CONFERENCE INTELLIGENCE / NOVEMBER 2026

TRAINCOMMS 2026

From poor connectivity to dependable digital rail services

An independent 3G4G executive briefing | London, 18–19 November 2026 | Thematic review

The central message

In July 2026, our video “Why Connectivity on Trains Is So Poor” explained why mobile service or an onboard Wi-Fi icon does not necessarily mean usable internet. Railway coverage gaps, the metal structure of carriages, high-speed movement, congestion, uplink limitations and constrained onward connectivity all contribute. TrainComms 2026 shifted the conversation from why the problem exists to what can be done about it.

The technology choices are improving: cellular networks, trackside fibre and radio, roof antennas, onboard Wi-Fi, radio-permeable windows and low-Earth-orbit (LEO) satellites all have roles. Of the practical measures discussed, the results from laser-treated train windows were especially striking: better direct mobile reception without adding active onboard radio equipment. Yet no equipment choice alone resolves the responsibilities, economics and assurance of an end-to-end rail service.

Rail connectivity is also evolving from a passenger amenity into part of the train’s wider digital foundation. That makes architecture, security, long-term support and responsibility as important as speeds and coverage.

THREE TAKEAWAYS

Experience over peaks

Continuity, latency, VPN use and recovery often say more than headline Mbps.

Fix the window barrier first

RF-transparent glazing offers a compelling passive improvement to direct mobile reception.

Decades, not upgrades

Routes and rolling stock need maintainable contracts, open interfaces and accountable owners.

The question has changed

The original video asked: why does connectivity fail on trains? The discussion now needs to ask: what design, commercial model and evidence would make it reliable for the whole journey? There is no single technology winner, and no assumption that every train or application should share one network.

This is an independent synthesis of the two-day discussion, not an official conference record. Figures from trials and operators are reported observations, not independently audited guarantees.

LESSON 1 / DEFINE THE SERVICE PASSENGERS ACTUALLY NEED

Useful connectivity is not the same as maximum speed

The 5 Mbps question reveals a real tension

A six-month train Wi-Fi comparison reportedly capped one group of services at 5 Mbps per passenger while leaving another uncapped. The measured satisfaction results were described as essentially indistinguishable. This does not establish that everyone always needs only 5 Mbps: concurrent users, the applications being run, the distribution of speeds and the test population matter. It does challenge the assumption that ever-higher per-device peak speeds automatically improve the passenger experience.

A different line of discussion called for significantly more capacity, especially where commuters work online or hundreds of passengers share a limited number of mobile connections. These views are not necessarily contradictory. A modest stable individual rate can feel better than a high but intermittent rate, while aggregate carriage and train demand can still require substantial capacity.

Judge a journey through real applications

A particularly useful reported trial supported a Microsoft Teams call through a corporate VPN over a roughly 144-mile journey, with only one disconnection mentioned. That is an anecdotal trial account rather than a controlled independent benchmark, but it illustrates why application continuity is a better test than a speed-test screenshot. Upload capacity, packet loss, jitter, handovers and tunnel recovery all matter to a working call.

Captive portals are another neglected problem. An authentication page that appears straightforward to the operator may frustrate passengers using corporate VPNs, secure DNS or automatic reconnection. The correct test is whether passengers can get online quickly, retain their privacy protections and stay connected—not whether a portal loads successfully.

Measure both demand and experience

A more informative specification would combine journey availability, successful application sessions, latency and jitter, useful uplink, load at busy times and total data per passenger-hour. The last measure can inform capacity planning, but should not replace performance measures for bursty or delay-sensitive applications.

Practical lesson

Set minimum service outcomes for common passenger activities, then dimension total capacity for realistic occupancy. Do not confuse a sensible per-user policy with a justification for under-provisioning the train-to-ground link.

A better dashboard than headline Mbps

A practical whole-journey scorecard should report successful VPN and video-call sessions, usable uplink, 10th-percentile throughput, packet loss, latency and time to reconnect after tunnels or bearer changes. Test at realistic passenger occupancy; a high peak speed on an empty train is not an adequate measure of service quality.

