



D4.1 Mobility Use Cases Report: Analysis of Cross-Border 5G and MEC Challenges

Issues and Challenges of 5G edge and distributed cloud integration for European corridors and smart communities

Type: Document, report

Dissemination Level: Public

Table of Contents

1	Executive Summary	2
2	Introduction	4
3	Requirements and Challenges from the Mobility Use Case Perspective .	6
3.1	OVERVIEW OF USE CASES AND DEPLOYMENT SCENARIOS.....	6
3.2	REQUIREMENTS OF MOBILITY USE CASES.....	7
3.3	CHALLENGES RELATED TO CONNECTIVITY & COMPUTE INFRASTRUCTURE	9
4	Landscape of EU Edge and MEC Providers	12
4.1	EDGE LANDSCAPE DIMENSIONS	12
4.2	ACTIVITIES AND OFFERINGS OF KEY EUROPEAN MEC PLAYERS.....	13
4.3	TECHNOLOGICAL PREREQUISITES AND DRIVERS OF MEC ADOPTION.....	17
5	Challenges for pan-European MEC Rollout.....	22
5.1	POLITICAL FACTORS.....	23
5.1.1	<i>Political Challenges in 5G Corridors</i>	<i>23</i>
5.1.2	<i>Political Challenges in Smart Communities</i>	<i>24</i>
5.2	ECONOMIC FACTORS.....	24
5.2.1	<i>Economic Challenges in 5G Corridors</i>	<i>24</i>
5.2.2	<i>Economic Challenges in Smart Communities.....</i>	<i>26</i>
5.2.3	<i>SOCIAL FACTORS.....</i>	<i>26</i>
5.2.4	<i>Social Challenges in 5G Corridors</i>	<i>26</i>
5.2.5	<i>Social Challenges in Smart Communities.....</i>	<i>27</i>
5.3	TECHNOLOGICAL FACTORS	28
5.3.1	<i>Technological Challenges in 5G Corridors</i>	<i>28</i>
5.3.2	<i>Technological Challenges in Smart Communities</i>	<i>30</i>
5.4	LEGAL FACTORS	31
5.4.1	<i>Legal Challenges in 5G Corridors</i>	<i>31</i>
5.4.2	<i>Legal Challenges in Smart Communities.....</i>	<i>32</i>
5.5	ENVIRONMENTAL FACTORS	32
5.5.1	<i>Environmental Challenges in 5G Corridors</i>	<i>32</i>
5.5.2	<i>Environmental Challenges in Smart Communities.....</i>	<i>33</i>
5.6	SYNTHESIS: CHALLENGE MAPPING TO PESTLE & STAKEHOLDER	34
5.7	REFERENCES.....	37

1 Executive Summary

Connected, Cooperative, and Automated Mobility (CCAM) and advanced mobility services represent some of the most demanding application domains for 5G and Multi-access Edge Computing (MEC). Previous project deliverables have demonstrated that many of these use cases can only be realized at scale if compute and connectivity are tightly integrated and deployed close to end users and infrastructure. Building on this foundation, this report summarizes the previously shown mobility-driven use cases and their technical and operational requirements and highlights the small extend and fragmentation of the current European edge and MEC landscape, and the systemic challenges that prevent the emergence of a truly pan-European edge infrastructure.

From a use-case perspective, the report focuses on high-impact mobility scenarios such as cooperative driving functions, collision avoidance, emergency vehicle alerts, Green Light Optimal Speed Advisory (GLOSA), platooning, real-time traffic management, and cross-border automated driving along European transport corridors. These use cases are characterized by mobility across large geographic areas, frequent transitions between networks and countries, and strong dependencies on real-time data exchange between vehicles, infrastructure, and backend systems. Compared to geographically bounded smart community applications, mobility use cases impose significantly higher and more heterogeneous demands on both network and compute infrastructure.

The requirements derived from these use cases can be grouped into deployment, technical, and service-level dimensions. Key deployment requirements include continuous coverage along corridors, support for multi-operator roaming with fast handover, multi-network redundancy for mission- and safety-critical services, and edge compute placement that follows user mobility. Technically, many mobility applications require ultra-low and predictable latency, high reliability (up to “five nines” for safety functions), flexible throughput ranging from small safety messages to high-bandwidth data streams, and advanced capabilities such as precise positioning, geofencing, network slicing, and local breakout. On the service level, stringent requirements apply to latency, reliability, security, and quality of information, particularly for safety-related use cases where delayed, incomplete, or inaccurate information can have severe consequences.

Against these requirements, the European edge and MEC landscape is still in a transitional phase. While several major mobile network operators have deployed MEC capabilities nationally - often in partnership with hyperscalers or through proprietary edge platforms - Europe lacks a mature, widely available, and interoperable pan-European MEC offering. Deployments range from private and on-premise MEC for industrial use cases to public, network-integrated MEC in selected metropolitan areas. Architecturally, the landscape is fragmented, with different operators pursuing hyperscaler-based MEC, sovereign telco edge solutions, or hybrid approaches. Although initiatives such as standardized network APIs, open-source platforms, and operator federations are emerging, commercial MEC availability remains limited in geographic scope and inconsistent across countries.

The report identifies a comprehensive set of challenges that explain why current MEC deployments fall short of mobility use-case needs and why a pan-European infrastructure has not yet materialized. Politically and institutionally, fragmented spectrum policies, divergent coverage obligations, and the absence of cross-border governance and cost-sharing frameworks hinder coordinated corridor deployments. Economically, high deployment costs, unclear and often negative business cases, immature revenue models, and the loss of traditional roaming revenues reduce operators' incentives to invest. Social factors such as public skepticism toward automated driving, data privacy concerns, and resistance to new infrastructure further slow progress. From a technological perspective, delayed rollout of 5G Standalone, non-functional cross-border roaming architectures, fragmented MEC platforms, and immature orchestration and slicing capabilities prevent seamless service continuity. Legal and regulatory uncertainties - particularly around data sovereignty, liability, and cybersecurity - add further complexity, while environmental constraints related to energy consumption, site construction, and sustainability increasingly influence deployment decisions.

2 Introduction

In previous deliverables of this project, we have explored a variety of potential use cases within the Connected, Cooperative, and Automated Mobility (CCAM) and broader mobility domains, as detailed in D3.1. Our findings demonstrated the advantages of leveraging edge computing and Multi-access Edge Computing (MEC) to meet the demanding requirements of these use cases. Building on this foundation, Deliverable D3.2 provided an overview of possible implementation scenarios, highlighting how these technologies can be effectively deployed in real-world environments.

This document extends the prior analysis by examining the specific requirements associated with mobility use cases and their implementation scenarios. Drawing upon the EU Connecting Europe Facility (CEF) initiative and its funded projects in mobility and smart communities, concrete examples include cross-border 5G corridors for automated vehicles, real-time traffic management, and smart community applications such as intelligent emergency response and environmental monitoring. In parallel, the 5G Automotive Association (5GAA) has contributed substantial analysis on the integration of MEC and CCAM, emphasizing interoperability, ultra-low latency, and the tight coupling of compute and connectivity for mission-critical applications.

A key contribution of our 5GMEC4EU project is its use-case-driven approach. We build on real mobility scenarios – such as cross-border automated driving, cooperative traffic services, and corridor-based safety applications – to derive concrete requirements for connectivity, compute placement, orchestration, and service exposure. These scenarios highlight that mobility use cases differ fundamentally from traditional smart community applications: they are highly dynamic, geographically distributed, and safety-critical, requiring predictable performance across long distances, multiple networks, and national borders. As a result, they expose limitations in today's predominantly national and fragmented MEC deployments.

Based on these insights, we have investigate implementation models for MEC along European corridors and in smart communities, including public MEC integrated into mobile networks, private and hybrid MEC deployments, and emerging federation concepts that allow applications to span multiple operator domains. Our work also examines how enabling technologies – such as 5G Standalone, local breakout, network slicing, standardized network APIs, and edge orchestration – can be combined to meet the stringent requirements of CCAM services in practice. This is highlighted in D3.2. In doing so, our work provides a reality check on the maturity of current solutions and identifies gaps between standardization, pre-commercial trials, and deployable production systems.

To this end, this paper identifies the existing and emerging edge and MEC providers in the European landscape and investigates the complexities involved in establishing a unified, pan-European Edge-Cloud infrastructure accessible to all use case developers. Building on the technical work and stakeholder engagement conducted within 5GMEC4EU, the challenges encountered are assessed from technical, regulatory, and business perspectives. Particular attention is given to cross-border deployment barriers, fragmented spectrum and coverage obligations, immature

federation and roaming architectures, unclear business models, and governance issues that hinder coordinated investment.

