CSL

Critical IoT Connectivity **Experts**

White Paper · Mission-Critical Connectivity for Roadside ITS

Resilient Connectivity for Traffic Management & ITS

Why ANPR, CCTV, radar, LiDAR and signal control systems need a multi-network, DualCore® security overlay: independent of shared networks not designed for mission-critical operations.

For highway-authority IT leads, ITS programme managers, and traffic and network operations teams.

Version: 5.0

Date: June 2026

1. The Connected Road Is Mission-Critical, and Exposed

EXECUTIVE SUMMARY

Traffic management risk no longer stops at the locked roadside cabinet. ANPR cameras, CCTV, radar, LiDAR, variable message signs, and signal controllers are increasingly IP-connected, with remote access now routine across many estates.

Across the 2026 traffic-technology season, the dominant themes are smart infrastructure, cybersecurity, AI-driven traffic control, and connected mobility[1]. Each depends on secure, near-continuous connectivity from the roadside to the control centre.

Yet a gap remains. Investment flows to detection hardware, AI analytics, and cloud platforms, but the communications layer carrying that data often runs over shared broadband, commodity cellular, or legacy copper, with no independently resilient failover path.

The fundamental question is not whether roadside devices are IP-connected. It is whether they should continue to share the same WAN path, the same public APN, and the same upstream dependency as general-purpose traffic, without explicit risk acceptance and a documented resilience strategy.

Physically exposed

Roadside cabinets, gantry-mounted cameras, and pole-top radar units sit in uncontrolled public environments; smart-city security research repeatedly identifies weak authentication, internet exposure, and poor device hardening.

Operationally critical

A compromised ANPR feed is a loss of visibility for law enforcement. A spoofed VMS message can cause confusion and disruption. A disabled signal controller can create unsafe junction behaviour or force degraded operation.

Legislatively in scope

Transport is already a regulated sector under the UK's NIS Regulations 2018. The Cyber Security & Resilience Bill proposes to expand these obligations, including incident reporting requirements, supply chain duties, and stronger regulatory enforcement powers, though final provisions remain subject to parliamentary passage[2].

Board-level takeaway: Roadside connectivity is now part of the operational risk surface. Where these systems support enforcement, safety, or congestion management, the communications layer should be specified, tested, and governed with the same rigour as the devices it serves.

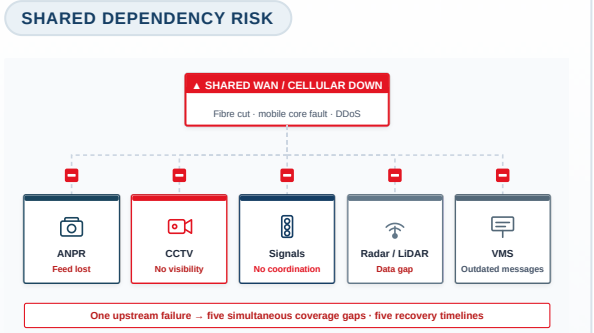


Figure 1: When ITS devices share a single upstream WAN, one outage creates a multi-domain cascade.

What a shared outage looks like

When roadside ITS devices share a single upstream broadband or commodity cellular path, one failure (a severed fibre, a mobile core outage, or a targeted DDoS) can cascade across every domain simultaneously: ANPR and enforcement feeds stop reaching back-office, police, or local-authority systems; CCTV stops transmitting at a critical junction; VMS boards continue displaying outdated messages; and signal controllers lose central coordination.

2. Sector Landscape: What the 2026 Season Reveals

No single event defines the traffic and transport sector, but taken together, the 2026 exhibition season offers a clear snapshot of where investment is flowing, and where it is not. From Intertraffic Amsterdam (the global benchmark for road infrastructure, traffic management, safety and parking) to the UK's own Commercial Vehicle Show, Traffex and Parkex, the same technologies dominate the floor[1]. The market is substantial and still growing: mainstream 2026 analyst estimates for ITS cluster around USD 54 billion to USD 63 billion, though figures vary widely with scope and methodology[13].

Across all of them the shift is the same: from low-tech infrastructure to high-tech, data-driven systems, with growing convergence between traffic management, road freight, enforcement and parking[4]. The recurring sub-themes (big data and cybersecurity, AI and machine learning, connected and automated driving, decarbonisation, and ANPR-based enforcement) all depend on resilient, secure data pathways from roadside to cloud.

