CSL

Critical IoT
Connectivity
Experts

Two Networks, One Warehouse | Architecture for Resilient Connectivity

Resilient Connectivity for Warehousing & Logistics

Two networks, one warehouse: why devices outside the main LAN need their own resilient connectivity solutions

Version: 1.3.3

Date: March 2026

1. Two Networks, One Warehouse

EXECUTIVE SUMMARY

Many large-scale warehouse operations now run two distinct networks. The **inner network** (Wi-Fi, WMS, scanners, voice picking) is managed by the customer's IT team. But a growing number of devices are better kept off that main LAN. They need secure, segregated connectivity on an **outer network** (a separate, managed connectivity domain). Budget and ownership for these OT and outer-network systems may sit with IT, estates, facilities, or operations — and is often unclear. Critical devices go un-upgraded because no single team fully owns the connectivity or appreciates the exposure when it fails. Third-party operators (installers, charge-point operators, maintenance providers) also need access to these systems but find it difficult to navigate large-organisation IT departments; because the outer network carries less sensitive customer data than the main LAN, providing controlled third-party access is simpler and lower-risk when it is segregated.

These are the devices CSL® connects: security systems, EV chargers, yard and gate equipment, cold chain sensors, and remote facilities. Each category has a compelling reason for network isolation: compliance, security, operational independence, or all three.

Some organisations can VLAN-segment these onto the existing LAN, but that still leaves shared failure modes, cross-team change control, and broadband dependency. VLANs reduce lateral movement risk but do not, on their own, remove WAN single points of failure.

If you already have SD-WAN and diverse fixed links, this paper helps you decide which outer-network devices require independent cellular cores.

Most warehouse operators are not directly designated as OES (Operators of Essential Services), but that distinction is increasingly irrelevant: regulated customers flow resilience requirements down through supply-chain procurement, making the operator's network architecture, in regulated supply chains, a contractual obligation rather than a voluntary choice. Network segregation aligns with ISO 27001 (A.8.22)[6], UK NIS Regulations 2018, and EU NIS2 where applicable[7].

The decision in brief:
Warehouses increasingly depend on devices that sit outside the main LAN: security cameras, EV chargers, yard gates, cold chain sensors. These devices need connectivity that is segregated, resilient, and managed independently. VLANs reduce lateral risk but, unless you also have diverse WAN paths, you retain shared failure modes. Many MVNO-based cellular backup solutions route through a single hosted core, potentially recreating the dependency they aim to remove: if that core fails, both the "primary" and "backup" SIMs go down together. CSL's Dual-Core architecture removes the shared-core dependency typical of MVNO architectures: two physically separate operator cores with independent control planes and SIM-resident failover: core independence, not just radio diversity.

Key terms: Core network = central infrastructure authenticating SIMs (not the mast). **MVNO core** = a hosted core shared across a SIM estate (architecture varies by provider). **Multi-RAN** = multiple radio networks; **multi-path** = independent cores end-to-end. Multi-RAN with a single core is not multi-path.

What this paper covers:

- The five device categories that need segregated connectivity
- Where every outer-network device sits on a typical warehouse site
- Why Multi-RAN alone does not remove single points of failure
- CSL DualCore, PACE, and DualCom Pro architecture
- Product formats and next steps for engagement

For: Heads of IT, facilities, procurement, and operations managing multi-site warehouse or logistics estates with security, EV charging, cold chain, or yard infrastructure.

5 categories
of devices are covered that benefit from segregated outer-network, hardened, resilient connectivity

Dual-Core
secure end-to-end connections operating on two independent operator cores with failover

Minimum architecture specifications needed for outer-network connectivity:

- ✓ **Dual-Core independence:** two separate operator cores, not profiles on one MVNO core
- ✓ **Router or SIM-resident failover:** no cloud dependency; device switches autonomously
- ✓ **Private APN + VPN:** end-to-end encryption; no public internet transit in the managed design
- ✓ **Full network segregation:** no layer-2 extension to customer LAN

Do you need an outer network?