By linking the empirical findings of the 5GMEC4EU project with external research, standardization activities, and comparable European initiatives, this document provides context and relevance for the requirements, landscape analysis, and challenge synthesis presented in the subsequent chapters. Ultimately, it aims to support policymakers, infrastructure providers, and ecosystem stakeholders in understanding why pan-European MEC remains difficult to realize today – and what conditions must be met to enable scalable, interoperable edge solutions that can support Europe’s future mobility and smart community ambitions.

3 Requirements and Challenges from the Mobility Use Case Perspective

3.1 Overview of Use Cases and Deployment Scenarios

As pointed out in previous works, there is plethora of use cases which are relevant in the CEF project context (see Deliverable 3.1). The following list is a summary of major use case categories with their individual functionalities. The analysis of challenges later in this paper will be based on these categories.

Category	Key Functions & Examples
Probe Vehicle Data (A)	Traffic data collection, event detection, reporting vehicles in distress
Road Works Warning (B)	Alerts for lane closures, operator vehicles, winter maintenance, automated vehicle warnings
Signage Applications (C)	In-vehicle dynamic speed limits, toll station information, enhanced driver orientation
Hazardous Location Notifications (D)	Alerts for slippery roads, obstacles, accidents, reduced visibility, emergency braking
Traffic Information & Smart Routing (E)	Real-time traffic updates, rerouting, smart points of interest, travel time estimation
Parking, Park & Ride, Multimodality (F)	Parking availability, public transport schedules, modal transfer advice, car-sharing
Intersections (G)	Green Light Optimal Speed Advisory (GLOSA), intersection violation warnings, in-vehicle signage at merges
Traffic Management (H)	Dynamic lane management, traffic bans, variable speed limits, non-autonomous zone notifications
Vulnerable Users (I)	Pedestrian warnings, road worker alerts, protection for users at public transport stops
Logistics (J)	Estimated time of arrival, dock reservations, optimal truck routing, terminal guidance
Level Crossing (K)	Warnings for malfunctioning/closing level crossings, detection of vehicles in critical areas

Law Enforcement (L)	Identification of vehicles of interest, law enforcement vehicle status, automated driving system monitoring
Payment Services (M)	Toll station or parking payment services
Remote Services (N)	Remote maintenance and monitoring

If one wants to implement use cases in these clusters, there are a few deployment scenarios which are relevant in a real-world setting.

Urban:

Dense edge node deployment for high data demand and complex interactions. Focus on integration with public transport and vulnerable road users.

Highway/Corridor:

Edge nodes at intervals for continuous coverage and low latency. Emphasis on high-speed cooperative maneuvers platooning and automated logistics.

Cross-border:

Interconnected MEC nodes for seamless handover between countries/operators. Address regulatory, technical, and operational challenges for seamless service continuity, roaming, and interoperability.

Each of these scenarios needs to be supported by the connectivity and compute infrastructure. The resulting requirements are shown in the next section.

3.2 Requirements of Mobility Use Cases

Mobility use cases generally have the highest requirements on connectivity and compute, compared to smart community use cases, which are geographically bounded. Once a MEC installation fulfills those stringent CCAM requirements, other use cases are as well covered.

The requirements of CCAM and mobility use cases can be clustered in three broad categories:

1. Deployment or operational requirements
2. Technical and functional requirements
3. Service level requirements

Deployment Requirements

- **Geofencing:** Essential for location-specific alerts such as road work warnings and environmental zones.

- **Multi-Network Redundancy:** Mandatory for mission-critical services (e.g., railway crossings), ensuring service continuity even if one network fails.
- **Multi-Operator Roaming:** Required for cross-border mobility, enabling handover between operators within one second to maintain service continuity.
- **Predictive QoS:** Anticipates network conditions to ensure consistent performance for critical applications.
- **Edge Computing:** Edge computing for localized decision-making can benefit from technologies like Local Break Out, 5G-Slicing and facilitates the growing convergence of AI, Edge Computing, and 5G networks.
- **Precise Positioning:** Enhances safety-critical applications like collision avoidance by providing accurate vehicle location data.

Technical and Functional Requirements

- Latency: Ultra-Low Latency (<20ms) critical for collision prevention (EVA, emergency brake light), tolerant for road condition reports (< 1 s). (Spikes are not a real issue, many messages will follow up)
- Throughput: Highest for HD map updates (50–100+ Mbps) and crowdsourced data, lowest for basic safety alerts (1–5 Mbps).
- Geofencing: essential for Road work warnings, environmental zones, and location-specific alerts.
- Multi-Network Redundancy: Mandatory for mission-critical services like railway crossings.
- Reliability: Mission/safety-critical services (e.g. V2V Safety, GLOSA) require 99.999% uptime. Non-safety services (e.g., traffic flow data) tolerate 99.9%.
- Multi-operator roaming for cross-border continuity (handover within 1 sec).
- Predictive QoS: Ensures consistent performance by anticipating network conditions
- Cybersecurity: Protects sensitive V2X communications from cyber threats
- Edge computing for localized decision-making can benefit from technology like Local Break Out, 5G-Slicing and facilitates the growing convergence of AI, Edge Computing, and 5G networks.
- Also to consider Precise Positioning: Enhances safety-critical applications like collision avoidance.

Service Level Requirements

- **Quality of Information (QoI):** In general, independent of the communication channel, information exchanged must be timely, appropriate, reliable, accurate, complete, concise, and secure. For safety use cases, vehicles must receive precise and up-to-date information about nearby vehicles, road hazards, and traffic signals.
- **Latency:** The time from event occurrence to actuation, including both data processing and communication, must be minimized. For collision avoidance, end-to-end latency should be 100 ms or less to enable timely vehicle reactions. Ultra-low latency (<20 ms) is critical for immediate safety functions, while less urgent data (e.g., road condition reports) can tolerate up to 1 second.
- **Data Rate and Message Size:** Safety messages typically range from 300 to 1400 bytes, depending on the number of detected objects and event types. Throughput requirements are highest for applications like HD map updates (50–100+ Mbps) and lowest for basic safety alerts (1-5 Mbps).
- **Range:** Communication range requirements can extend up to 300 meters in highway scenarios to provide sufficient reaction time at high speeds.
- **Reliability:** Mission- and safety-critical services, such as V2V safety and Green Light Optimal Speed Advisory (GLOSA), require extremely high transmission reliability of the communication channel, often above 99.999% uptime. Non-safety services, like general traffic flow data, can operate with 99.9% reliability.
- **Security:** Ensuring data integrity and privacy is mandatory, especially for safety-critical and regulatory-compliant applications. Cybersecurity measures are essential to protect sensitive V2X communications from threats.

3.3 Challenges related to Connectivity & Compute Infrastructure

The implementation of the above scenarios is dependent on significant prerequisites which have to be fulfilled. This poses challenges on many levels for a pan-European deployment, e.g., technical and organizational levels. The key insights from our interactions with stakeholders are summarized below.

CCAM and Mobility Use-Case Challenges

- **Cross-Border Handover and Interoperability:** Ensuring application-level and network-level session continuity as vehicles cross national borders is a major hurdle, requiring rapid and reliable handover between different operators' networks and national infrastructures. Diverse network architectures, PLMN (Public Land Mobile Network) interconnections, and differences in hardware and protocols exacerbate this challenge.

- **Roaming and Multi-Operator Federation:** Seamless service across operators depends on harmonized roaming agreements, standardized APIs/interfaces, and MEC federation—allowing edge resources and services to be transferred or federated as vehicles move between operators or countries. Lack of standardization slows progress and adds complexity.
- **Regulatory and Data Privacy Constraints:** Differences in regulatory regimes, spectrum policies, and data privacy requirements (especially EU vs. non-EU) hinder the flow of critical vehicle and mobility data, complicating compliance and data-sharing across borders.
- **Diverse CAM Application Requirements:** Use-cases (e.g., collision avoidance, platooning, hazard warnings, high-definition map updates) have dramatically different requirements for reliability, latency, and throughput, which stretch current network design and force trade-offs between universal coverage and high network performance.
- **Edge/Cloud Continuum and Orchestration:** Continuous service in mobility scenarios depends on dynamic orchestration across the cloud-edge continuum. Lack of unified orchestration approaches and limited interoperability between edge platforms/providers hinder low-latency, reliable service delivery across regions.
- **Legacy Integration and Migration:** The transition from 4G/LTE to 5G, and integration of legacy roadside and vehicle units, results in fragmented connectivity, unpredictable service continuity, and additional operational complexity.
- **Cybersecurity & Trust:** V2X communications, particularly those critical for safety, require robust, harmonized authentication, encryption, and data integrity mechanisms to ensure reliable and lawful operation across ecosystem partners.