LESSON 2 / REMOVE THE CARRIAGE BARRIER FIRST

Laser-etched train windows deserve far more attention

The measured improvements were substantial

Metallised train windows are designed for thermal performance but can significantly weaken mobile signals inside a carriage. In high-speed field testing performed by SNCF across three French mobile networks and presented at TrainComms 2026, fully RF-transparent, laser-treated windows delivered reported downlink gains of 52–286%, uplink gains of 45–201%, and 33–40% fewer connection errors compared with conventional coated glass. The figures are observed ranges across tests, not a guaranteed improvement on every route or train.

A further comparison found that fully treated carriages also performed better than those with only alternate windows treated: up to 22% more downlink throughput, up to 60% more uplink throughput and approximately 25–30% fewer errors. Taken together, these are among the conference's most compelling measured results. They also reinforce an important point from our earlier video: the problem can be the train itself, even where an outdoor mobile signal exists.

Laser etching versus repeaters: the passive solution has a strong advantage

For the specific job of helping passengers' phones connect directly to outdoor mobile networks where those networks have coverage, our assessment is that laser-etched windows are normally the preferred first choice over active onboard repeaters. They require no power-hungry amplification chain, operating software, dedicated signal distribution or ongoing active-radio maintenance. They also avoid repeater-specific band configuration, oscillation and interference management, and approval and support arrangements. This offers a compelling engineering and lifecycle-cost argument for treating glazing before introducing additional radio equipment.

That is an independent design judgement, reinforced by conference discussion and the move to RF-transparent windows in new trains. It is not a claim of proven universal superiority: the reported field percentages compare treated and conventional coated glazing, not a controlled etching-versus-repeater test. Window retrofits still need approval, testing and cost assessment.

Properly engineered repeaters can be useful when glazing treatment is impractical or a specific design requires them. However, combining repeaters with RF-transparent glazing can reduce isolation between the repeater's external and internal antennas, increasing the risk of feedback and interference unless carefully engineered.

Treating windows does not replace other connectivity systems

Radio-transparent glazing improves direct cellular service for passengers whose network provides coverage. It may also reduce the load on onboard Wi-Fi. But it cannot fix external blackspots, does not serve Wi-Fi-only devices directly and does not bond several operators' links into one backhaul. Roof antennas with an onboard gateway and Wi-Fi remain useful for those jobs. In practice, the strongest design can combine treated windows with good trackside coverage and a properly sized Wi-Fi system, rather than framing every option as a substitute for the others.

A genuine trade-off: 6 GHz Wi-Fi and emissions beyond the carriage

The same radio transparency that benefits a passenger's cellular signal reduces attenuation of Wi-Fi emissions escaping from inside the train. This raises specific questions for 6 GHz Wi-Fi 6E/7 deployments, including moving-vehicle rules, power levels and protection of incumbent systems. This was identified as a practical obstacle requiring measurement and regulatory engagement; it

should not be turned into a blanket claim that 6 GHz Wi-Fi is either universally permitted or prohibited in treated carriages.

Trackside networks require substantial civil infrastructure

London Underground demonstrates the difficult engineering behind a coverage map: confined work areas, access windows, power, fibre, radio sites, emergency-service requirements and continuing maintenance. Stations may use higher-capacity bands, while tunnels rely on different propagation designs such as radiating (leaky-feeder) cable. Neutral-host installations can serve several operators, but need coordination and clear fault ownership.

Trackside fibre can outlive several radio generations and support blackspot remediation, stations, railway operations and future neutral-host or high-capacity radio services. Its business case depends on sites, power, access rights, partners and benefits extending beyond one railway service.

Practical lesson

First, remove unnecessary attenuation from the carriage: assess RF-transparent, laser-treated glazing before investing in active repeaters solely to overcome window losses. Then dimension roof antennas, Wi-Fi and trackside infrastructure for the actual coverage and capacity gaps.