The 2026 season at a glance

2026 Event	Sector lens	Recurring technology themes
Intertraffic Amsterdam Mar · global	Traffic management, safety, parking, smart mobility	Big data & cybersecurity, AI/ML, C-ITS, connected & automated driving
Commercial Vehicle Show Apr · NEC Birmingham	Road freight & fleet	Decarbonisation, AI, emerging fleet technology, connected vehicles
Traffex May · Coventry	UK highways & asset management	Implementation, detection & enforcement, network performance
Parkex May · Coventry	Parking & kerbside	ANPR enforcement, EV infrastructure, digital transformation
Highways UK Oct · NEC Birmingham	Strategic road network	Digital roads, resilience, future ITS

Across every one of these events the common thread is the same: growing dependence on real-time, IP-connected data flows from roadside to back office. Detection, enforcement, freight and parking innovation all assume that connectivity is reliable, secure, and always on, and cooperative systems such as C-V2X deepen it further. The sector is investing heavily in smarter roadside systems, but is the connectivity beneath them resilient enough to match?

The connectivity gap the sector overlooks

Walk any of these exhibition halls and you will find radar that counts vehicles, AI that predicts congestion, and cameras that read plates at motorway speeds. What receives less attention in market messaging is the resilience architecture that carries roadside data from device to control centre, and what happens when that path fails.

Many roadside ITS estates still connect via one of three paths: local authority broadband (often shared with corporate IT), commodity 4G/5G SIMs on public APNs, or legacy copper/fibre. These paths are often optimised for availability and coverage rather than for a segregated, independently resilient security overlay. In many cases, DualCore failover across physically separate operator cores, private APN routing, and end-to-end VPN encryption are not provided as standard without additional design.

≈1,000
More IT providers in scope under the Cyber Security & Resilience Bill[2]

1,988
Cyberattacks per day on the average UK business (Q1 2026)[5]

24 hrs
Proposed initial incident notification window under the Bill[2]

3. The Regulatory & Threat Landscape

The regulatory accelerant

In force now: Transport is a regulated sector under the UK NIS Regulations 2018, with existing duties on operators of essential services to manage network and information system security.

Proposed in the Bill: The Cyber Security and Resilience Bill, introduced in November 2025, cleared its Commons committee stage in February 2026 and, following carry-over into the 2026–27 session, completed its Commons stages (report stage and third reading) in June 2026 and was brought to the House of Lords, where it received its first reading on 17 June 2026 (HL Bill 32); its Lords second reading is scheduled for 14 July 2026. It proposes to expand scope to include critical suppliers, introduce 24-hour initial notification and 72-hour incident reporting, and give regulators power to investigate supply chain vulnerabilities. The Bill also proposes strengthened enforcement powers[2]. As at 26 June 2026 the Bill had not received Royal Assent; the remaining Lords stages and dates, final obligations, commencement dates, thresholds, and secondary legislation should be confirmed against the official Bill record and Hansard before you rely on it.

Operational implication: Highway authorities, traffic management centres, and their key technology suppliers should anticipate stricter duties on network security, resilience, and incident notification, making connectivity architecture a governance question, not just an engineering one.

Implication: For operators in scope of NIS, roadside ITS connectivity that depends on single-path backhaul, public exposure, or weak encryption should be tested against the operator's risk assessment, resilience objectives, and incident-reporting duties.

Governance context: For UK operators of essential services, the issue is not simply whether a device is connected, but whether the network and information systems supporting the essential function are resilient, governable, and recoverable. In practice, this aligns with the NIS regime and the NCSC Cyber Assessment Framework, both of which focus on security outcomes, resilience, and the ability to sustain essential functions under attack or failure[3].

Supply chain dimension: The security of roadside ITS no longer sits solely with the highway authority or control room. Device vendors, system integrators, mobile providers, WAN providers, and cloud analytics suppliers all shape the resilience of the service. The Bill's emphasis on critical suppliers makes connectivity architecture a supply-chain issue as much as a network issue[2].

Regulatory references correct as of 26 June 2026; verify against current legislation before reliance.

Who attacks roadside ITS, and why

Roadside ITS faces at least three distinct threat actors, each with different motivations and capabilities. **Opportunistic attackers** scan for exposed devices using tools such as Shodan, which indexes internet-connected infrastructure including traffic controllers, CCTV cameras, and SCADA systems, many still configured with default credentials[7].

Ransomware operators increasingly target local authorities and transport organisations. A major UK transport operator's 2024 cyber incident demonstrated that transport operators are high-value targets, with customer data access, operational disruption, and reputational exposure extending well beyond the initial technical compromise[8].