Existing and Future 5G Corridor & Smart Community Connectivity Challenges

- **Continuous High-Quality Coverage:** Achieving uninterrupted 5G coverage along long corridors and in cross-border or low-density regions remains challenging; gaps persist due to topography, infrastructure limitations, and varying degrees of operator investment.
- **Capacity and Traffic Surge Planning:** Real-time, safety-critical services (especially for level 3+ autonomous vehicles) can saturate available capacity—requiring sophisticated, adaptive planning and potentially dense site deployment in some locations.
- **Network Slicing and Resource Allocation:** Slicing is essential for supporting heterogeneous CCAM requirements, but managing slices with predictable QoS across diverse operators and geographies remains an open operational and technical challenge.

- **MEC Placement and Orchestration:** Placing MEC nodes to balance coverage, latency, and resiliency, while ensuring efficient orchestration and cost control, is non-trivial. Coverage, capacity, and performance must be dynamically optimized for variable traffic and use-case demand.

Business, Financial, and Institutional Challenges

- **Non-Harmonized Investment and Cost Sharing:** Different deployment incentives, funding mechanisms (e.g., CEF, public-private), and cost models among operators, road authorities, and other stakeholders lead to fragmented infrastructure and service availability.
- **Undefined Revenue Models:** Monetization strategies for CAM services are not yet mature. The value split between infrastructure providers, OEMs, and service/content providers is unresolved, leading to business uncertainty and slower innovation uptake.
- **Stakeholder Coordination:** Multi-party collaboration is vital for shared infrastructure, data, and operational models, but aligning interests and ensuring fair risk/reward sharing remains difficult, especially across borders and administrative boundaries.

4 Landscape of EU Edge and MEC Providers

4.1 Edge Landscape Dimensions

Architectural Strategies: Distributed MEC vs. Sovereign Edge

MEC only functions as intended when it is deployed directly within the telecommunications provider's network and close to end users, such as factory machines or connected vehicles. If the infrastructure is not located within the telecommunications provider's network, it is referred to as edge computing instead. An overview of possible locations within the network can be found in Figure 1.

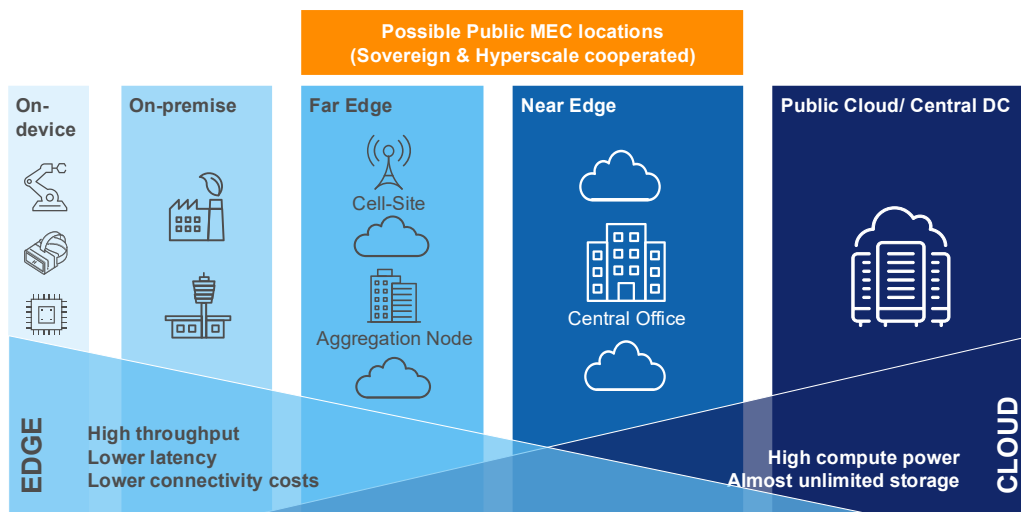


Figure 1: Edge versus Cloud locations along the telco network

The distinction between Public MEC and Private MEC is primarily determined by factors such as infrastructure location, network configuration, and access permissions. The following outlines these differences clearly:

Private MEC (also known as "Dedicated MEC" or "On-Premise MEC")

- **Location:** The edge computing infrastructure (servers and data storage) is physically **installed directly on the premises** of a company (e.g., in a factory hall, a hospital, or on a farm).
- **Network:** Private MEC is typically combined with a private 5G campus network (Mobile Private Network, MPN). These networks can operate completely independently or be configured as a separate, private "slice" of a public network.
- **Usage:** The infrastructure is **exclusively dedicated for the sole use of this one company**.

- **Benefits and Use Cases:** The greatest advantage is complete control over the data, as sensitive information does not have to leave the premises (maximum data sovereignty and privacy). It also enables extremely low latency (e.g., 3 to 4 milliseconds), which is essential for highly critical industrial applications such as autonomous mobile robots (AMR), machine vision for quality control, or predictive maintenance.

Public MEC (also known as "Distributed MEC" or "Mobile Edge")

- **Location:** The computing power is **deeply embedded in the public 4G/5G mobile network of the telecommunications provider**. The servers are not at the customer's site, but at network nodes, base stations, or in regional data centers of the telcos (often in partnership with cloud providers like AWS or Google Cloud).
- **Network:** It uses the regular, public mobile network.
- **Usage:** It is a **shared infrastructure**. App developers, various companies, and end users with smartphones or connected devices can simultaneously access these edge resources.
- **Benefits and Use Cases:** Public MEC provides very broad geographic coverage ("Broad Reach"). It is ideal for devices that are mobile ("Off-premise devices" such as connected and autonomous cars) or for users at public places like amusement parks, transportation hubs, or stadiums. It brings cloud applications closer to the mobile end user without the need to set up a dedicated private network.

In summary: Private MEC is your own high-performance server in your private mobile network on your company's premises. **Public MEC** is distributed computing power in the public mobile network, drastically reducing latency for all mobile users and devices on the road or in the city.

European mobile network operators have embraced two principal architectural approaches for public MEC: the hyperscaler-based MEC model, frequently developed in collaboration with global hyperscalers, and the Sovereign MEC model, which prioritizes localized data handling and adherence to national regulatory requirements. In order to attain full European sovereignty, the implementation of a Sovereign MEC model is considered indispensable and is the focus of the CEF funding initiative.

4.2 Activities and Offerings of Key European MEC Players

Vodafone and the AWS Wavelength Integration

Vodafone has established itself as a leader in Europe's Distributed MEC model through its extensive partnership with Amazon Web Services (AWS). By integrating AWS Wavelength Zones at the edge of its 4G and 5G networks, Vodafone enables developers to deploy applications achieving single-digit millisecond latency. This architecture eliminates multiple transmissions between aggregation sites and the

public internet, which traditionally contribute to cloud latency. Vodafone initiated its MEC service rollout in the UK and Germany in early 2021, later expanding to Spain in 2023 [4.1].

Vodafone Market	Active Wavelength Cities	Key Infrastructure/Nodes
United Kingdom	London, Manchester, Cambridge, Oxford, Birmingham, Bristol, Cardiff	First commercial centre in London (2021)
Germany	Berlin, Munich, Dortmund, Dusseldorf, Cologne	First AWS Zone in Dortmund (2021)
Spain	Malaga, Granada, Córdoba, Jaén, Almería, Seville (Andalusia)	Pilot launched in Southern Spain (2023) [4.2]

Deutsche Telekom


First Generation Telco Edge Cloud (TEC) with MobileEdgeX [4.3]

MobileEdgeX was established by Deutsche Telekom AG in early 2018 and subsequently acquired by Google Cloud [4.4]. The company was conceived as a federated "Telco Edge Cloud," aiming to develop a unified marketplace and orchestration platform that connects application developers with the MEC infrastructures of diverse Mobile Network Operators (MNOs) globally. The platform played a significant role in GSMA pre-commercial trials for latency-sensitive applications. Its primary focus included supporting Extended Reality (XR), Augmented Reality (AR) tours, real-time multiplayer gaming, and visual positioning systems [4.5]. In Germany, Telekom and the MobileEdgeX Team operated two primary MEC locations.

