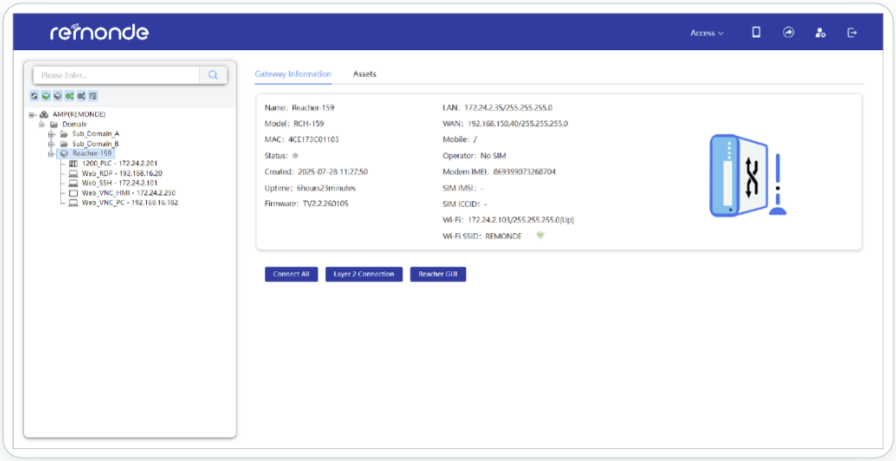
Identical machines can keep the same factory IP scheme — sessions always reach the intended vehicle, never a look-alike.

Man-in-the-middle prevention

The security mechanism formed by client, server and gateway is immune to man-in-the-middle attacks.

No IT expertise required

Service managers administer the whole remote-access system through simple drag-and-drop and query operations.



AMP WEB CONSOLE

Every machine, one console

The domain tree shows each gateway with its status, uptime, firmware, network and SIM information, together with the devices behind it.

Connect All opens every authorised channel at once; **Layer 2 Connection** and the gateway GUI are one click away.

SPECIFICATIONS

Technical data

SYSTEM	
Processor	ARM Cortex, 800 MHz
Operating system	Embedded Linux
Memory	256 MB RAM / 8 GB Flash

ELECTRICAL & WIRED INTERFACES	
Power supply	12–24 V DC
Connector	Automotive-grade sealed connector (power, CAN, RS232, Ethernet)
Ethernet	1 × 10/100 Mbps — LAN, static IP, DHCP
Serial	1 × RS232 (Rx/Tx)
CAN	1 × CAN bus

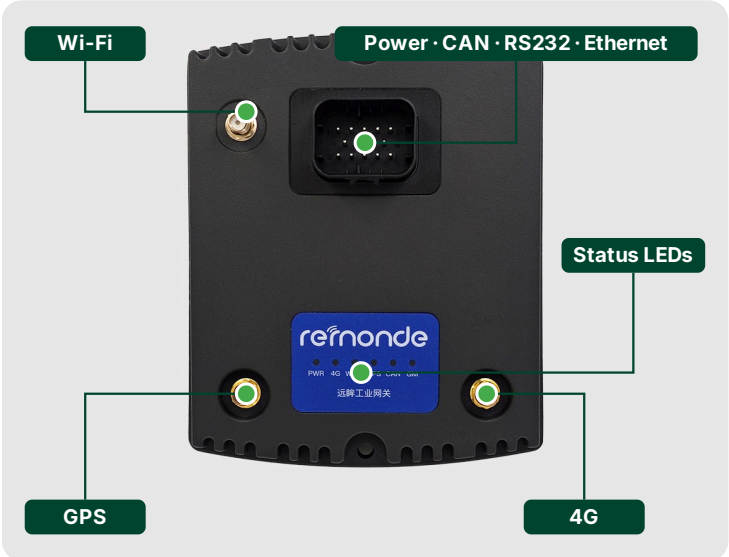
WIRELESS	
Cellular	4G LTE (European band variant available)
Wi-Fi	2.4 / 5.8 GHz dual-band
GNSS	GPS, independent positioning chip
SIM / antennas	1 × Micro-SIM · 3 × SMA (4G, Wi-Fi, GPS)

REMOTE ACCESS	
Channels	2 remote-access channels
Interfaces	CAN, Ethernet (LAN), Wi-Fi, RS232
Devices	Controllers, PLCs, displays/HMIs, drives — all brands; CODESYS V2.3 over CAN (e.g. EPEC)
Web access	VNC / RDP / SSH in browser; Layer 2 via MAC
Connectivity	Outbound, encrypted, port 443

DATA COLLECTION & CLOUD	
Channels	1 × CAN bus
Protocol	CANopen
Cloud protocol	MQTT 3.1 / 5.0, encrypted
Platforms	RMC cloud; customised private cloud available

ENVIRONMENTAL & MECHANICAL	
Operating temp.	−20 °C to +60 °C
Rel. humidity	5 % to 95 %
Housing	Metal casing with cooling fins
Mounting	Bolted, 2 mounting points
Conformity	CE, WEEE

Connections & indicators



Status LEDs

PWR	Power status
4G	Cellular network status
Wi-Fi	Wi-Fi network status
GPS	GPS positioning status
CAN	CAN communication status
GM	Server (AMP) connection status

Micro-SIM slot and reset button are located under the service cover on the rear side.

CZ Mobility
Electrified System Solutions
mehmet.berber@czmobility.com
+90 506 432 69 09
www.czmobility.com