State-aligned actors probe transport and critical national infrastructure for strategic disruption potential; the NCSC has warned that UK critical infrastructure, including transport networks, faces an enduring and significant cyber threat, increasing the importance of resilience in systems that support essential services[9].

Roadside ITS sits at the intersection of all three: devices are internet-exposed, the operating authorities are public-sector targets for ransomware, and the infrastructure itself has strategic value.

4. The Threat Model & Why a Security Overlay

Attack vectors by device type

Device Class	Threat Scenario	Consequence
ANPR cameras	Interception of plate data, feed manipulation, DDoS on backhaul	Loss of law-enforcement visibility; evasion of LEZs, tolling, stolen vehicle tracking
CCTV / surveillance	Hijacking of streams, PDoS (phlashing) to destroy firmware, man-in-the-middle injection	Evidence gaps; traffic management centre loses situational awareness
Radar / LiDAR	Spoofed vehicle counts, tampered speed data, sensor disruption	False congestion signals; incorrect speed enforcement; flawed planning data
Signal controllers	Unauthorised command injection, timing manipulation; C-V2X exploitation where connected-vehicle interfaces are deployed	Unsafe junction states; gridlock; potential for physical harm to road users
VMS / message signs	Message tampering via default credentials, physical access exploitation	Public misinformation; disruption; reputational damage to highway authority

Cybersecurity researchers have ranked traffic surveillance cameras and smart traffic signals among the most vulnerable smart-city assets[6]. Reports still find roadside IoT devices with default credentials, unencrypted backhaul, and hard-to-patch firmware in the field[7].

Not hypothetical: international examples

In 2024, researchers disclosed a critical vulnerability enabling remote code execution on a deployed traffic signal controller, which could be used to alter signal timing or force a fail-safe flash mode[10]. Variable message signs have been physically tampered with in multiple incidents, replacing safety warnings with offensive content[11]. And in a separate 2023 incident in Europe, unsecured radio frequencies were used to trigger emergency stops on around 20 trains[12].

In each case, insecure communications design, internet exposure, or weak authentication amplified the impact.

Scenario: what a single-path failure looks like in practice

Consider a local authority operating 20 ANPR cameras, 15 CCTV feeds, and 8 VMS boards across a city-centre Clean Air Zone, all backhauled over a single shared broadband WAN. When the broadband provider suffers a regional outage lasting four hours, every enforcement camera loses connectivity simultaneously. CAZ violations go unrecorded, CCTV evidence is lost for any incidents during the window, and VMS boards display outdated diversion messages that no longer reflect live conditions. The authority has no independent failover path because all devices share the same upstream dependency. Recovery requires the broadband provider to restore service, a timeline the authority cannot control.

Why a security overlay, not just network segmentation

Network segmentation (VLANs, firewalls, ACLs) limits lateral movement inside a network. It does not remove a shared upstream dependency. If the broadband circuit feeding a roadside cabinet is cut, every VLAN on that circuit loses connectivity. If the commodity mobile core serving ANPR and CCTV SIMs has a platform outage, segmentation inside the traffic management centre is irrelevant; no data arrives. Segmentation still matters for containing an incident inside the ITS environment, but the shared upstream path is a separate problem, and that is what a security overlay addresses.

A security overlay communications layer can be deployed below and independently of the site network. In the CSL architecture, it is designed to provide a separate data path, using different operator cores, different APNs, and different encryption tunnels, so that roadside devices can maintain connectivity even when the primary WAN or shared mobile service fails.

5. How the Security Overlay Works

Read from bottom to top. Roadside devices send data upward through one of two independent encrypted paths (Core A or Core B) to the traffic management centre and cloud. The active core is selected automatically – delivered either by the rSIM® at the SIM layer, or by a CSL managed router at the gateway. Corporate IT (top right) runs on a completely separate network.