Edge Infrastructure

Today

- 5 Datacenters in Germany, each with 48 servers (384 CPUs, 4 Nvidia T4 GPUs)
- Connected via Mobile Network
- 100Gbit/s redundant



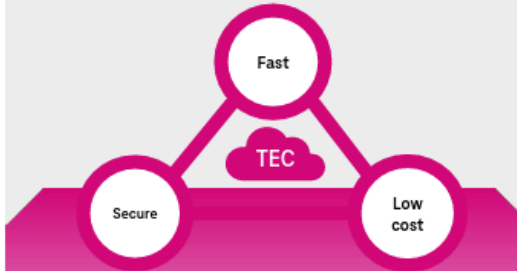
Buildout '25/'26

- 10+ Datacenters with additional capacity
- Server/GPU update
- Connected via Fixed NW

Customer needs

- ❖ Realtime critical applications
- ❖ Processing of highly secure and sensitive data
- ❖ Mobility critical applications
- ❖ Clarity of the network context
- ❖ Cost and efficiency optimization
- ❖ Reduce complexity and TCO
- ❖ Data sovereignty
- ❖ Scalability
- ❖ Trust

How TEC solves pain points



- ✓ Scaling directly and globally
- ✓ Better user experience
- ✓ Reduced latency
- ✓ Reduced time to market
- ✓ Build in security
- ✓ Reduced infrastructure costs
- ✓ Real-time security

Telekom Market	Cities	Key Infrastructure/Nodes
Germany	Berlin, Düsseldorf, Frankfurt, Hamburg, Nürnberg	5 Locations across Germany

Second-Generation Edge Connect (compatible with IPCEI CIS standards)

Telekom is launching its second-generation Edge Cloud called “Edge Connect” at five key locations in Germany, focusing on Germany's major traffic hubs to process data locally. The system uses open source software and will be expanded further. Its "Second-Generation Edge Connect" meets IPCEI-CIS Reference Architecture standards, enabling Telekom's edge infrastructure to operate as part of an interoperable European ecosystem rather than as an isolated network.

Telefonica and the 17-Node Spanish Edge Plan

Telefonica's "Edge Plan" represents one of the most extensive national edge service deployments in Europe. The company is promoting business-to-business (B2B) edge services via 17 planned nodes throughout Spain. In contrast to Vodafone's broader, cross-border strategy, Telefónica is concentrating on comprehensive integration within Spain's productive sectors [4.6].

Telefónica Market	Cities	Key Infrastructure/Nodes
Spain	Madrid, Valencia, Seville, Bilbao and A Coruña	with 12 additional nodes planned in Spain to increase capacity

TIM Italy

Developed in partnership with Noovle, Google Cloud, and Ericsson, TIM is launching a cloud-based 5G solution that automates industrial processes and real-time services via Edge/MEC Computing. The project leverages TIM's Telco Cloud infrastructure, Google Cloud, and Ericsson's 5G Core and automation technologies [4.7].

Telia: NorthStar Project

Telia and Ericsson have partnered to launch the "NorthStar" 5G innovation program in the Nordic and Baltic regions. The initiative accelerates industrial innovation in Sweden by providing organizations access to advanced 5G features, such as network slicing and positioning, not yet on public networks. It offers a sandbox environment for testing and sometimes connects to the public core network for large-scale applications [4.8].

Building infrastructure for innovation

- ED5GE: Connecting Sweden's Smart Communities with RISE
- Supporting sustainable development and safer communities with advanced connectivity
- 5G NETC: Building out Sweden's 5G transport corridors to support remote controlled/autonomous transport, as well as drones and rail

NorthStar

Co-funded by the European Union

4.3 Technological Prerequisites and Drivers of MEC Adoption

5G Standalone (SA)

The true benefits of Multi-access Edge Computing (MEC) are achieved when it is deployed alongside a 5G Standalone (SA) network architecture. Unlike 5G Non-Standalone (NSA), which depends on a 4G LTE core, 5G SA features a cloud-native core that enables ultra-reliable low-latency communications (URLLC) and supports network slicing [4.9].

By the end of 2024, Europe continued to lag in terms of 5G SA coverage, which remains a significant issue for the region's competitiveness against other. Despite this, the number of operational 5G SA networks in Europe saw substantial growth between 2023 and 2024.

The deployment of SA allows for the implementation of the User Plane Function (UPF) at the edge, a critical component of the 3GPP 5G Core that enables local breakout of data [4.10]. This local processing ensures greater data privacy and locality, which is a key requirement for our CEF use cases as shown above.

Interoperability and the Rise of Network APIs

A recurring challenge for developers has been the fragmentation of MNO networks. An application developed for Vodafone might not easily run on Telekom Deutschland or Telefónica Spain without significant modification. To resolve this, the industry has coalesced around two major initiatives: the GSMA Open Gateway and the CAMARA project.

GSMA Open Gateway and CAMARA

The GSMA Open Gateway initiative, supported by over 69 major MNO groups representing 78% of the global market, aims to standardize Network APIs. These APIs abstract complex network functions into simple, programmable interfaces for developers [4.11].

API Category	Specific APIs	Industry Impact
Security & Fraud	SIM Swap, Verification, Match, Number KYC	Reducing online fraud, replacing SMS OTPs
Connectivity Control	Quality on Demand (QoS), Provisioning, Slice	Guaranteeing bandwidth for critical video or industrial links
Location Services	Edge Discovery, Geofencing, Device Location Retrieval	Real-time asset tracking and site security
Insights	Population Density, Device Reachability	Urban planning, supply chain optimization

Orange has been particularly active in this space, offering an "API Playground" through its 19 global 5G Labs [4.12]. These standardized APIs ensure that a developer can "plug into" the capabilities of 5G networks through a single framework, accelerating time-to-market for innovative services. Notably, this effort is not limited to Orange; other major European operators including Telekom Deutschland, Vodafone, Telefónica, TIM, Telia, and Telenor are also working extensively to incorporate these APIs into their infrastructures. By adopting unified API frameworks, these operators are enabling a more seamless integration of advanced network features across Europe, further expanding access for developers and driving innovation in the 5G ecosystem [4.13].

The MWC 2026 Milestone: The European Edge Continuum

By Mobile World Congress (MWC) 2026, the European MEC market achieved a major milestone: the successful live demonstration of the "European Edge Continuum." This initiative, a federation of the five largest European operators such as Deutsche Telekom, Orange, Telefónica, TIM, and Vodafone marks the creation of a truly pan-European federated edge cloud.

Strategic Implications of the Federated Edge

The federation transforms what were previously isolated "edge silos" into a seamless, interconnected infrastructure. It provides a single-entry point for enterprises to deploy and manage applications across multiple operators' nodes.

1. **Extended Geographic Reach:** Developers can access the combined footprint of the five largest MNOs through a single interface.
2. **Dynamic Workload Allocation:** Intelligent distribution of applications across federated nodes ensures optimal performance and cost efficiency.
3. **Service Continuity:** Mobility-aware orchestration ensures that a service remains active as a user or device (such as a connected vehicle) moves between different networks and across borders.
4. **Sovereignty and Compliance:** The model ensures built-in data sovereignty and interoperability, aligning with European values and regulatory requirements [4.14].

Challenges and Future Outlook

Despite the progress, the European 5G MEC market is still in its infancy and faces several hurdles. The fragmentation of spectrum policies across EU member states remains a barrier to unified cross-border services. Furthermore, the profitability of the telecom sector is under pressure, with real-term revenue declines impacting the ability of operators to sustain high levels of investment, especially when this investment does not lead to short-term, guaranteed revenue streams [4.15].

However, the "compelling event" for MEC is the rise of Generative AI. As enterprises look to deploy large language models (LLMs) and agentic AI like Deutsche Telekom's RAN Guardian, the need for localized, low-latency compute will likely increase [4.16]. The shift towards "AI-first" networks suggests that the next phase of 5G evolution will be defined by the Cloud Continuum, where MEC nodes act as the localized brains of an automated society [4.17, 4.18].

In conclusion, the period between 2024 and 2026 has seen the European MEC market mature from a series of isolated pilots into a federated, interoperable infrastructure. The combination of 5G Standalone, standardized Network APIs via CAMARA, and the collaborative "Edge Continuum" model provides a robust framework for enterprises to innovate. As the industry moves toward commercial industrialization, the success of these initiatives will be a determining factor in Europe's digital sovereignty and its role in the global digital economy.

The upcoming chapter will outline the primary challenges encountered by mobile operators as they expand their MEC solutions throughout Europe.

References:

[4.1] Vodafone. Vodafone expands access to AWS Wavelength for business customers in more European countries.