LESSON 3 / SATELLITE OFFERS CHOICE, NOT AUTOMATIC RESILIENCE

A multi-bearer future needs realistic railway products

The market is broader than one constellation

LEO satellite is a genuine new option on routes with poor terrestrial coverage, but the discussion was not simply about Starlink. OneWeb services, including rail-oriented terminals, provide another approach. The possibility of future choices involving additional constellations, such as Amazon Leo, strengthens the case for avoiding proprietary integration. It should not be mistaken for an assurance that multi-constellation interoperability exists today.

Dynamic switching between GEO and LEO systems, or moving transparently among multiple LEO networks using a common terminal, remains a difficult combination of hardware, software, commercial and operational requirements. Railway procurement should distinguish an integration roadmap from an available, supported feature.

High-speed rail is not a road vehicle or an aircraft

A train may need reliable operation at 300–400 km/h, with multiple carriages, challenging roof geometry, overhead equipment, long tunnels and frequent obstruction. These speeds should be treated as requirements to be demonstrated and contractually supported, rather than assumed capabilities of every satellite service or terminal. Satellite proposals need route-specific speed profiles, installation approval, terminal certification, coverage testing and contractual commitments. An antenna demonstrated on one route or train type is not necessarily a standard fleet-ready product.

Rail assets are built for long lives. If terminals must be refreshed frequently, the cost is not only hardware: it includes engineering access, certification, training, spares, service disruption and e-waste. Contracts should cover tariffs, speed permissions, planned obsolescence, software support, repairability and who pays for forced upgrades.

There is no satellite path through a tunnel

Satellite service still depends on a usable view of the sky. Tunnels, covered stations, cuttings and obstructions force a return to terrestrial coverage, onboard buffering or application-level continuity. Combining cellular and satellite improves resilience only if the failure modes are different and the switching process preserves sessions where required.

Direct-to-device satellite is unlikely to be a general solution for passengers using handsets inside metal-bodied trains. Handset uplink power, roof attenuation, glazing, beam visibility and moving-vehicle geometry are major constraints. Niche emergency or messaging services should be evaluated separately from broadband train connectivity.

Practical lesson

Procure satellite as a clearly specified bearer in a hybrid architecture—not as a universal substitute for trackside networks or as proof that every train can now offer uninterrupted broadband.

LESSON 4 / SEPARATE RISK EVEN WHEN SHARING INFRASTRUCTURE

The most important disagreement was architectural

One platform for everything—or separate systems?

There are genuine benefits to an onboard digital platform carrying passenger Wi-Fi, payment, crew apps, CCTV, diagnostics and other information services: fewer duplicate boxes, easier data sharing and potentially better procurement economics. But integrating more services also increases the blast radius of a failure or cyber incident. A busy, fast-changing passenger network should not casually become the path on which an essential railway function depends.

The alternative is physical or strong logical separation according to the consequence of failure. Passenger internet, business-critical crew applications, operational technology and safety-related train communications need clearly distinct assurance levels. Railway control and future FRMCS/GSM-R migration cannot be treated as ordinary passenger broadband features. Where a shared physical network is justified, reserved resources, segmentation, independent local operation and verified fault isolation must be demonstrable.

Open software is useful only with disciplined operations

Open APIs, modular onboard applications and container platforms such as Kubernetes could make trains less dependent on single-purpose proprietary boxes and simplify updates across fleets. Yet containers do not solve poor radio coverage, and software changes on moving assets require secure credentials, version control, offline operation, rollback and support across long equipment lifetimes.

Monitoring and intrusion detection within industrial switches may provide earlier visibility of suspicious activity without additional dedicated appliances everywhere. That is useful defence in depth—not a substitute for network segmentation, secure updates, least-privilege access or incident response. It can also add a new management and support obligation.

Failover is a service, not a diagram

Two links may still share one gateway, power system, management cloud or supplier. Resilience depends on independent failure modes, transparent prioritisation and reliable recovery from tunnels, network loss and equipment faults. Critical onboard functions must retain defined local behaviours when external connectivity disappears.

Practical lesson

Decide which services can share assets, which must be isolated, and which require independent safety assurance before selecting hardware or inviting vendors to propose a single “connected train” platform.