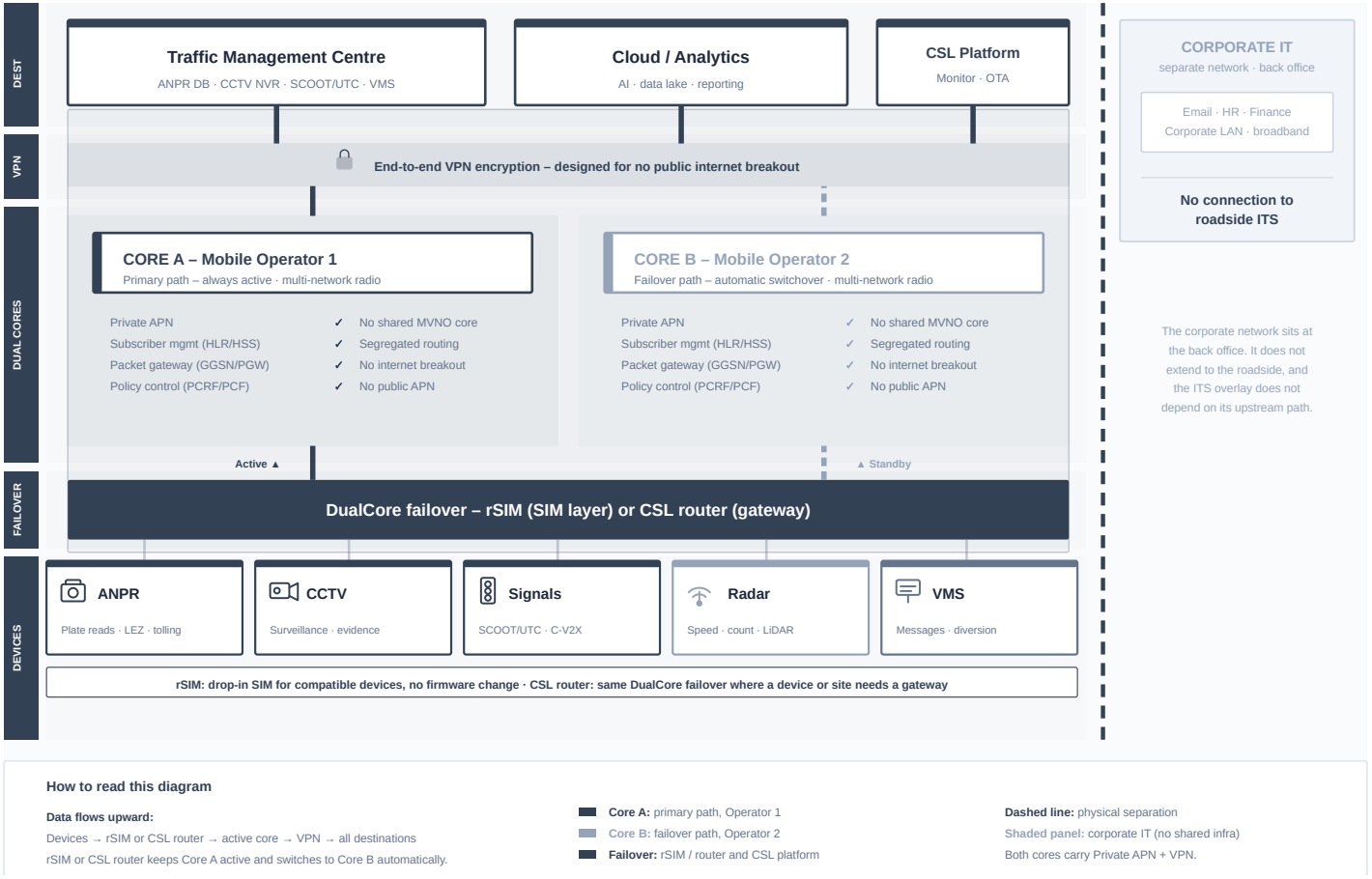


Figure 2: CSL DualCore security overlay. Data flows from roadside devices (bottom) through one of two independent encrypted paths to the TMC and cloud (top); the active core is selected automatically. CSL delivers DualCore either through the rSIM at the SIM layer (a drop-in SIM for compatible devices) or a CSL managed router at the gateway (for sites or devices that need one). Corporate IT (top right) is physically separate.

6. The Overlay Architecture

Overlay vs. underlay: what changes

Attribute	Commodity Connectivity	Security Overlay (CSL)
Mobile core	Single shared MNO/MVNO core	DualCore: two physically separate operator cores (Core A + Core B)
Radio access	Often multi-RAN, but routed through a single shared core	Multi-network/multi-RAN on both DualCore profiles (Core A and Core B)
APN	Public / shared APN	Private APN on both cores
Encryption	Application-layer only (if at all)	End-to-end VPN; designed for no public internet breakout
Failover	Manual SIM swap or none	Automatic DualCore failover – rSIM (SIM layer, below firmware/OS) or CSL router (gateway)
Monitoring	Device-level only	CSL platform: connectivity health, heartbeat, OTA SIM management
Physical independence	Shares site broadband or single MNO	Entirely independent of site LAN, broadband, or primary MNO path

Design principle: The communications path that carries ANPR hits, CCTV streams, radar telemetry, and signal commands should never inherit the same single point of failure as the general-purpose connectivity it runs alongside. Segregation limits the scope of any compromise. Independence removes the shared dependency. Here, “physically separate” cores mean distinct operator-core infrastructure, including subscriber-management, packet-gateway and policy-control; deployment evidence should confirm the exact architecture.