<https://www.vodafone.com/news/newsroom/technology/vodafone-expands-access-aws-wavelength-business-customers-european-countries>

[4.2] Mobile Europe. Vodafone to expand MEC to more European countries with AWS. <https://www.mobileeurope.co.uk/vodafone-to-expand-mec-to-more-european-countries-with-aws/>

[4.3] Business Wire. Mavenir und MobileEdgeX ermöglichen globale Edge-Konnektivität mit Deutsche Telekom. <https://www.businesswire.com/news/home/20210623005395/de>

[4.4] GSMA. Google acquires edge computing company MobileEdgeX. <https://www.gsma.com/solutions-and-impact/technologies/networks/latest-news/google-acquires-edge-computing-company-mobileedgex/>

[4.5] GSMA Foundry. Telco Edge Cloud TEC pre-commercial trial. <https://www.gsma.com/get-involved/gsma-foundry/telco-edge-cloud-tec-pre-commercial-trial/>

[4.6] Telefónica. Telefónica activates edge commercial services to empower businesses in Spain. <https://www.telefonica.com/en/communication-room/press-room/telefonica-activates-edge-commercial-services-empower-businesses-spain/>

[4.7] TIM. TIM Cloud Network 5G (press release). <https://www.gruppotim.it/en/press-archive/market/2021/PR-TIM-Cloud-Network-5G-28giugno2021.html>

[4.8] Telia Company. NorthStar functionality areas. <https://www.teliacompany.com/en/articles/northstar-functionality-areas>

[4.9] Connect Europe. State of Digital Communications – 2025 edition. <https://connecteurope.org/sites/default/files/2025-01/State%20of%20Digital%20Communications%20-%202025%20edition.pdf>

[4.10] 3GPP. Edge computing. <https://www.3gpp.org/technologies/edge-computing>

[4.11] GSMA. GSMA Open Gateway supporters. <https://www.gsma.com/solutions-and-impact/gsma-open-gateway/supporters/>

[4.12] Orange. 5G Lab (Orange 5G Lab / API Playground). <https://5glab.orange.com/en/>

[4.13] CAMARA Project. CAMARA. <https://camaraproject.org/>

[4.14] Deutsche Telekom (MWC). European edge continuum: Connecting Europe through federated edge innovation. <https://mwc.telekom.com/session/european-edge-continuum-connecting-europe-through-federated-edge-innovation>

[4.15] Connect Europe. State of Digital Communications – 2025 edition.
<https://connecteurope.org/sites/default/files/2025-01/State%20of%20Digital%20Communications%20-%202025%20edition.pdf>

[4.17] Deutsche Telekom. Strategic partnership with Google Cloud.
<https://www.telekom.com/en/media/media-information/archive/strategic-partnership-with-google-cloud-1090376>

[4.18] Deutsche Telekom. Milestone for Europe's digital sovereignty.
<https://www.telekom.com/en/media/media-information/archive/milestone-for-europe-s-digital-sovereignty-1102498>



5 Challenges for pan-European MEC Rollout

The challenges for telcos to implement a pan-European are analyzed using a PESTLE analysis. This PESTLE analysis identifies and clarifies the key barriers to 5G Multi-access Edge Computing (MEC) deployment across the European Union, distinguishing between two distinct operational contexts and stakeholder groups. The analysis addresses challenges specific to 5G Corridors (cross-border highway and transport infrastructure) and Smart Communities (urban and regional deployments), while separating concerns of Telco operators (telecommunications companies responsible for network infrastructure) from Non-Telco stakeholders (municipalities, road authorities, automotive manufacturers, technology providers, and service operators).

This structured approach helps policymakers, investors, and operators understand where interventions are most needed and which stakeholder groups must drive solutions.

The core purpose of this Challenges section is to dissect why the deployment of 5G Multi-access Edge Computing (MEC) technologies across the EU lags behind the requirements of high-priority applications such as Cooperative, Connected, and Automated Mobility (CCAM) in corridors and smart communities, and why telcos—the natural providers of network-integrated edge infrastructure—are not advancing the ecosystem as urgently as needed. This analysis draws on empirical insights from targeted stakeholder interviews, including Deutsche Telekom's Edwin Fischer, alongside representatives from Telefónica (TEF), Vodafone (VF), and Orange, as well as desk research from prior deliverables (D3.1/D3.2) and the evolving 5GMEC4EU white-paper concept.

Three guiding questions frame the discussion:

- Why are telcos not as far advanced in MEC deployment as required for pan-European use cases? Edwin Fischer from Deutsche Telekom highlights a fundamental "chicken-and-egg" dilemma: service providers show little demand for even continental cloud platforms, let alone operator-specific MEC instances, restricting services to networks with existing MEC support or optimal routing—effectively limiting them to "restricted roaming".
- Why are telcos not actively fostering the broader MEC ecosystem? Without a "Big Biz Opportunity", no actor prioritises the necessary changes, such as shifting from home routing to local breakout in visited networks (prerequisite for 5G Standalone), or negotiating lawful interception for MEC-routed traffic.
- What does this mean for EU corridors and smart communities? Achieving seamless pan-European MEC coverage demands consensus on PLMN-specific MEC or shared national edge clouds, but current fragmentation in demand, architecture, and operations perpetuates silos.
- To ensure comprehensive coverage, the analysis applies a PESTLE lens (Political, Economic, Social, Technological, Legal, Environmental) across

Technical, Regulatory, and Business challenge categories, synthesising insights to inform D4.2 architecture guidance and WP5 business models.

5.1 POLITICAL FACTORS

5.1.1 Political Challenges in 5G Corridors

Telco Perspective:

Challenge 1: Multi-Country Spectrum Fragmentation

- Each EU member state runs independent spectrum auctions with different rules and timelines, making it nearly impossible for telcos to deploy identical networks across borders. [5.1]
- Example: Germany completed its 3.5 GHz auctions in 2019; France delayed until 2020–2022; Spain's proceeded even later via IPCEI-CIS framework. A single corridor spanning three countries requires three separate infrastructure investments with misaligned timelines. [5.1][5.2][5.3]
- Why it matters: Telcos must navigate 27 different regulatory regimes, tripling legal and compliance costs. Planning a cross-border 5G corridor becomes a 3–5 year effort just to align spectrum rules. [5.10][5.48]

Challenge 2: Divergent Coverage Obligations

- Germany requires 98% coverage; France requires 80% of the population; Spain's obligations vary by region. These conflicting mandates force telcos to over-engineer some areas and under-serve others. [5.1][5.2]
- Impact: Increases per-kilometer deployment cost and delays harmonized rollout.

Non-Telco Perspective:

Challenge 3: Cross-Border Governance Vacuum

- No single authority manages corridor deployment. Road authorities (France), transport ministries (Germany), telecom regulators (Luxembourg), and police (cross-border law enforcement) operate independently with no unified permitting process. [5.12]
- Example: Site acquisition for a highway MEC node requires approval from road authority (4–8 weeks), environmental authority (6–12 weeks), local municipality (2–6 weeks), and sometimes regional government (8–16 weeks). Processes differ by country. Total time: 2–24 months. [5.22]
- Why it matters: Projects stall; road authorities cannot guarantee corridor continuity because telcos don't commit until permits are confirmed.

Challenge 4: No Legal Framework for Cross-Border Cost Sharing



- Who pays for MEC nodes at borders? The country of origin, the country of termination, or shared? Unclear legal responsibility delays investment decisions and creates distrust between stakeholders. [5.3][5.12]

5.1.2 Political Challenges in Smart Communities

Telco Perspective:

Challenge 5: Municipal Fragmentation & Competing Priorities

- Each municipality has different smart city priorities (traffic, parking, public transport, environmental monitoring). Telcos cannot deploy a "one-size-fits-all" MEC; they must customize for local needs. [5.4][5.22]
- Impact: Prevents economies of scale; 50 smart cities require 50 different solutions.

Non-Telco Perspective:

Challenge 6: Local Political Resistance to Infrastructure

- Citizens oppose new cell towers citing health, environmental, and visual concerns. Politicians, fearing backlash, delay site approvals. [5.21][5.22]
- Example: In urban areas, average site approval time is 4–8 weeks; with citizen opposition, approval extends to 12–24 months. [5.22]

Challenge 7: Competing Vendor Allegiances

- European cities increasingly demand "vendor diversity" (avoiding sole dependence on Chinese or US suppliers), but few vendors offer complete European solutions. Municipalities cannot mandate vendor choice without reducing competition and inflating costs. [5.5][5.6]

5.2 ECONOMIC FACTORS

5.2.1 Economic Challenges in 5G Corridors

Telco Perspective:

Challenge 8: Unsustainable MEC Deployment Costs

- MEC deployment for a 20,000 km cross-border corridor costs €75–115k per location for basic coverage, scaling to €250k per location for comprehensive deployment. [5.7][5.20][5.35]
- Breakdown:
 - Civil works (trenching, cable, site prep): 40–50% of cost
 - Compute/server equipment: 20–30%

- Power infrastructure (backup generators, grid extensions): 15–20%
- Operational setup & staffing: 10–15%
- Example: A France–Germany–Luxembourg corridor (600 km, 30 MEC locations) costs €2.25–7.5M. ROI is negative if demand is unproven. [5.3][5.35]
- Why telcos hesitate: Network infrastructure investment (€70B/year EU-wide) is directed toward core 5G and fiber. MEC gets <3% because business case is unclear. [5.7][5.8][5.13]

Challenge 9: Finite CEF2 Funding Creates Artificial Urgency

- EU's Connecting Europe Facility 2 (CEF2) co-funds 55–60% of corridor MEC costs (~€2B digital budget across 27 MS). Without co-funding, projects fail economic tests. [5.9]
- Problem: Once CEF2 expires (2027), telcos must justify continued investment from operational budgets. If demand remains unproven, investment stops. [5.9][5.48]
- Ripple effect: European digital sovereignty is lost as hyperscalers (AWS, Azure) fill the gap. [5.47]

Challenge 10: Roaming Revenue Collapse Undermines Business Models

- Telcos historically earned margin from roaming (customers roaming into their network paying premium rates). EU roaming regulations eliminated 40–50% of roaming revenue. [5.48]
- Impact: Telcos have no revenue stream to monetize MEC across borders. Even if infrastructure is built, no clear way to charge customers for edge services.