Life-safety or ARC-signalled systems on site	Yes
EV fleet charging dependent on OCPP backhaul	Yes
Cold chain with regulatory audit trail requirement	Yes
Yard/gate systems beyond the building envelope	Yes
Single warehouse, all devices on managed LAN, no compliance mandate	Evaluate

Control mapping: segregated outer network	
Network segmentation	ISO 27001 A.8.22[6]; no layer-2 extension between networks
Supply-chain resilience	UK NIS Regs 2018 / EU NIS2 Art. 21[7]; independent managed service
Change control isolation	Outer-network changes do not traverse customer IT change windows; third-party operators access segregated systems without IT gatekeeping
Data processing	GDPR Art. 28; segregated management data (CSL may act as processor for certain data where defined contractually)

2. Site Connectivity Architecture

To protect and separate life safety, security and operationally critical assets, parallel, segregated networks are required: i.e. when the LAN goes down, outer-network devices (security, EV, yard, cold chain) keep working because they were never on the site LAN. There is no layer-2 extension between them and therefore their attack surfaces are significantly reduced.

INNER NETWORK
Customer LAN: inside building only

Customer-managed · on-premises · standard IT

WAREHOUSE OPERATIONS

- AP **Wi-Fi / LAN** Floor coverage
- WMS **WMS / ERP** Pick, pack, ship

INFRASTRUCTURE

- LAN **LAN Switches** Core + distribution
- SRV **Local Servers** ERP / WMS host

CONNECTIVITY

- ISP **Customer broadband** Internet / VPN to HQ

Shared dependency
Broadband failure takes everything on the LAN down together

These devices belong on the LAN

OUTER NETWORK
CSL-managed: perimeter, yard & building systems

CSL-managed · segregated from LAN · using secure BB & cellular

1 · SECURITY & LIFE-SAFETY

- **CCTV / ANPR** Perimeter + building
- AC **Access Control** Doors + turnstiles
- FP **Fire Panel** → ARC signalling
- ID **Intruder Panel** → ARC signalling

2 · EV CHARGING

- EV **Fleet Chargers** Depot OCPP (Open Charge Point Protocol) backhaul

3 · YARD & GATE MANAGEMENT

- GT **Gate In / Out** ANPR + barriers
- WB **Weighbridge** Automated capture

4 · COLD CHAIN MONITORING

- T° **Temperature Sensors** Continuous logging

5 · REMOTE FACILITIES

- RF **Outbuildings** Gatehouses, pump rooms, etc

TRAFFIC DESTINATIONS (OFF-SITE)

- **ARC** Alarm Receiving Centre
- **CSL Platforms** Management & Monitoring

Key principle: These networks share a physical site but have no shared network infrastructure, no shared LAN addressing domain, and no routine transit between them (no LAN backhaul; no L2 adjacency). All outer-network devices connect via CSL's DUAL-CORE cellular cores (Core A + Core B), with PACE (BB + Core A + Core B + SAT) at the Outpost. Traffic is Private APN segregated + VPN encrypted.

Figure 1: Conceptual view: inner network (customer LAN) and outer network (CSL) operate as parallel, independent systems.