Architecture principle: inner network vs. outer overlay

A highway authority's corporate IT (email, HR, finance) runs on the inner network, via standard broadband and LAN infrastructure. Roadside ITS devices (ANPR, CCTV, radar, signal controllers) should run on an **outer security overlay**: physically separate, independently resilient, and managed end-to-end by a specialist connectivity provider.

CSL's DualCore architecture provides exactly this: a security overlay communications layer that operates independently of the authority's corporate WAN, with DualCore failover (delivered via the rSIM or a CSL managed router), Private APN, and VPN encryption as standard.

When the corporate broadband goes down, the outer overlay is designed to keep ANPR, CCTV, radar, and signal control operational, because it does not depend on the same upstream path.

About CSL Group

CSL Group is a UK and EU telecommunications company specialising in resilient connectivity for critical IoT. With a Private APN + VPN infrastructure supporting over 3.5 million active connections[14], we provide the outer connectivity layer, independent of site LAN and general-purpose broadband, for security, life-safety, telemetry, and operational technology endpoints across multiple sectors. Our managed range spans IoT SIMs, the DualCore rSIM, and secure managed routers. Our current partnerships and deployments across retail, security, and connected infrastructure apply the same managed-resilience principles described in this paper.

How CSL supports roadside ITS architecture

Multi-network on both profiles: Each DualCore profile (Core A and Core B) is itself multi-network/multi-RAN across multiple operators' radio. Commodity links are often multi-RAN but routed through one shared core; DualCore keeps that on both profiles, with two separate cores beneath.

Verified core independence: Two separate operator cores, each with its own subscriber-management, packet-gateway and policy-control (HLR/HSS, GGSN/PGW, PCRF/PCF). If Core A fails, rSIM switches to Core B automatically, at the SIM layer.

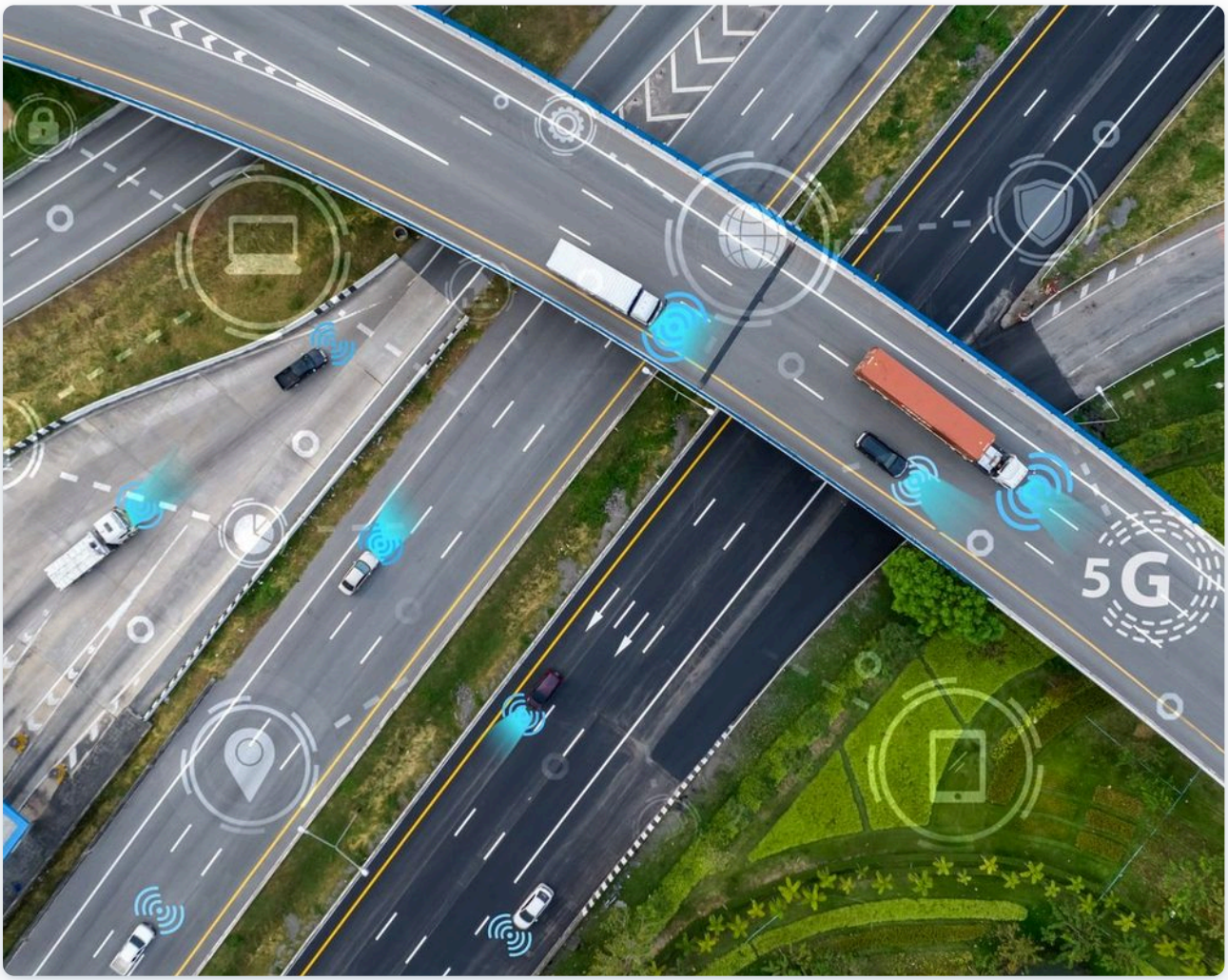
SIM-layer deployment: rSIM is a drop-in SIM for compatible devices that adds DualCore resilience at the SIM layer, with no firmware or hardware changes. Where the device and module support it, rSIM also enables GSMA SGP.32-aligned over-the-air profile management.