Non-Telco Perspective:

Challenge 11: Freight/Logistics Stakeholder Willingness-to-Pay Uncertain

- Automotive manufacturers hesitate to invest in 5G modems (€500–2,000 per vehicle) without proof that connected/autonomous features increase value or reduce operating costs. [5.11][5.14]
- Example: Trucking companies see fuel savings of ~3–8% via platooning, but won't deploy until infrastructure is guaranteed across 80%+ of corridors. Chicken-and-egg problem. [5.11][5.12]

Challenge 12: Road Authority Budget Constraints

- Road authorities lack capital to co-invest in MEC. Their budgets focus on maintenance (potholes, repaving). Smart infrastructure is perceived as luxury, not necessity. [5.12]

5.2.2 Economic Challenges in Smart Communities

Telco Perspective:

Challenge 13: Fragmented City Deployments = No Scale Economics

- 34 mobile network operators in EU; assume 50% have MEC ambitions. Each deploys separate MEC infrastructure in the same city. [5.8][5.10]
- Example: Berlin has 4 major operators. If each builds MEC, cost per operator is €10–15M for city-wide coverage. If shared infrastructure, cost would be €5–7M per operator. Fragmentation nearly doubles per-operator CAPEX. [5.20][5.35]

Challenge 14: Unclear Revenue Models for MEC Services

- What should telcos charge for MEC? Per-minute? Per-MB? Subscription? Device subscription? No industry consensus. [5.13]
- Real problem: Smart city applications (traffic optimization, environmental monitoring, smart parking) generate social value (reduced congestion, lower emissions) but not direct revenue to offset MEC deployment cost. [5.4][5.14]
- Example: A city saves €50M/year in traffic congestion; telco's MEC enables this. But telco captures €0 of that value. Who funds the MEC? [5.4][5.14]

Non-Telco Perspective:

Challenge 15: City Budgets Exhausted by Other Digital Priorities

- Smart city budgets split among broadband, fiber, smart lighting, smart parking sensors, traffic cameras, etc. MEC is one of many competing priorities. [5.4]
- Impact: Cities prefer to buy MEC services from cloud providers (AWS, Azure) rather than co-invest with telcos, because cloud providers bundle compute with other services. [5.13][5.35]

Challenge 16: Enterprise Demand for MEC Remains Speculative

- Manufacturing plants, hospitals, retailers claim they need MEC for edge AI, real-time inventory, AR/VR. But willingness-to-pay is low. [5.31][5.32]
- Example: A factory might save €500k/year via predictive maintenance on MEC vs. cloud. But upfront MEC integration cost is €2M. ROI = 4 years; too risky for most enterprises. [5.31][5.35]

5.2.3 SOCIAL FACTORS

5.2.4 Social Challenges in 5G Corridors

Telco Perspective:

Challenge 17: Public Skepticism About Automated Vehicles & V2X Safety

- Only 30% of Europeans support autonomous vehicles; 35% are actively opposed. [5.15][5.16]
- Why it hurts telcos: If public rejects autonomous vehicles, demand for corridor MEC evaporates. Telcos cannot justify €250k/location investment on speculative AV adoption. [5.11][5.15]

Non-Telco Perspective:

Challenge 18: Data Privacy Fears Among Motorists

- 71% of European motorists are unwilling to share vehicle data due to privacy concerns. [5.16][5.17]
- Real risk: V2X communication requires vehicles to broadcast location, speed, heading to infrastructure. Citizens fear data misuse (insurance companies charging based on driving behavior, law enforcement tracking, commercial data brokers). [5.17][5.33]
- Impact: Road authorities cannot promote V2X services; public resistance stalls ecosystem. [5.16][5.18]

Challenge 19: Job Displacement Anxiety in Transport

- Automated vehicles threaten truck drivers (1.3M in EU), taxi drivers, bus operators, and logistics workers. [5.18]
- Social consequence: Labor unions and regional governments resist automation. Investment in AV infrastructure seen as anti-worker. [5.18]
- Telco angle: Communities decline to permit MEC sites if seen as promoting job-killing automation.

Challenge 20: Digital Divide Exacerbates Rural Deployment Gap

- MEC deployment prioritizes high-density urban corridors (France, Germany, Benelux) due to cost-benefit. Rural Eastern Europe, Southern Portugal, and Nordic periphery lag in coverage. [5.19][5.43]
- Why it matters: Safety benefits of connected vehicles (collision avoidance, hazard detection) are greatest on rural highways, yet infrastructure is sparse there. [5.11][5.19]
- Equity issue: 40% of cross-border corridors are in sparsely populated regions with lower ROI, so investment is deferred indefinitely. [5.3][5.19]

5.2.5 Social Challenges in Smart Communities

Telco Perspective:

Challenge 21: Community Skepticism About Surveillance

- Smart cities require dense sensor networks (cameras, movement tracking, environmental sensors). Residents fear surveillance and loss of privacy. [5.21][5.40]
- Impact: Activists block sensor deployments; municipalities face public backlash; telcos cannot market "smart city MEC" without addressing privacy concerns. [5.21]

Non-Telco Perspective:

Challenge 22: Participatory Governance Bottlenecks

- Successful smart cities involve citizens in planning (participatory budgeting, citizen councils, public workshops). This slows decision-making. [5.22]
- Example: Barcelona's smart city initiatives involve >10 public consultations per major project, extending timelines by 6–12 months. [5.22]

Challenge 23: Inclusivity & Accessibility Requirements

- EU accessibility standards require smart city services to work for elderly, disabled, and low-income residents. Adds cost and complexity to application design. [5.23]
- Impact: Telcos and municipalities must ensure MEC-enabled apps work for all users, not just tech-savvy urbanites. [5.23][5.22]

5.3 TECHNOLOGICAL FACTORS

5.3.1 Technological Challenges in 5G Corridors

Telco Perspective:

Challenge 24: Roaming Handover Delays Exceed Safety Requirements

- When a vehicle crosses from German to French network, roaming triggers home routing: traffic reroutes through German operator's core network, adding 500 ms–2 seconds latency. [5.3][5.24][5.26]
- Safety-critical problem: Emergency vehicle alert (EVA) requires <100 ms latency. Current roaming adds 5–20x that delay. [5.11][5.26]
- Why: ETSI MEC federation standards (Mp1–Mp5 interfaces) are defined but not implemented in production systems. Telcos would need to rebuild roaming architecture—a €2B+ investment across EU. [5.24][5.25]

Challenge 25: Spectrum Configuration Mismatch at Borders



- Real example from 5GCroCo project: France uses 8+2 TDD slot configuration (8 downlink, 2 uplink); Germany uses 4+1. At border, vehicles experience: [5.26]
 - 35–40% throughput drop (450 Mbps → 280 Mbps) [5.26]
 - 50 ms latency spike during handover [5.26]
 - Session interruptions lasting 2–5 seconds [5.26]
- Why it matters: Platooning (trucks following at 5-meter separation at 80 km/h) becomes unsafe if latency spikes by 50 ms. [5.11][5.26]

Challenge 26: Immature 5G Standalone (5G SA) Deployment

- Local Breakout (LBO)—a critical feature that routes traffic locally at edge rather than through home network—requires 5G SA. [5.2][5.29]
- Current reality: Most EU networks still rely on 5G NSA (Non-Standalone, using 4G core). 5G SA rollout is 2–3 years behind schedule. [5.27][5.29]
- Impact: Telcos cannot offer low-latency edge services until 5G SA is operational. Corridors cannot launch until 2027–2029. [5.27][5.31]

Non-Telco Perspective:

Challenge 27: Fragmented MEC Platforms Prevent Inter-Operability

- Vodafone deployed AWS Wavelength MEC; Deutsche Telekom uses Azure MEC; Telefónica built proprietary OnLife MEC; Orange has MEC-2. [5.28][5.31]
- Real problem: An automotive OEM developing a lane-change assistance app must code against 4+ different APIs, deploy 4+ times, test 4+ times. [5.10][5.24]
- Cost to OEM: €500k–2M per unique MEC platform supported. [5.35]
- Why architectures diverged: ETSI standards exist but lack implementation details. Each operator made independent choices. [5.24][5.25]

Challenge 28: Network Slicing Orchestration Non-Functional

- CCAM requires distinct slices for: [5.2][5.29]
 - uRLLC (ultra-reliable low-latency): V2V collision warnings (<20 ms, 99.999% uptime) [5.2]
 - eMBB (enhanced mobile broadband): HD map updates (100 Mbps, <1 sec latency) [5.2]

