ERICSSON

The always-connected fleet playbook

Meeting uptime, security, and performance targets with 5G Wireless WAN

Overview

Table of Contents

03 The operational reality of managing fleet connectivity

04 Core fleet applications that depend on connectivity

05 The technology behind dependable fleet networking

07 Deployment choices that determine long-term results

08 The leadership checklist for 5G fleet connectivity

Fleet vehicles have become mobile edge environments, and IT teams are now resposible for keeping them secure and operational. Applications inside the vehicles, including edge AI, video, telematics, and location services, have become operational dependencies. Connectivity, therefore, must be treated as critical infrastructure.

When connectivity drops, outages create blind spots that can undermine safety decisions and delay critical video uploads, while also leaving compliance records with gaps to be reconciled. Fleet data demands will continue to rise, especially upstream from vehicle to cloud. 5G is the solution positioned to meet that demand while still giving IT centralized control.

Image courtesy of Getty Images

The operational reality of managing fleet connectivity

Managing connectivity for a mobile fleet is fundamentally different from managing a fixed enterprise network. Vehicles are constantly in motion, crossing coverage zones, switching networks, and operating in environments IT teams don't control. As a result, network conditions constantly fluctuate, making consistent performance difficult to guarantee.

At the same time, fleet IT teams are expected to support these distributed systems without physical access to the vehicles themselves. When something goes wrong, there's no help desk visit or cable to reseat, yet downtime still impacts drivers, dispatchers, customers, and, in some cases, public safety. The pressure to deliver reliable, secure connectivity remains high, even as visibility and hands-on troubleshooting are limited. These constraints translate into several critical network requirements for fleet operations.

Continuity is essential: connections must persist as vehicles move, so workflows aren't interrupted mid-route or mid-task.

Upstream performance is just as important as downstream, since vehicles continuously send telemetry, sensor data, event logs, and video back to central systems.

Security must extend to the vehicle, which often operates in unmanaged environments while accessing sensitive data (e.g., payment, customer, or law enforcement information).

Centralized management is what makes fleet requirements achievable at scale.

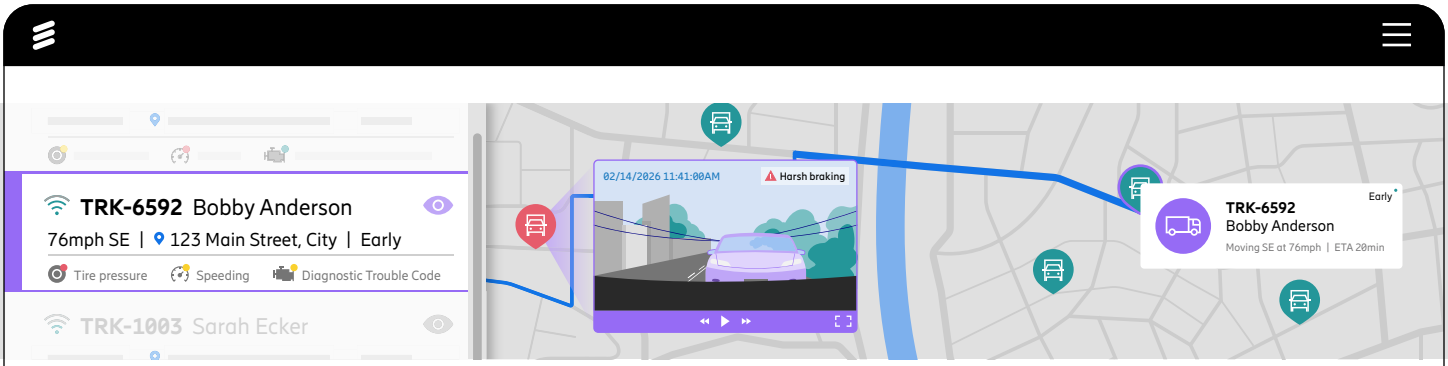
By standardizing configurations, monitoring network health in real time, and resolving issues remotely, IT teams can keep vehicles operational without pulling them off the road. Just as importantly, centralized control creates a consistent foundation on which modern fleet technologies can run reliably.