LESSON 5 / BUY OUTCOMES, RETAIN CONTROL AND AVOID LOCK-IN

Capacity, network APIs and contractual accountability

Prioritisation can help, but does not create radio capacity

The discussion included GSMA Open Gateway/CAMARA Quality on Demand (QoD), which can request preferential network treatment for a specified data flow. The approach is not confined to 5G; it can be implemented in 4G too, subject to network support. It creates an intriguing choice: improve the train gateway's cellular links or prioritise individual passengers' connections, particularly where the operator offers paid connectivity or commercial premium service options.

One low-cost rail example also highlighted the commercial tension: paid Wi-Fi at around €3, a train carrying up to roughly 1,000 passengers and a limited group of cellular backhaul links. The precise modem count requires further verification, but the capacity-sharing problem is clear.

However, QoD or slicing cannot eliminate a physical dead zone, exhausted site capacity or inadequate antenna performance. Preferential treatment changes how scarce resources are allocated. Whether it is effective needs before-and-after route measurements, clear charging rules and evidence of benefit to actual applications. The conference provided limited rail-specific evidence of network slicing at scale.

Who owns the data, network and operational decisions?

Supplier sovereignty is not confined to satellites. Buyers need to understand where connectivity traffic is routed, where diagnostics and CCTV are stored, who can access them, what happens when contracts end and whether a replacement supplier can take over without rebuilding the train. The same questions arise with onboard software, SIM management, cloud dashboards and outsourced security operations.

Railway procurement periods are long, but equipment and software evolve quickly. A technically successful proof of concept can still fail an operator's requirements for cyber assurance, spares, price stability, data governance or supplier support. Neutral-host infrastructure and multi-vendor APIs are valuable only when they reduce practical switching costs rather than adding interfaces without clear accountability.

What a credible procurement should ask

- Define acceptance criteria at the passenger device and at the operational application, not solely at a router or satellite terminal.
- Test at busy occupancy, in tunnels, at handovers and when a preferred bearer fails; capture application recovery as well as throughput.
- Identify the safety and cyber boundary for every service and document who authorises changes to it.
- Obtain explicit lifecycle, pricing, replacement, data-portability and fault-ownership commitments from every supplier.

The real commercial test is not the lowest cost per advertised Mbps. It is total cost of delivering a reliable, measurable service over the equipment and infrastructure lifecycle.

LESSON 6 / AN AGENDA FOR THE NEXT PHASE

What still needs more evidence

Not every promising area received equal attention. A future-facing roadmap should test, rather than assume, the value of Wi-Fi 8, onboard 6 GHz deployments, AI-driven application traffic, 5G network slicing, CAMARA-based prioritisation and consistent multi-bearer orchestration. FRMCS boundaries need to be addressed through railway-specific standards and assurance, not by analogy with consumer 5G.

The most urgent evidence gaps concern whole-journey availability, train-to-ground capacity under load, independent cellular/satellite failure behaviour, commercially supported rail-speed profiles, upgrade costs and the business case for shared trackside infrastructure. Trial outcomes should be documented with route, train configuration, test dates and limits, and be reproducible by the buyer.

Five lessons to take into the next investment cycle

- Start with the passenger or operational outcome, then find the weakest link in the chain.
- Treat window attenuation as a first-order problem: prioritise passive RF-transparent glazing where feasible, then add active equipment for needs it cannot solve.
- Treat passenger access and safety-related operations as different assurance problems.
- Test VPNs, sessions, failure recovery and whole-route availability alongside speed.
- Procure for sovereignty, replaceability, security and maintainable costs over years—not a short demonstration.

Continue from our original video

The July 2026 3G4G video and accompanying article explain the technical causes of poor train connectivity. This briefing adds the architectural, economic and operational choices required to improve it.

Watch: Why Connectivity on Trains Is So Poor

Read: Why Connectivity on Trains Is Still So Poor

PURCHASE THE DETAILED REPORT

A comprehensive TrainComms 2026 research report, containing detailed session analysis, technical findings and independent 3G4G assessments, has also been prepared. For information about availability, pricing and professional licensing, please contact reports@3g4g.co.uk, quoting “TrainComms 2026 Research Report”.

Independent analysis by 3G4G | www.3g4g.co.uk | Updated 21 November 2026