- mMTC (massive machine-type): Probe vehicle data (moderate latency, high scale) [5.2][5.11]
- Current state: No vendor provides unified orchestration across these slices. Manual tuning per corridor; no dynamic adaptation. [5.30][5.31]
- Example: Traffic spikes cause latency spikes in uRLLC slice if orchestration cannot auto-scale resources from eMBB slice. Safety applications fail. [5.30][5.11]

5.3.2 Technological Challenges in Smart Communities

Telco Perspective:

Challenge 29: Orchestration & Automation Gaps Prevent MEC Scaling

- MEC app lifecycle (instantiation, scaling, migration, termination) requires sophisticated orchestration across heterogeneous hardware, telco, and cloud providers. [5.10][5.30]
- Reality: Most MEC deployments require manual intervention 30–40% of the time. Automated failover, load balancing, and app migration are incomplete. [5.30]
- Impact: Operating costs are high; response time is slow. MEC doesn't meet latency SLAs reliably. [5.30][5.35]

Challenge 30: AI/Edge Convergence Nascent

- Smart city applications (traffic optimization, pedestrian detection, environmental monitoring) increasingly rely on AI/ML at the edge. [5.31][5.32]
- Problem: Edge hardware has limited compute (constrained by power, cooling, cost). Training large AI models locally is impractical; models must be pre-trained in cloud, then deployed to edge. [5.31]
- Operational burden: Continuous model updates, version management, and rollback procedures are immature. [5.31][5.32]

Non-Telco Perspective:

Challenge 31: Cybersecurity Requires Standardized V2X Authentication

- Smart cities and corridors collect sensitive data: location, identity, behavior. V2X (vehicle-to-infrastructure) communication must authenticate every message. [5.17][5.33]
- Current fragmentation: Different countries propose different authentication protocols (PKI standards, key management, revocation lists differ). [5.33][5.34]

- Impact: Vehicles cannot operate seamlessly across borders without re-authentication, causing handover delays. [5.26][5.33]

5.4 LEGAL FACTORS

5.4.1 Legal Challenges in 5G Corridors

Telco Perspective:

Challenge 32: GDPR Cross-Border Data Movement Ambiguity

- CCAM requires vehicles to report location, speed, heading to infrastructure across borders. GDPR restricts movement of EU citizen data to non-adequate jurisdictions. [5.17][5.33]
- Real dilemma: If French MEC node sends data to German MEC, is that a cross-border transfer? Standard Contractual Clauses (SCCs) provide legal cover, but enforcement is uncertain post-Schrems II ruling. [5.33][5.34]
- Telco burden: Extensive legal review per cross-border flow; data residency policies required; audit overhead adds 10–15% to operational cost. [5.33][5.35]

Challenge 33: Vendor Restriction Compliance Costly

- EU 5G Toolbox recommends restricting "high-risk suppliers" (Huawei, ZTE) in RAN and potentially core network. [5.5][5.6]
- Implementation challenge: RAN equipment has 5–10 year lifespans; replacing all Huawei/ZTE CPE and RAN units to de-risk requires €5–8B across EU (30–40% of CPEs are high-risk supplier equipment). [5.36][5.39]

Non-Telco Perspective:

Challenge 34: Autonomous Vehicle Liability Framework Non-Existent

- If a vehicle using 5G MEC-enabled autonomous steering causes an accident, who is liable? OEM? Telecom operator? Road authority? [5.37][5.38]
- Current reality: Few EU countries have legislated L3+ liability. Uncertainty deters investment. [5.37][5.38]
- Example: France proposed liability framework in 2025; Germany still debating. Two different standards mean OEMs cannot deploy nationwide solutions until 2027–2028. [5.37][5.38]

Challenge 35: Data Sovereignty Regulations Multiply Compliance Burden

- EU GDPR (federal level) + KRITIS-DachG (Germany) + specific NIS2 transpositions (per country) + evolving data localization rules (Hungary, Poland pushing stricter local storage). [5.17][5.39][5.40]

- Impact: Telcos and municipalities cannot design a single CCAM system; must customize for each jurisdiction. [5.39][5.40]

5.4.2 Legal Challenges in Smart Communities

Telco Perspective:

Challenge 36: Smart City Data Ownership Disputes

- Who owns data collected by MEC-enabled smart city sensors? Municipality? Telco? Third-party cloud provider? Residents? [5.40][5.21]
- Example: A smart traffic light produces real-time flow data. City wants to share with researchers; privacy advocates oppose. Telco uncertain whether it can resell anonymized data. [5.40]
- Operational impact: Data governance uncertainty delays service launches; revenue models remain unclear. [5.40][5.35]

Non-Telco Perspective:

Challenge 37: Standardization Compliance Requires Frequent Updates

- ETSI, 3GPP, and IEEE publish new standards annually. Municipalities and service providers must update systems, requiring certification and re-testing. [5.24][5.29]
- Burden: Average 4–6 month lag between standard publication and implementation readiness. Smart city deployments in 2026 may be obsolete by 2028 if updates are missed. [5.24][5.25]

5.5 ENVIRONMENTAL FACTORS

5.5.1 Environmental Challenges in 5G Corridors

Telco Perspective:

Challenge 38: Energy Consumption & Carbon Cost of Dense Site Deployment

- 5G requires 2–3x denser cell sites than 4G. Dense site deployment in rural corridors (where power grid is weak) requires backup generators or expensive grid extensions. [5.41][5.42]
- Numbers: Each 5G site consumes 10–20 kW continuous (vs. 5 kW for 4G). A 20,000 km corridor needs 300+ sites = 3–6 MW baseline load. [5.41][5.43]
- Cost impact: Solar/wind integration costs €100k–200k per site. Most corridor sites rely on grid + diesel backup, increasing carbon footprint by 30–50% vs. urban deployment. [5.42][5.45]
- EU compliance risk: Q1 2026 EU Data Centre Energy Efficiency Directive targets carbon neutrality for all DCs (including edge nodes) by 2030. Corridor

MEC nodes may be swept into scope, forcing renewable integration. [5.43][5.44]

Challenge 39: E-Waste from High-Risk Supplier De-Risking Campaign

- Replacing 200–250M CPEs of Huawei/ZTE origin generates 500k–1M tons e-waste across EU by 2028. [5.36][5.47]
- Disposal cost: €50–100 per unit to recycle responsibly = €10–25B systemic cost. Telcos hesitant to absorb. [5.36][5.47]

Non-Telco Perspective:

Challenge 40: Construction Impact on Corridors & Protected Habitats

- MEC nodes require trenching for power, fiber, and cooling. Corridors pass through protected habitats (wetlands, bird sanctuaries, forests). [5.19][5.46]
- Regulatory delay: Environmental impact assessments add 6–12 months per project. Some sites rejected outright due to habitat risk. [5.22][5.46]

5.5.2 Environmental Challenges in Smart Communities

Telco Perspective:

Challenge 41: Urban Cooling & Power Density Increases

- Urban MEC nodes dissipate higher power density (co-location with other equipment). Air cooling becomes insufficient; liquid cooling required. [5.45]
- Cost: Liquid cooling infrastructure adds 20–30% to site CAPEX and 10–15% to OPEX. [5.45]
- Carbon impact: Most EU cities source 40–60% electricity from renewable; dense MEC power draw strains grids, increasing reliance on peak power plants (natural gas), raising carbon intensity. [5.43][5.46]

Non-Telco Perspective:

Challenge 42: Circular Economy & Supply Chain Resilience Unclear

- MEC equipment sourcing relies on global supply chains (Taiwan, South Korea, Japan). Supply shocks (as seen in 2021–2022 semiconductor crisis) disrupt deployments. [5.36][5.47]
- EU autonomy issue: No European chip manufacturer produces the custom processors needed for MEC; dependency on imports creates geopolitical risk. [5.47]
- [5.19] European Environment Agency. (2025). Digital Infrastructure & Rural Coverage Gaps in EU.

- [5.22] Barcelona Activa. (2025). Participatory Governance in Smart Cities: Timelines & Best Practices.

