GSMA | AI100 人工智能百人会

Mobile AI

Connected Embodied Intelligence

A Key Path to Real-World Deployment

© GSMA 2026. All rights reserved.

Disclaimer

This document is not an Industry Specification and is not developed or maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

This document does not represent the official position of the GSMA. The GSMA is the publisher and owner of this document, but views and opinions expressed in this report may be solely those of the author(s) and do not necessarily reflect the views of the GSMA.

This document is provided "AS IS", for information only. The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for and disclaims any liability for the accuracy or completeness or timeliness of the information contained in this document. Any use of the information contained in this document is at the user's own risk and the user assumes liability for any third-party claims associated with such use. In no event shall the GSMA be liable for any direct, indirect, incidental, special, consequential or punitive damages, or any loss of profits, revenue, data or business opportunities arising out of or in connection with the use of or reliance on this document.

No licence is granted by implication, estoppel or otherwise under any intellectual property right of the GSMA or any third party. Nothing in this document shall be construed as granting any licence or right to use any trademark of the GSMA without prior written permission. Nothing in this document is intended to confer any benefit or right on any third party.

The GSMA is under no obligation to update, revise or supplement this document. The GSMA may withdraw or modify this document at any time without notice.

Antitrust Notice

The information contained herein has been prepared in accordance with the GSMA's Antitrust Policy: https://legal.gsma.com/wp-content/uploads/2025/11/Antitrust-Policy-October-2025.pdf

Executive Summary

Embodied intelligence is moving from laboratory demonstrations towards continuous operation in factories, logistics sites, energy, commercial services and public services. A standalone robot, however, is constrained by on-board computing, energy, data and cost, which limits complex cognition, continuous learning, multi-robot collaboration and lifecycle governance. This white paper proposes Connected Embodied Intelligence as a research framework for how mobile networks, edge and cloud computing and operations platforms can complement on-device intelligence. It is written primarily for mobile network operators and robotics companies, and focuses on mobile robots.

The paper describes four areas where connectivity can add value: layered coordination between on-device control and edge or cloud intelligence, on-demand compute offloading, multi-robot collaboration, and trusted connectivity combined with trustworthy AI and functional safety. In each case, network capabilities complement rather than replace on-device intelligence, and safety-critical control remains on the robot. Because requirements differ by scenario, the paper outlines four networking tiers and proposes assessing performance against end-to-end task outcomes rather than network metrics alone.

Nine case studies from China, covering industrial sites, power grid inspection, firefighting and rescue, logistics, commercial services and large events, illustrate current practice and the role the network actually played in each.

The paper closes with directions for industry discussion: scenario-based network planning, integrated network and computing infrastructure, open interfaces and network APIs such as GSMA Open Gateway, a full-lifecycle trust framework, Responsible AI, joint testing and sustainable business models. These reflect industry research findings and do not represent GSMA policy positions or technical specifications. The paper also sets out an enabling policy environment for connected embodied intelligence, drawing on the GSMA's published policy recommendations on AI readiness.

Contents

Chapter 1. 02
Industry Context and Network Foundations: From Robot Showcases to Connected Operations

Chapter 2. 05
Single-Robot Limits and the Role of Connectivity:
Connectivity as a Key Path to Operating Embodied Intelligence at Scale

Chapter 3. 09
Connected Embodied Intelligence:
Concept and Technical Architecture for Device-Edge-Network-Cloud Collaboration

Chapter 4. 16
Core Value of Connected Embodied Intelligence

Chapter 5. 19
Industry Case Studies

Chapter 6. 31
Development Path and Policy Recommendations:
Building the Infrastructure for Connected Embodied Intelligence

Conclusion 41

Appendix: Glossary 42

References 43

Acknowledgements 45

Foreword



Sihan
Head of GSMA Greater China

A new wave of scientific and technological innovation, led by large models, advanced computing and robotics, is gathering pace, and artificial intelligence is moving from the digital world into the physical world. Embodied intelligence is a key vehicle for bringing AI into the real economy. It is progressing from laboratory validation and single-robot demonstrations towards real-world settings such as factories, industrial parks, energy, logistics, commercial services and public services. The yardstick for measuring its progress is changing accordingly. A compelling one-off demonstration is no longer enough. Embodied intelligence must also be able to operate continuously, make decisions autonomously, work collaboratively and create real value in complex, dynamic and open environments.

In our view, the future development of embodied intelligence can be summarised as the "Four Shifts": towards autonomy, generality, collaboration and practical deployment. Autonomy means that intelligent agents can perceive their environment, understand tasks, make decisions and take action with greater independence. Generality means that capabilities evolve from specific tasks and specific environments to being transferable and reusable across tasks and scenarios. Collaboration means that agents no longer operate in isolation, but work effectively with other agents, with people and with digital systems. Practical deployment means that embodied intelligence moves beyond laboratories and showcases to operate stably, safely and cost-effectively in the real world, continuously creating measurable value.