With that foundation in place, fleets can begin to support a growing range of applications — each with its own performance, reliability, and security demands. Understanding which applications depend on connectivity, and how critical that connectivity is, is the next step in designing a network strategy that keeps fleets moving.

Image courtesy of Getty Images

Core fleet applications that depend on connectivity

Connectivity delivers value only when it reliably supports the applications that keep fleet operations running. For IT teams, the priority is understanding how each workload behaves on the network and designing policies that maintain steady performance as vehicles move through changing coverage.



Telematics for vehicle health and compliance

Telematics go beyond location. This data captures operational signals that help teams manage driver behavior, vehicle health, fuel or energy usage, and compliance. Examples include speeding alerts, harsh braking and rapid acceleration, engine fault codes, battery voltage, fuel consumption, excessive idling, hours-of-service logs, and electronic logging device (ELD) reporting.

The value of telematics depends on continuity. Frequent and timely event reporting provide teams with a reliable record for maintenance planning, safety programs, and compliance documentation. When links degrade, telemetry can arrive late or intermittently, reducing confidence in the data and limiting its usefulness.

From a network standpoint, telematics is an always-on workload that must stay reliable under stress. The upload connection must remain steady and supported by link monitoring and device health so teams can address issues before they become an outage. If IT only learns about a problem after a vehicle drops offline, the disruption has already happened.

Cameras and surveillance for oversight and evidence

Video introduces network traffic patterns that look different from telemetry. Uploads often arrive in bursts and place sudden demand on outbound capacity, especially when multiple clips or streams are involved.

A practical deployment supports two patterns. Immediate transmission is reserved for situations where timeliness matters, whereas routine footage is uploaded through controlled windows and synchronized later. This approach helps control cellular usage costs while preserving readiness, and it works best when the network enforces prioritization so that video does not disrupt telemetry or administrative access.

GPS, AVL, and RTK for higher confidence decisions

Location identification started as "where is the vehicle," but fleets now use it to run daily operations — not just check route compliance. Accurate GPS/AVL data supports trip history and replay, confirms speed and direction, and triggers geofencing alerts when vehicles enter or leave specific areas. When incidents happen, accuracy can also clarify what occurred, down to which lane a vehicle was in. As fleets add more automation, many will need more precise positioning than standard GPS can consistently provide.

Real-time kinematics (RTK) can deliver centimeter-level accuracy with third-party applications, making location data valuable beyond mapping. It can flag unsafe driving patterns such as swerving or harsh braking and provide clearer evidence for accident or citation investigations. In controlled sites such as yards or storage facilities, RTK can support machine-to-machine coordination for tasks such as docking. It raises the bar for connectivity, since precision location needs consistent performance as vehicles travel.

The technology behind dependable fleet networking

A 5G Wireless WAN (WWAN) foundation needs the right coverage, but it also needs control. Fleets have long relied on in-vehicle routers, but new demands are exposing gaps in speed, resiliency, and optimization. Failover can be slow, multi-modem capacity can go unused, and sessions can still drop when conditions change.

SD-WAN for control in motion

Fleet networks get stressed in predictable ways: coverage shifts as vehicles move, congestion appears without warning, and upload demand spikes when video clips or event data must be quickly dispatched. When the network treats all traffic the same, those moments lead to slowdowns, dropped sessions, and reactive troubleshooting.