5.6 SYNTHESIS: CHALLENGE MAPPING TO PESTLE & STAKEHOLDER

#	Challenge	PEST	Context	Telco/ Non-Telco	Key Blocker
1	Multi-Country Spectrum Fragmentation	P	Corridor	Telco	Regulatory will
2	Divergent Coverage Obligations	P	Corridor	Telco	Political consensus
3	Cross-Border Governance Vacuum	P	Corridor	Non-Telco	Institutional design
4	No Legal Framework for Cost Sharing	P	Corridor	Both	Political agreement
5	Municipal Fragmentation	P	Smart City	Telco	Market heterogeneity
6	Local Political Resistance	P	Smart City	Non-Telco	Community acceptance
7	Competing Vendor Allegiances	P	Smart City	Non-Telco	Policy clarity
8	Unsustainable MEC CAPEX	E	Corridor	Telco	Business case
9	Finite CEF2 Funding	E	Both	Telco	EU budget
10	Roaming Revenue Collapse	E	Corridor	Telco	Regulation
11	AV Willingness-to-Pay Uncertain	E	Corridor	Non-Telco	Market adoption
12	Road Authority Budget Constraints	E	Corridor	Non-Telco	Public funding

13	Fragmented City MEC Deployments	E	Smart City	Telco	Market structure
14	Unclear Revenue Models	E	Smart City	Telco	Business model innovation
15	City Budget Constraints	E	Smart City	Non-Telco	Municipal spending
16	Enterprise Demand Speculative	E	Smart City	Non-Telco	Market adoption
17	Public Skepticism on AVs	S	Corridor	Non-Telco	Public perception
18	Data Privacy Fears	S	Corridor	Non-Telco	Trust & regulation
19	Job Displacement Anxiety	S	Corridor	Non-Telco	Labor policy
20	Digital Divide in Rural Areas	S	Corridor	Both	Funding & business case
21	Community Surveillance Skepticism	S	Smart City	Non-Telco	Privacy-by-design
22	Participatory Governance Bottlenecks	S	Smart City	Non-Telco	Process design
23	Inclusivity & Accessibility	S	Smart City	Both	Design standards
24	Roaming Handover Latency	T	Corridor	Telco	Federation architecture
25	Spectrum Config Mismatch at Borders	T	Corridor	Telco	Harmonization
26	5G SA Deployment Immature	T	Both	Telco	Network upgrade cycle
27	Fragmented MEC Platforms	T	Both	Non-Telco	Standards & competition
28	Network Slicing Orchestration	T	Both	Telco	Software maturity



29	Orchestration & Automation Gaps	T	Smart City	Telco	Software engineering
30	AI/Edge Convergence Nascent	T	Smart City	Telco	Technology maturity
31	V2X Auth Standardization	T/L	Both	Both	Standards body agreement
32	GDPR Cross-Border Ambiguity	L	Corridor	Telco	Legal clarity
33	Vendor Restriction Compliance	L	Both	Telco	Supply chain overhaul
34	AV Liability Framework Missing	L	Corridor	Non-Telco	Legislation
35	Data Sovereignty Rules Multiply	L	Both	Both	EU/MS coordination
36	Smart City Data Ownership	L	Smart City	Both	Governance model
37	Standards Compliance Lag	L/T	Smart City	Both	Change management
38	Energy Consumption & Carbon	En	Corridor	Telco	Grid infrastructure
39	E-Waste from De-Risking	En	Both	Telco	Circular economy policy
40	Environmental Impact Delays	En	Corridor	Non-Telco	Planning process
41	Urban Cooling & Power Density	En	Smart City	Telco	Infrastructure capacity
42	Supply Chain Resilience	En	Smart City	Both	EU manufacturing



5.7 References

- [5.1] Knospe, M., & Steingröver, K. (2020). 5G for CAM: A Deployment Metastudy. Synthesis of 5G-MOBIX, 5GCroCo, 5G-CARMEN studies.
- [5.2] Potters, P., et al. (2025). D3.2 5G Edge Deployment Scenarios for CCAM Use Cases. 5GMEC4EU Project, Version 0.9.
- [5.3] Detecon International. (2025). Metastudy on 5G Deployment for Connected Automated Mobility. Cross-border corridor analysis.
- [5.4] European Commission. (2025). Smart Cities & Communities: Policy Framework Update.
- [5.5] CMS Law. (2025). 5G at a Crossroad: Vendor Risk & Security in Europe.
- [5.6] Bird & Bird. (2026). Germany Security Focus: 5G Vendor Restrictions & KRITIS-DachG. Published January 11, 2026.
- [5.7] TelecomAnalysis. (2025). Navigating the Future of Telecom CAPEX: Western Europe 2024–2030. Published August 3, 2025.
- [5.8] Connect Europe. (2025). State of Telecoms Infrastructure & Investment in Europe: 2025 Report.
- [5.9] European Commission. (2025). Connecting Europe Facility 2: Digital Funding Overview.
- [5.10] BEREC. (2024). BEREC Report on Cloud and Edge Computing Services. Published March 2024.
- [5.11] 5GAA. (2025). Mobile Edge Computing Use Cases & Evaluation Methodology. July 2025.
- [5.12] CEDR/CCAM Cooperative. (2025). European Road Authority Perspectives on CCAM Deployment.
- [5.13] McKinsey. (2025). The Future of Telcos: Mapping Routes to Renewed Success.
- [5.14] Accenture. (2026). The Impact of 5G on the European Economy.
- [5.15] Nature. (2025). Investigating Preferences for Autonomous Vehicle Use. Published August 24, 2025.
- [5.16] CCAM Cooperative. (2025). Public Acceptance & Trust in Automated Driving: 3rd Webinar Series.
- [5.17] ISACA. (2024). Cloud Data Sovereignty Governance & Risk Implications. Published November 17, 2024.

- [5.18] ETUC / European Trade Union Confederation. (2025). Impact of Automation on European Transport Workforce.
- [5.19] European Environment Agency. (2025). Digital Infrastructure & Rural Coverage Gaps in EU.
- [5.20] Technopolis Group. (2025). Europe's Race for Computing: Progress & Challenges in Edge Infrastructure Deployment. Published October 1, 2025.
- [5.21] World Economic Forum. (2026). Europe's Smart City Privacy Paradox. Published January 4, 2026.
- [5.22] Barcelona Activa. (2025). Participatory Governance in Smart Cities: Timelines & Best Practices.
- [5.23] EU. (2025). Web Accessibility Directive & Smart City Compliance.
- [5.24] ETSI. (2025). ETSI MEC Architecture & Federation White Papers.
- [5.25] GSMA. (2025). GSMA Open Gateway Initiative: MEC Interoperability Progress.
- [5.26] 5GCroCo Project. (2025). Cross-Border Corridor Deployment Results: Spectrum & Handover Analysis.
- [5.27] Ookla. (2025). 5G Coverage in Europe: NSA vs. SA Deployment Status. Published October 1, 2025.
- [5.28] Sagar Nangare. (2025). Edge Computing & 5G: Telco's Next Growth Engine. LinkedIn, September 14, 2025.
- [5.29] 3GPP. (2025). Release 18: Network Slicing & Resource Management Enhancements.
- [5.30] Technopolis Group. (2025). MEC Orchestration & Automation Maturity Assessment.
- [5.31] Nokia. (2026). Europe's AI Ambition & Edge Computing Convergence. Published January 15, 2026.
- [5.32] SNS JU. (2025). Research & Innovation on Cloud for 6G Networks. Published June 2025.
- [5.33] Diva Portal. (2025). Edge Computing & GDPR: Technical Security & Legal Analysis.
- [5.34] CIGIONLINE. (2025). Cross-Border Compliance Challenges & Data Sovereignty.
- [5.35] IARCGROUP. (2026). Europe Edge Computing Market: Vendor Landscape & De-Risking Costs. Published January 5, 2026.

- [5.36] Gartner. (2025). High-Risk Supplier Replacement: Supply Chain Cost Impact 2026–2030.
- [5.37] French Ministry of Interior. (2025). Autonomous Vehicle Liability Proposal: Legislative Framework.
- [5.38] German Federal Ministry of Transport. (2025). AV Liability Framework: Stakeholder Consultation Draft.
- [5.39] German Federal Ministry of Interior. (2025). KRITIS-DachG: Critical Infrastructure Protection Act 2025.
- [5.40] GDPR.eu. (2025). Smart City Data Governance: Ownership & Consent Models.
- [5.41] PMC/NCBI. (2024). Energy Efficiency for 5G & Beyond: Potential & Limitations. Published November 19, 2024.
- [5.42] CTO Magazine. (2025). 5G Environmental Impact & Sustainability. Published December 3, 2025.
- [5.43] European Commission. (2026). Q1 2026 Data Centre Energy Efficiency Package: Carbon-Neutral Targets.
- [5.44] EU. (2023). Energy Efficiency Directive 2023/1791: 11.7% Consumption Reduction Target by 2030.
- [5.45] Integrin. (2026). European Data Centre Cooling & Power Infrastructure Outlook 2026. Published January 2, 2026.
- [5.46] European Environment Agency. (2025). Electricity Grid Carbon Intensity by Region.
- [5.47] World Economic Forum. (2026). Europe's Digital Autonomy: Semiconductor Supply Chain Analysis. Published January 4, 2026.
- [5.48] Wray Castle. (2026). Telecom Regulation 2026: Industry Leaders' Priorities. Retrieved January 2026.