Private APN on both cores: Traffic is designed to remain within CSL's private network, with no public internet breakout, and is protected by end-to-end VPN encryption from roadside device to control centre or cloud.

Heritage in life-safety signalling: Private VPN connectivity to hundreds of ARC locations across Europe[14]. Architecture principles proven in alarm signalling apply directly to ITS backhaul.

Managed routers, proven in security: For a site that needs a router rather than a drop-in SIM, CSL supplies managed routers trusted across the security industry (intruder-alarm and CCTV): data on a Private APN with end-to-end VPN, hardened with no default credentials, centrally managed and monitored.

Single managed service: Connectivity, failover, monitoring, and OTA SIM lifecycle, all managed by CSL as a single service.



7. Deployment Profiles & Next Steps

Applicable deployment profiles

Urban junction
8× ANPR, 12× CCTV, 2× radar, 4× signal controllers, 2× VMS

Motorway corridor (10 km)
40× ANPR, 30× CCTV, 20× radar/LiDAR, 15× VMS, gantry controllers

Clean Air Zone / LEZ
ANPR enforcement ring, VMS signage, environmental sensors, payment integration

Temporary / event
Rapid-deploy CCTV towers, mobile ANPR, temporary signal control for roadworks

Next steps: assess your roadside connectivity risk

Before engaging with CSL, highway authorities and ITS integrators can apply a quick self-assessment to their current roadside estate. At minimum, roadside ITS connectivity should be private, encrypted, monitored, independently failover-capable, and separable from general-purpose corporate or site WAN dependencies.

Five-question connectivity risk test

1. Is there a single shared upstream dependency (broadband, MNO, or fibre) serving multiple ITS device types?
2. If that upstream path fails, is failover automatic and independent at core level, or does it require manual intervention?
3. Is the APN private and dedicated, or does ITS traffic share a public APN with general-purpose devices?
4. Does traffic between roadside devices and the control centre avoid public internet breakout entirely?
5. Can resilience be added to existing deployed devices without hardware modification or firmware change?

If the answer to any of these is "no" or "unsure," there may be an unmanaged single point of failure in your roadside ITS estate.

Minimum evidence to request from connectivity providers

- Proof that failover uses separate operator cores, not shared-MVNO routing
- Confirmation that the APN is private and segregated from public and general-purpose traffic
- Confirmation that traffic avoids public internet breakout
- Evidence of recovery/failover testing and documented recovery times
- A statement of where security responsibility sits between device vendor, integrator, WAN provider, and overlay provider

CSL works with highway authorities, local authorities, and ITS integrators to surface single points of failure in roadside connectivity and design a resilient DualCore overlay around them, producing the assurance evidence your board, auditor, or risk owner will ask for, mapped to the checklist above.