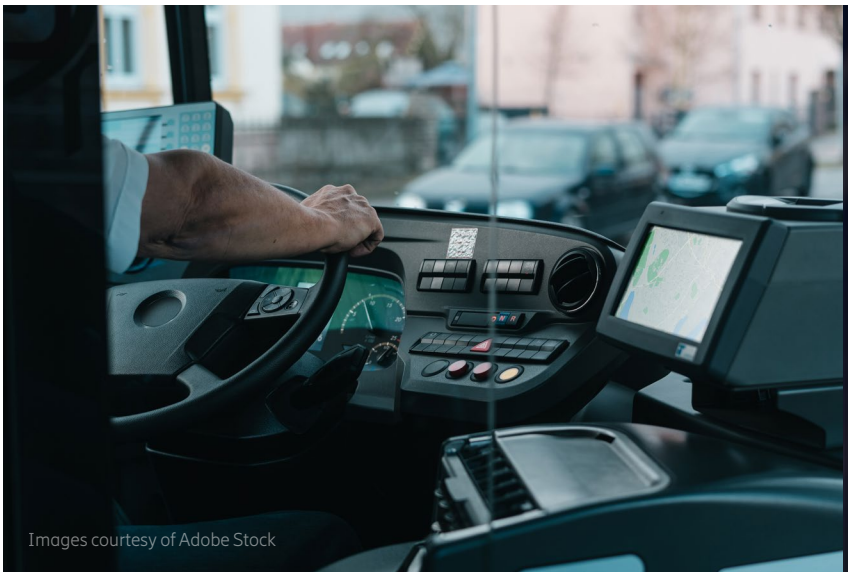
SD-WAN with traffic steering gives IT a way to handle fleet traffic based on application needs, rather than leaving performance to chance. Without it, even multi-modem setups can behave like a single link, with redundancy sitting idle. With SD-WAN, traffic can shift to the best-performing link to keep critical sessions stable.

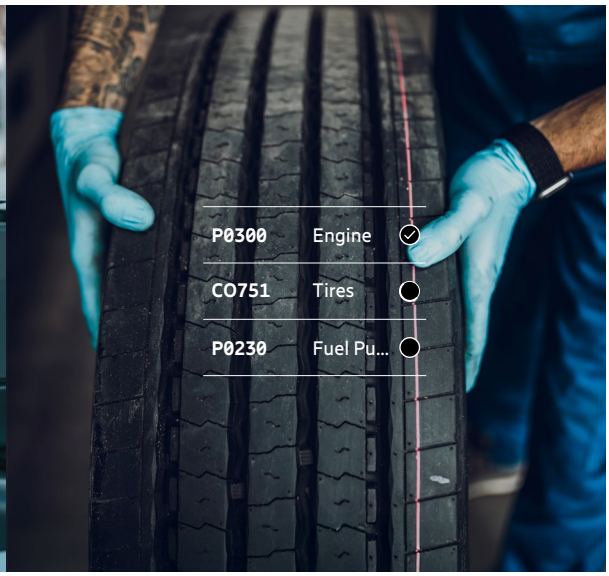
Prioritization is where teams feel the difference. Under load, critical traffic can stay on the strongest available path. Over time, that improves consistency across changing conditions and reduces disruptions that lead to troubleshooting.

Intelligent bonding for higher uptime

Many fleets plan for redundancy, but redundancy alone doesn't guarantee continuity. A link can look available while still experiencing packet loss or brief outages, which leads to retries, jitter, and lag. When only one path is used at a time, capacity and resiliency sit idle.

Full multilink bonding addresses this by aggregating all available modems into a software-defined "larger pipe." It splits and reassembles traffic flows across links to deliver more throughput than a single modem. For the most critical applications, selective packet duplication adds protection against loss and short interruptions to help sessions stay intact.





Images courtesy of Adobe Stock


Image courtesy of Getty Images

Resiliency that matches mobile conditions

Traditional failover is often too slow—and too blind—for fleet operations. Some failover solutions take two full minutes and offer no insight into whether the backup network will help, making recovery a guessing game. Failover can land on a worse or unavailable network, and failing back adds another downtime hit.

Dual-SIM Dual-Standby (DSDS) is built to avoid those pitfalls. Failover can happen in seconds, not minutes, and users can see the secondary network's health before switching. That enables smarter decisions, reduces the likelihood of failback, and avoids adding a second modem just to keep vehicles connected. Fleet teams should set failover targets in seconds, since dropped sessions and downtime are exactly what modern WWAN resiliency is meant to prevent.