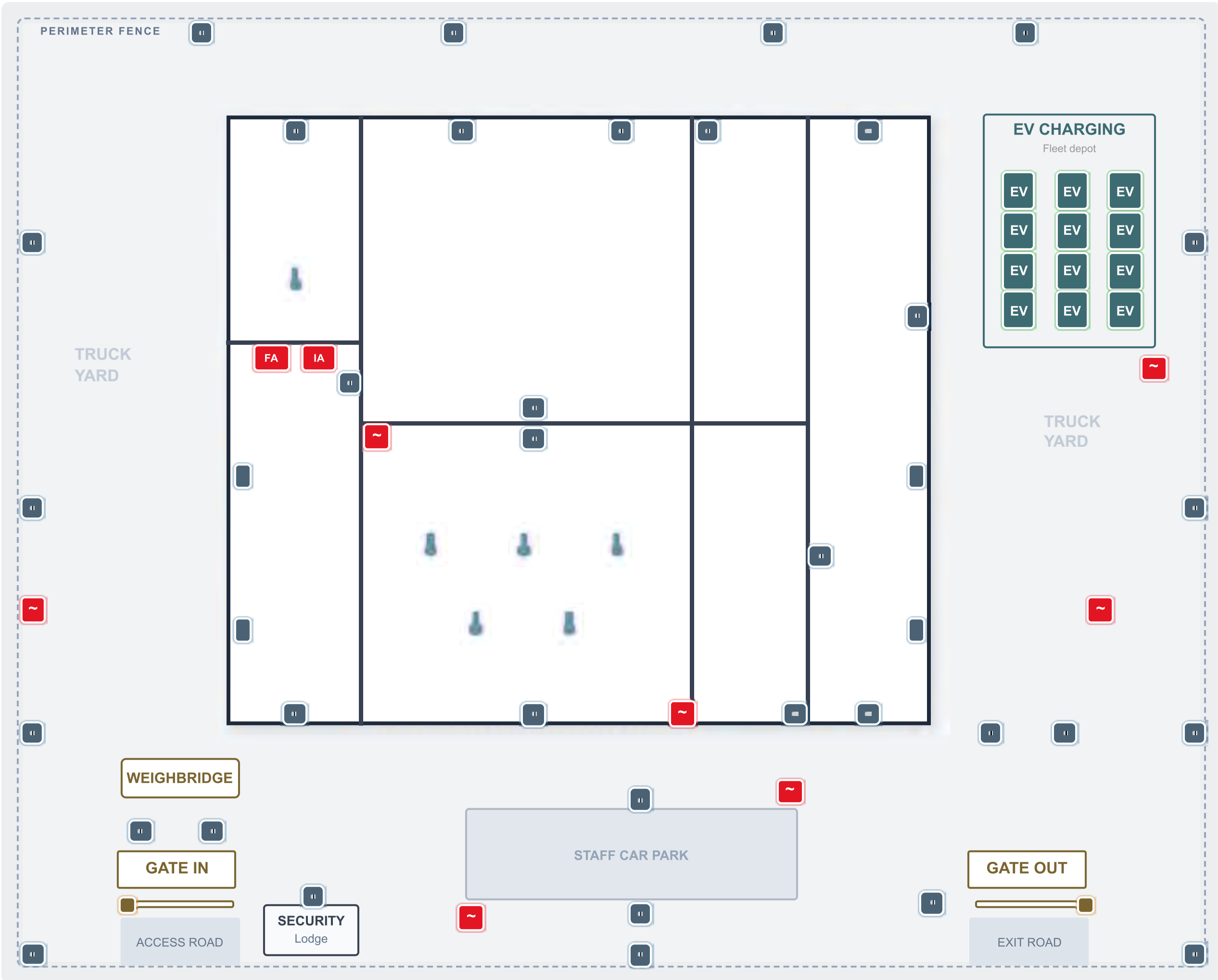
An example typical 40-door DC profile:

60 CCTV/access points · 12 EV chargers · 2 gate/ANPR systems · 150 cold chain sensors · 3 remote outbuildings

3. Where CSL Connects

Every coloured marker in the figure below is a device on CSL's segregated outer network: off the customer inner network LAN, connected via Dual-Core cellular with Private APN + VPN protection. Colours indicate the device categories.

All illustrated endpoints → CSL Dual-Core cellular (Private APN + VPN) → ARC & CSL Platform · No path through customer LAN



CSL Outer Network Endpoints All devices segregated from customer LAN · Connected via Dual-Core cellular (Private APN + VPN)

- **Life-safety**: FA Fire / Intruder; Thermal
- **Surveillance**: CCTV / ANPR; Access control
- **Yard / Gate**: GATE Gate; Weighbridge
- **Cold Chain**: Temp sensor
- **EV Charging**: EV EV charger
- **Remote Facility**: Satellite depots with standalone connectivity

4. The Network Architecture Gap

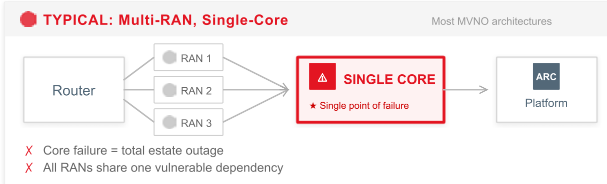
Every device shown on the site diagram on the previous page (Figure 2) requires a WAN path back to its platform or ARC, and that outer network requires its own resilient connectivity, not a shared broadband connection. But many cellular backup offerings, particularly MVNO-based designs, often route traffic through an unprotected **single hosted core**[3], potentially recreating the shared dependency they aim to remove.

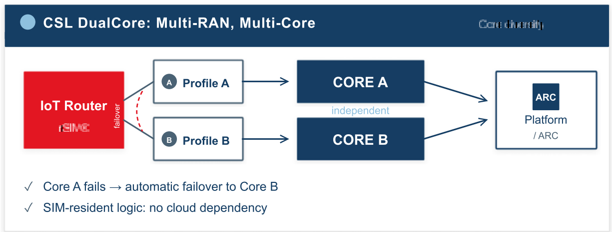
The diagram opposite illustrates the difference. Multiple radio access networks converging on one core is multi-RAN, not multi-path. Resilience requires **core independence**: two physically separate operator cores with independent control planes and SIM-resident failover.