Option A
Open a consultative discussion about your roadside estate

Option B
Schedule a 30-minute architecture briefing with a CSL connectivity specialist

Glossary of Terms

Plain-language definitions for the technical terms and acronyms used in this paper.

ANPR Automatic Number Plate Recognition. Cameras that read vehicle plates for enforcement, tolling and zone access.

APN / Private APN Access Point Name: the gateway between a device and a mobile data network. A Private APN keeps traffic on CSL's network and off the public internet.

ARC Alarm Receiving Centre. A monitoring centre that receives and acts on life-safety and security alarm signals.

CCTV Closed-Circuit Television. Roadside cameras used for monitoring and incident evidence.

CNI Critical National Infrastructure. The assets and services a country depends on, including transport networks.

C-V2X Cellular Vehicle-to-Everything. Cellular communication between vehicles and roadside infrastructure.

CVE Common Vulnerabilities and Exposures. The public catalogue of known security flaws, each with a reference number.

DualCore CSL's resilient architecture using two physically separate mobile operator cores, so a device can fail over from one core to the other without relying on a single shared core. Delivered via the rSIM or a CSL managed router.

eSIM An embedded SIM whose network profiles can be provisioned and switched remotely (see GSMA SGP.32).

ETSI TS 102 940 The ETSI standard for ITS communications security architecture and security management.

GGSN / PGW Gateway GPRS Support Node / Packet Gateway. The core function that routes mobile data to and from external networks.

GSMA SGP.32 The GSMA specification for remote SIM provisioning for IoT devices (the IoT eSIM standard).

HLR / HSS Home Location Register / Home Subscriber Server. The core function that holds subscriber identity and authorises network access.

ITS Intelligent Transport Systems. Networked technology used to monitor and manage roads and traffic.

LEZ / CAZ Low Emission Zone / Clean Air Zone. Areas where vehicle access is managed by emissions, usually enforced with ANPR.

LiDAR Light Detection and Ranging. A laser-based sensor that builds a 3D picture of the road scene.

managed router A CSL router that delivers DualCore failover at the gateway, where a device or site needs a router rather than a drop-in SIM.

MNO / MVNO Mobile Network Operator / Mobile Virtual Network Operator. An MVNO sells service over a host MNO's network and usually runs some of its own infrastructure, so traffic can depend on both the host operator's core and the MVNO's own systems, not a genuinely independent second core.

multi-RAN / multi-network The ability to use more than one operator's radio access network (RAN), selecting the best available signal.

NCSC CAF National Cyber Security Centre Cyber Assessment Framework. The UK framework for assessing the cyber resilience of essential services.

NIS Regulations Network and Information Systems Regulations. The UK regime for the security of essential and digital services, being updated by the Cyber Security and Resilience Bill.

OT Operational Technology. The hardware and software that directly monitors or controls physical equipment such as signals and sensors.

OTA Over-the-air. Remote update or switching of SIM profiles without physical access to the device.

PCRF / PCF Policy and Charging Rules Function / Policy Control Function. The core function that applies data policy and quality-of-service rules.

radar A sensor that detects vehicle presence, speed and count using radio waves.

rSIM CSL's resilient SIM. A drop-in SIM for compatible devices, holding two network profiles, that switches to the standby core automatically at the SIM layer with no firmware or hardware change. Where the device and module support it, it also enables GSMA SGP.32-aligned remote profile management.

SCOOT / UTC Split Cycle Offset Optimisation Technique / Urban Traffic Control. Systems that coordinate traffic signals across a road network.

signal controller The roadside unit that operates a set of traffic signals.

TMC Traffic Management Centre. The control room that monitors and operates the road network.

VMS Variable Message Sign. An electronic roadside sign that displays live messages and diversions.

VPN Virtual Private Network. An encrypted tunnel carrying data end to end between a device and its destination.

Sources & Notes

References supporting the analysis in this paper. Sources are cited by name; parliamentary and regulatory positions re-verified 26 June 2026.

Official / public sources

[1] 2026 road-sector exhibition season: Intertraffic Amsterdam (10–13 Mar 2026, RAI); Commercial Vehicle Show (21–23 Apr 2026, NEC Birmingham); Traffex & Parkex (co-located; 20–21 May 2026, CBS Arena, Coventry); Highways UK (14–15 Oct 2026, NEC Birmingham).