To move from where we are today towards the Four Shifts, connectivity is a key path for embodied intelligence to achieve operation at scale, continuous service and multi-party collaboration. Connectivity in this sense does not mean that every action depends on a remote network at all times. Rather, it means connecting robots to wider systems of intelligence, operations and governance, built on a foundation of safe local autonomy.

The real world is open, dynamic and uncertain. A standalone robot has limited computing resources, energy, data and cognitive capacity, and struggles to meet the combined demands of complex decision-making, real-time response, continuous learning, multi-robot collaboration and full lifecycle governance. Once connected, the robot itself can link to edge computing, cloud-based models, industry knowledge and external data, gaining more sustained and wider-ranging intelligent support. When robots can connect with one another, with people and with the digital world in a trusted, efficient, real-time and secure way, isolated robots can become coordinated fleets that sense one another, share information and carry out tasks together. When connectivity is further combined with compute scheduling, model iteration, security governance and industry systems, embodied intelligence can turn technical capability into productivity that can be deployed at scale and operated continuously.

The role of communication networks is therefore changing. They are no longer merely channels for transmitting data, but important infrastructure linking robots, edge computing, cloud intelligence, other agents, human operators and industry systems. Multi-layered connectivity, including 5G, 5G-Advanced, Wi-Fi, industrial Ethernet, mesh networking and, looking ahead, 6G, can support a more flexible division of labour and closer collaboration across device, edge, network and cloud.

It should be stressed that being connected is not an end in itself, nor is it simply a matter of adding a communication module to a robot. Its significance lies in overcoming the limits of standalone intelligence and bringing connectivity, computing, data and intelligence together as a whole, providing important support for the Four Shifts. Connectivity is the path; the Four Shifts are the direction. In future, the competitiveness of embodied intelligence will depend not only on how far an individual robot can go, but also on whether the entire intelligent system can be connected, work together and evolve together.

Exploring this direction requires the participation of many parties. Telecom operators, robotics companies, network and equipment vendors, computing and model providers, industry users, research institutions and standards organisations can all contribute perspectives on technical architecture, interfaces, security mechanisms, testing frameworks and business models. With its leading mobile communications infrastructure, complete robotics industry chain and wide range of industry application scenarios, China offers a strong foundation for research into connected embodied intelligence. At the same time, embodied intelligence is a global innovation challenge, and China's industry practice can inform related discussions across the global Mobile AI ecosystems.

This white paper proposes "connected embodied intelligence" as a research framework, with the aim of encouraging the mobile industry and the robotics industry to discuss and validate approaches to connectivity, computing, collaboration, security and operation at scale. We hope it will serve as a useful reference for research and exchange among industry partners, and we welcome comments and suggestions from all parties.

As a Chinese saying goes, "The road is long and hard, but those who keep walking will arrive." On the road to real-world deployment, GSMA looks forward to working hand in hand with partners across the global mobile and robotics industries, harnessing connectivity to bring intelligence together and collaboration to unlock value, so that the Four Shifts of embodied intelligence bear fruit worldwide and, together, we can chart a new blueprint for the era of intelligent connectivity.

Chapter 1.

Industry Context and Network Foundations: From Robot Showcases to Connected Operations

Embodied intelligence is moving from technical validation towards real-world application. Around the world, robots are beginning to take on practical work in sectors such as manufacturing, warehousing and logistics, and energy and utilities, including depalletising, loading, assembly, inspection and sorting. In complex real-world environments, capabilities such as real-time remote operation and device-cloud collaborative intelligence place high demands on network latency, bandwidth and coverage continuity. The integration of communication networks with embodied intelligence is therefore becoming an important path towards adoption at scale..

Who this paper is for. This paper is written primarily for two audiences: mobile network operators, who need to understand what robots will require from networks, edge computing and network APIs; and robotics companies, who need to understand what connectivity can and cannot provide and how to design their products for it. Industry users, network and equipment vendors, platform providers and standards organisations may also find it relevant. The paper focuses on mobile robots, such as humanoid, wheeled and quadruped robots, which move through changing environments and are constrained by on-board power, computing and coverage. Fixed industrial robots are discussed only where they work alongside mobile robots or share the same on-site networks.

1.1 Global Momentum: Embodied Intelligence and Communication Networks Are Converging

Embodied intelligence has become a strategic priority for governments and industry in a growing number of major economies. Policy agendas increasingly link robotics and AI with digital infrastructure, real-world testing and standards development, while robot makers, AI developers, cloud providers and mobile operators continue to invest in the field. China is one of the most active markets: it has identified embodied intelligence as a future industry in its national planning and introduced a series of supporting measures covering technology development, application scenarios, standards, and testing and training of robots in real operating environments.