> **If you already have cellular backup:** check whether your provider routes through a single hosted core[3]. A core-level incident can take down the connected estate simultaneously. **The question to ask:** "*Do all our SIMs route through one hosted core network? If that core fails, what fails over, and who controls it?*" If the answer involves waiting for an upstream operator to restore service, you have multi-RAN but not multi-path.

Architecture comparison

Architecture	Failure mode	Core diversity	Recovery
Single LAN (broadband)	WAN outage disables all devices incl. security	None	ISP-dependent
LAN + cellular (single-core MVNO)	Shared core[3]; core failure takes all SIMs down	No	Hours+
CSL Dual-Core outer network	**Independent cores; SIM-resident failover**	**Yes: always**	**Autonomous**





[3] MVNO architectures typically route all SIM profiles through a single hosted core network; if that core fails, all connected SIMs lose service simultaneously regardless of radio-access diversity. Architectures vary by provider; ask for a core-network topology diagram and confirm core-level failover ownership. Core outage recovery can take hours or longer depending on root cause and upstream provider. Uptime Institute (2024) identifies network-related issues as the leading category of IT service outage causes.

[4] HPE Aruba, Warehouse Wi-Fi Best Practices (2025), §3.

[5] HPE Aruba Networking, *Warehouse WLAN Design & Deployment Guide*, TechDocs, 2025: environmental factors including racking, temperature-controlled zones, and inventory variability.

5. Why Architecture Matters for the Outer Network

Segregated devices need independent failover

Security systems need to reach the ARC during a broadband outage; that is their entire purpose. EV chargers need to maintain fleet charging schedules when the site Wi-Fi is down. Cold chain sensors require continuous data trails for compliance. These devices need connectivity that **operates independently of the warehouse LAN** and fails over autonomously.

A Scenario: 14:00, broadband or core cellular networks fail
CCTV and access control go dark. ANPR gates stop reading plates; HGVs queue. EV chargers lose OCPP connectivity. Cold chain sensors stop reporting. The ARC loses its primary signalling path. The IT team has no visibility or prioritisation of these outer-network devices — their budget may sit with estates or facilities, firmware upgrades stall because no single team owns them, and the third-party installer who needs remote access cannot get past the corporate IT gatekeeping process.

With DualCore: When a path failure is detected, each device first attempts local RAN alternatives on its current profile. If local recovery is not possible, the device switches to its second core profile autonomously. Security signalling restores. Gates resume. Cold chain data continues unbroken. No ticket raised, no site visit, no dependency on the broadband provider's repair timeline.

Outdoor and perimeter challenges

Many outer-network devices sit beyond the building envelope: ANPR cameras, weighbridges, yard kiosks, gate readers, EV chargers, perimeter CCTV. These locations are cellular-primary by necessity, using external antennas on routers that serve localised device clusters. Metal cladding, loading dock openings, and seasonal stock movement all affect RF propagation[4,5].

With CSL's Dual-Core architecture, a cellular path failure triggers a graduated recovery sequence: the device first exhausts available local RAN alternatives before switching to its alternate core profile autonomously, with no manual intervention, no site visit, and no dependency on the customer's IT team.

CSL product formats for the outer network

CSL provides six product formats spanning SIM-level failover, dedicated alarm signalling, managed routers, multi-radio hub devices, fixed-line broadband, and LEO satellite, covering every layer of PACE architecture frameworks (Primary, Alternate, Contingency, Emergency).

Each product and service format delivers Dual-Core connectivity on a segregated network. This means that you can deploy by device category, starting with the highest-priority zones. Installation is seamless and typically no complex new cabling is required.

See next page for the full product range →

6. The CSL Product Range

CSL provides six product formats for the warehouse outer network: from SIM-level failover to LEO satellite. Each delivers Dual-Core connectivity on a segregated network, managed end-to-end by CSL.

rSIM®

All device categories

eUICC SIM with dual operator profiles and SIM-resident failover logic. Drop-in for existing cellular routers and IoT gateways. Supports sgp.32 OTA profile management.

Serves: security, EV, yard, cold chain, remote systems and vehicles

DualCom Pro range

Security & life-safety

Dedicated alarm signalling devices (including GradeShift Pro dual-path) connecting fire and security panels to ARCs via CSL's Gemini Global Platform. Dual-path up to DP4, multi-network WorldSIM.

Serves: fire panels, intruder panels, heat-detection camera signalling

IoT Routers

Multi-category site connectivity

Fully managed, remotely monitored site routers with built-in Dual-Core. Serve localised device clusters for security systems, EV chargers, yard equipment, and remote-site backhaul.

