ERICSSON

Checklist: Deploying 5G and network security for mass transit operations

For public transportation agencies, 5G connectivity is crucial for delivering safe, efficient, and passenger-friendly services. From route tracking and fare collection to customer Wi-Fi and security cameras, IT managers must ensure networks can handle the demands of modern transit systems. This checklist outlines the essential steps and considerations for a successful 5G deployment supporting mass transit fleets.

Key questions to consider

- ☐ What is the objective for implementing 5G in transit vehicles (e.g., providing passenger Wi-Fi, improving route tracking, and connecting POS, video surveillance, and digital signage)
- ☐ What metrics and benchmarks must the system deliver for it to be considered a success?
- ☐ Can the network handle the increased traffic from passenger Wi-Fi, telematics, POS, digital signage, and HD video?
- ☐ Which applications — such as real-time route tracking, contactless fare collection, and emergency communications — are most critical to support?
- ☐ How does the agency plan to securely scale with additional vehicles or new applications such as digital ticketing, AVLs, and rider engagement apps?
- ☐ How will the IT team manage in-vehicle devices, including hardware/software refreshes, zero-touch provisioning, and troubleshooting?
- ☐ How will security (multi-layered, zero trust, and intrusion detection/prevention) scale with network growth?
- ☐ What's the worst-case outage or security scenario (e.g., loss of POS or video feeds) and how would it be mitigated?

Best practices

- Gather input from all stakeholders for alignment (IT, fleet ops, procurement, and safety/security teams).
- Treat network security as a foundational part of planning.
- Don't rely only on in-house generalists; work with trusted partners/vendors for deployment and ongoing management.
- Assess whether legacy systems can support 5G applications or if a refresh is needed.