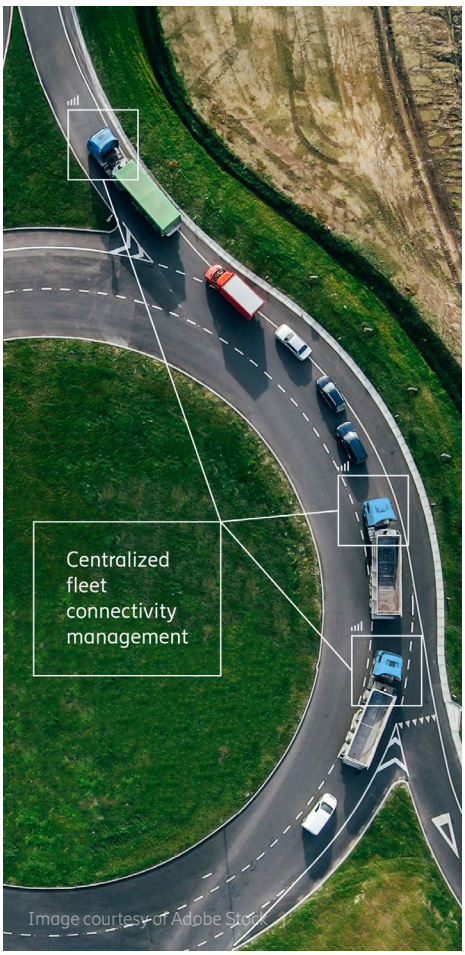
Security and control beyond the perimeter

Fleet connectivity extends the enterprise attack surface to thousands of mobile endpoints, making consistent policy enforcement essential, particularly when vehicles generate sensitive operational data. Security measures such as traditional VPNs are often cumbersome to deploy and manage across large fleets, leaving opportunities for large-scale attacks.

Zero trust principles support least-privilege access and reduce lateral movement during incidents. Built-in firewall controls help standardize baseline protection, while segmentation contains the blast radius if a device or user is compromised.

Cloud management helps lean IT teams by turning security into repeatable operations and supporting AI-assisted triage. Ericsson NetCloud's ANA helps teams surface anomalies earlier and reduces time spent on routine diagnostics when issues arise across many vehicles.

Deployment choices that determine long-term results



Fleet performance depends on deployment choices that hold up over time, not solutions that force a rip-and-replace later.

- Antenna placement can determine how well vehicles connect at the edge of coverage.
- Ruggedized hardware helps equipment withstand vibration, long run times, and harsh weather.
- Modular connectivity setups let teams upgrade key components without replacing everything in the vehicle.
- Centralized cloud management improves IT's ability to roll out standard configurations, monitor performance, and troubleshoot remotely.

A 5G WWAN setup for fleets provides clearer visibility and greater control when conditions change. Centralized management makes that practical at scale by keeping policies consistent across vehicles and resolving many issues without taking vehicles out of service. As fleets add more devices and precision services, 5G gives teams the headroom to grow without reworking the network every time.

Learn more about enterprise wireless solutions

The leadership checklist for 5G fleet connectivity

Modern fleets run on always-on systems inside the vehicle. For leadership teams, the goal is not "faster connectivity." The goal is predictable operations: consistent visibility, controlled risk, and a network foundation that can scale without repeated redesign.

Getting started checklist

- **SD-WAN for application-aware control in motion**
  Set clear targets for uptime, recovery time, and data availability tied to safety, compliance, and service continuity.
- **Identify the workloads that must remain stable under pressure**
  Confirm which applications cannot tolerate session resets or delays, then document what "acceptable interruption" means in seconds.
- **Validate capacity where it matters most**
  Fleet demands are increasingly upstream. Ensure the network plan supports video uploads, event reporting, and telemetry without disrupting essential traffic.
- **Treat security as foundational to the deployment**
  Standardize zero trust access, segmentation, and encryption so vehicles follow the same security posture across routes, regions, and teams.
- **Choose an operating model that scales with the fleet**
  Centralized cloud management should support standardized configuration, proactive monitoring, and remote troubleshooting without pulling vehicles out of service.
- **Make hardware and lifecycle decisions for long-term upgrades**
  Confirm connectivity hardware solutions for real conditions, then select modular platforms that support future expansion without full replacement.

Learn more about enterprise wireless solutions

Questions to discuss with your fleet management team

1. What is the worst-case outage scenario for our operations, and what recovery time is acceptable?
2. Which workflow fails first when connectivity degrades, and what does that failure cost us?
3. Can our security controls remain consistent across thousands of moving endpoints?
4. Do we have the tools and partners needed to deploy and manage this at fleet scale?