Serves: EV chargers, yard kiosks, CCTV clusters

CSL Outpost

Hub sites (multi-category)

Quad-radio design with up to four independent 4G/5G modules, delivering PACE-level redundancy for hub sites aggregating multiple device categories across a single managed appliance.

Serves: large DCs with 3+ device categories

CSL Broadband

Primary layer (PACE)

Fully managed fixed-line broadband on a segregated network with static IP, business-grade SLAs, and built-in cellular failover. The Primary layer in a PACE deployment.

Serves: primary WAN for outer-network traffic

CSL Satellite

Emergency layer (PACE)

LEO satellite connectivity for remote or coverage-constrained sites. The Emergency layer in PACE, independent of all terrestrial infrastructure. Provides last-resort backhaul when cellular is unavailable.

Serves: remote depots, coverage gaps

PACE architecture: **P**rimary (CSL Broadband) + **A**lternate (MultiRAN Core A cellular) + **C**ontingency (Multi-RAN Core B cellular) + **E**mergency (LEO satellite). Each layer is bonded or independent. The Outpost delivers all four in a single managed appliance; CSL Routers and rSIM and can provide the Primary, Alternate and/or Contingency layers as secured and resilient drop-in upgrades to existing infrastructure.

rSIM®
Dual-Core SIM

DualCom Pro 4
Alarm signalling

IoT Router
Site connectivity

CSL Outpost
Multi-radio hub

Physical footprint: a router or SIM swap per device category. No new cabling, no rack space beyond the existing comms cabinet.

7. Next Steps

Every warehouse has devices that should not sit on the main IT network, and are often prohibited by security policy from doing so. CSL provides the segregated, resilient outer network for these devices as a fully managed service — removing the need for any internal team, whether IT, estates, or facilities, to own and maintain additional connectivity infrastructure, and giving third-party operators a straightforward path to the systems they service.

1. Discover

We help you review your current device estate, identify which categories need segregated connectivity, and map shared dependencies. Typically 1 to 2 weeks, no commitment is required.

2. Size

Share your site count, device categories, and compliance requirements. We'll assess your estate and deliver a zone map per site, a dependency register, and a resilience business case.

3. Protect

Deploy by device category, starting with the highest-exposure zones first. No new cabling, no rack space beyond the existing comms cabinet. rSIM drops into existing routers, or deploy fully managed CSL IoT Routers and Outpost hubs for new installations. DualCom Pro replaces or upgrades existing alarm signalling devices.

We'll identify which devices need an outer network, map the dependency risk, and recommend the right deployment path for your estate.

Get in touch

Web: csl-group.com/contact-us
Email: sales@csl-group.com
Phone: +44 (0) 1895 474 474

For detailed cost-of-downtime modelling, zone-level exposure analysis, and procurement-ready ROI figures, see the full white paper: Resilient Connectivity for Warehousing & Logistics (v3.27).

About CSL Group

CSL Group is a UK and EU-based telecommunications company specialising in resilient connectivity for critical IoT applications. With over **3.5 million active SIM subscriptions**[8] (UK and European IoT estate, Q4 2025) and VPN + private APN infrastructure, CSL provides the segregated outer network for devices that should not share the main LAN: security systems, EV chargers, cold chain sensors, and remote-site infrastructure.

Why CSL

Genuine core independence: Two separate operator cores, not multiple profiles routed through a shared MVNO core

3.5M+ active SIM subscriptions[8]: Proven at scale across critical-infrastructure verticals (UK and European IoT estate, Q4 2025)

Private APN / VPN: Segregated connectivity with end-to-end encryption; no public internet breakout in the managed design

Single managed service: Connectivity, failover, monitoring, and OTA lifecycle management in one contract

Heritage advantage: CSL securely connects to private ARC VPN infrastructure across 270+ European locations[8], purpose-built for life-safety signalling

Sources & notes: [3] Uptime Institute (2024), network-related issues as leading IT service outage category. MVNO core architectures vary by provider; verify with a topology diagram and confirm core-level failover ownership. [4] HPE Aruba, *Warehouse Wi-Fi Best Practices* (2025), §3. [5] HPE Aruba Networking, *Warehouse WLAN Design & Deployment Guide*, TechDocs, 2025. [6] ISO/IEC 27001:2022, Annex A Control 8.22: Segregation of networks. [7] Directive (EU) 2022/2555 (NIS2), Art. 21; UK NIS Regulations 2018, Reg. 10. Applicability is sector- and supply-chain-dependent; consult your compliance team. [8] SIM subscription and infrastructure figures are CSL Group internal data (Q4 2025).