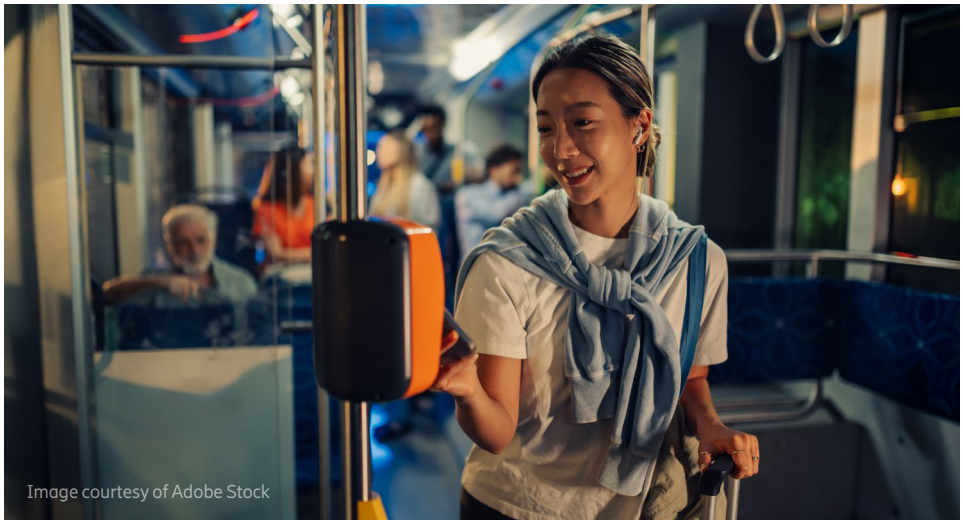


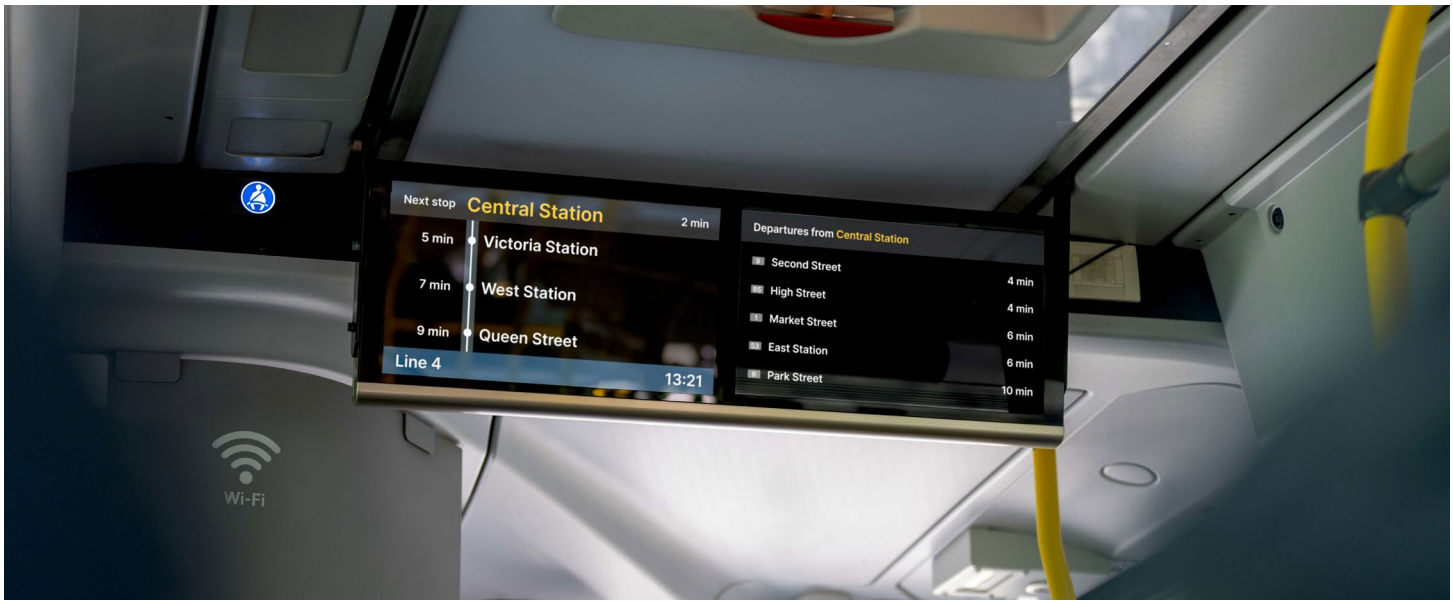
Image courtesy of Adobe Stock

Quick check:

Do you have a complete solution in place to ensure constant connectivity and secure communications across your mass transit fleet?

Data and network security	Need to address	Solution in place
Ability for 3rd party IT and contractors to access the network securely		
Encrypted data transmissions		
Enforce zero trust security across all devices and endpoints		
Implement cloud-based content filtering for rider Wi-Fi		
Isolate fare/payment data from passenger Wi-Fi and other traffic		
Run IDS/IPS technologies to minimize attack points		

Networking equipment	Need to address	Solution in place
Automate router power on/off with vehicle ignition		
Deploy ruggedized, 5G/LTE vehicle routers able to withstand shock, vibration, and temperature		
Enable dual-modem failover for seamless coverage across multiple carriers		
Install external, vehicle-mounted antennas optimized for 5G bands		
Monitor vehicle locations and cellular health of the devices		
Support for Ethernet and Wi-Fi as WAN; dual-band concurrent Wi-Fi		



Network management	Need to address	Solution in place
Centralize cloud-based network management and analytics		
Enable remote configuration, troubleshooting, and updates		
Monitor onboard connected devices remotely		
Monitor real-time vehicle location and signal strength by route		
Simplify fleet-wide changes with configuration groups		

Rider and operational use cases	Need to address	Solution in place
Deliver digital signage connectivity and real-time service updates		
Provide passenger Wi-Fi capacity for 100+ clients		
Provide reliable connectivity for driver tablets and apps		
Secure POS and fare payment processing		
Stream HD video from onboard surveillance cameras		
Support real-time GPS/AVL, telematics, and route optimization		

Learn more about enterprise wireless solutions