[2] Cyber Security and Resilience (Network and Information Systems) Bill: introduced 12 Nov 2025, carried over into the 2026–27 session (cleared Commons committee stage Feb 2026; completed Commons report stage and third reading June 2026; brought from the Commons to the House of Lords as HL Bill 32 (Lords first reading 17 June 2026), with Lords second reading scheduled for 14 July 2026; Royal Assent not yet granted); amends the NIS Regulations 2018 (expanded scope, faster incident reporting, critical-supplier duties, stronger enforcement); the April 2025 Policy Statement estimates an additional 900–1,100 managed service providers in scope, alongside data centres and large load controllers. Verify current status and final provisions before reliance. The 900–1,100 estimate is from the Cyber Security and Resilience Policy Statement (DSIT, 1 Apr 2025); House of Commons Library CBP-10442.

[3] DfT NIS guidance for transport operators of essential services; NCSC Cyber Assessment Framework (CAF).

Industry / analyst sources

[4] Sector-shift analysis from 2026 event programmes (Commercial Vehicle Show, "Fuelling Change"; Traffex, "Roads. Reality. Results."; Parkex).

[5] Beaming, "Q1 2026 Cyber Threat Report" (an average of 1,988 per day on UK businesses, Q1 2026).

[6] UC Berkeley Center for Long-Term Cybersecurity, "The Cybersecurity Risks of Smart City Technologies" (White Paper, Mar 2021; 2020 survey of 76 experts ranking emergency alerts, street video surveillance and smart traffic signals among the highest-risk assets).

[7] Highways Today, "Cybersecurity Challenges to Secure Smart Highway Infrastructure" (May 2025).

[8] Transport for London cyber security incident (Sept 2024); NCA/NCSC-led response. TfL stated some Oyster card refund data may have been accessed, possibly including bank account numbers and sort codes for around 5,000 customers, who were contacted directly. The ~5,000 figure as reported by BBC News (Sept 2024) and The Register (Sept 2024).

[9] NCSC Annual Review 2025 ("it's time to act"): the gap between the threat to UK critical national infrastructure and the ability to defend it continues to grow, with a dedicated chapter on defending CNI; ransomware assessed as the most pressing threat, with incidents spanning retail, manufacturing and transport.

[10] CVE-2024-38944 (NVD; CWE-94): remote code execution on the Intelight X-1L traffic controller, Maxtime v1.9.6.

[11] VMS / road-sign tampering, Encinitas, California (portable signs altered to show offensive messages).

[12] Poland railway "radio-stop" incident (Aug 2023): roughly 20 trains halted via unencrypted radio commands; two arrests.

[13] Global ITS market sizing varies considerably by scope and methodology. 2026 estimates include Mordor Intelligence (Intelligent Transport Systems Market, USD 36.55bn), Global Market Insights (~USD 54.3bn) and Grand View Research (~USD 62.7bn); confirm current figures before reliance.

CSL internal data

[14] CSL Group internal data, Q4 2025.

Academic & Standards References

The specific claims in this paper are evidenced by the inline citations on the previous page. The peer-reviewed literature and published standards below provide the broader technical and regulatory grounding for resilient ITS connectivity.

Peer-reviewed literature

Lamssaggad, A., Benamar, N., Hafid, A. S. & Msahli, M. (2021). A Survey on the Current Security Landscape of Intelligent Transportation Systems. *IEEE Access*, 9, 9180–9208.

Javed, M. A., Ben Hamida, E. & Znaidi, W. (2016). Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors*, 16(6), 879.

Galego, N. M. C. & Pascoal, R. M. (2022). Cybersecurity in Smart Cities: Technology and Data Security in Intelligent Transport Systems. In *Perspectives and Trends in Education and Technology* (Smart Innovation, Systems and Technologies, vol. 256). Springer.

Standards & frameworks

ETSI TS 102 940 (V2.1.1, 2021). *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.* Cited as background architecture context; this paper makes no claim of ETSI conformance or certification for the CSL security overlay.

GSMA SGP.32. *eSIM IoT specification: remote SIM provisioning for IoT devices.*

ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information security management systems.*

NCSC Cyber Assessment Framework (CAF). See source 3 above.

Related CSL resources

More on resilient, DualCore connectivity from CSL, delivered via the rSIM or a CSL managed router. rSIM product overview: csl-group.com/solutions/rsim. Sector white papers: UK policing, EV charging, warehousing & logistics, and hospitals (shared failure point). eSIM standards (GSMA SGP.32): eSIM, eUICC & iSIM FAQ. Full index: white papers and blog.