Across these agendas, a common shift is visible: embodied intelligence is no longer treated as an isolated robot product, but as part of a broader system that brings together computing, data, application scenarios, networks and security. The mobile industry is part of this shift. Operators are working with industry partners to support robots, drones, connected vehicles and AI applications [24], and the ITU's IMT-2030 framework identifies the integration of AI and sensing with communication as a direction for future 6G systems [7]. Together, these developments provide both industry and infrastructure momentum for connected embodied intelligence.

1.2 Technology Evolution: From Standalone Capabilities to Multimodality, Device-Cloud Collaboration and Collective Intelligence

Embodied intelligence is evolving from breakthroughs in individual capabilities toward integrated system capabilities. Its technological progress is no longer confined to improvements in the mechanical body, motion control, or the performance of a single algorithm.

Instead, a broader technical system is emerging, combining multimodal perception, embodied foundation models, real-time motion control, closed-loop data systems, and multi-agent collaboration. Robots are evolving from automated equipment that executes predefined programs into intelligent agents that understand their environments and tasks and can learn and act autonomously in open environments.

First, perception is moving from single sensors towards multimodal, high-dimensional and always-on sensing. Robots need to process multi-source information simultaneously, including vision, depth, LiDAR, speech, touch and joint states. In effect, a robot becomes a mobile multimodal data-collection platform that continuously generates large volumes of uplink data, with traffic bursts during phases such as anomaly detection and remote takeover.

Second, decision-making is evolving from rule-based and task-specific models towards embodied foundation models and vision-language-action (VLA) models. VLA models bring visual understanding, language instructions and action mapping into a single model, enabling robots to move beyond executing specific skills towards understanding natural language, decomposing complex tasks and generalising across scenarios. However, stronger model capabilities mean continued growth in parameter count, context length and inference compute. Constrained by power consumption, heat dissipation, weight and cost, the robot body cannot keep increasing its peak computing capacity indefinitely. A layered intelligence architecture is therefore more likely to emerge, combining real-time autonomy on the robot body, low-latency inference at the edge, and complex cognition and training in the cloud.

Third, control is shifting from a single timescale to coordination across multiple timescales. Joint servo control, balance and emergency stop require hard real-time closed loops on the robot body, while environment understanding, task planning and multi-robot scheduling operate on longer timescales. The network needs to provide appropriate connectivity and service assurance for intelligent tasks running at different timescales across the robot body, the edge and the cloud.

Fourth, capability evolution is moving from one-off “model delivery” to a continuous closed loop of data, training, deployment and feedback. The long tail of real-world problems makes failure cases, environmental data and operational logs important sources of model improvement. Network requirements therefore extend beyond one-time access to high-capacity data backhaul, delivery of models and skills, over-the-air (OTA) updates, version auditing and cross-site data collaboration.

Fifth, the form of the system is evolving from single-robot intelligence towards collaboration among multiple robots and heterogeneous agents. Scenarios such as manufacturing, logistics, hospitals and campuses involve humanoid robots, wheeled robots, quadruped robots and unmanned vehicles operating alongside equipment such as lifts and access-control systems. The key capability lies not only in how intelligent an individual robot is, but in whether different devices can share location, maps, events and task status, and divide work dynamically.

Many of the network requirements of embodied intelligence therefore arise from its own technological evolution. Multimodal perception drives high uplink capacity; device-cloud collaboration requires low latency and edge computing; multi-robot collaboration requires high reliability, time synchronisation and continuous coverage; the data feedback loop requires stable backhaul and model distribution; and operation at scale requires identity, access control, security and programmable network capabilities. The more embodied intelligence advances towards general-purpose, autonomous, collaborative and real-world deployment, the more the network needs to be integrated into the intelligent system as infrastructure for both connectivity and service assurance.

1.3 Communication Networks as the Foundation for Continuous Evolution

Across diverse scenarios, embodied intelligence depends heavily on networks for remote operation, multi-robot collaboration and large-scale data backhaul. The capabilities of embodied intelligence are not formed through a static process of one-time training and one-time deployment, but through a continuous cycle of real-world operation, data backhaul, failure-case analysis, model training, simulation-based validation, version release and renewed operation. Long-tail problems that robots encounter in the real world, such as transparent packaging, deformable objects, reflective metal surfaces, non-standard placement and temporary obstacles, are difficult to cover with laboratory data alone. Turning mass-produced robots into manageable data nodes is key to converting experience scattered across individual robots into shared capabilities.

In this cycle, the network plays three roles. First, it carries the backhaul of multimodal data and operational logs, enabling development teams to identify failure modes. Second, it carries the distribution of models, skills and policies, so that a capability learned by one robot can, after review, be synchronised to robots of the same type. Third, it carries version, permission and rollback information, so that model upgrades are no longer a matter of manual, robot-by-robot maintenance but become a phased, auditable operational process. In other words, connectivity turns the robot from a standalone product into an intelligent service node that can be operated on a sustained basis.

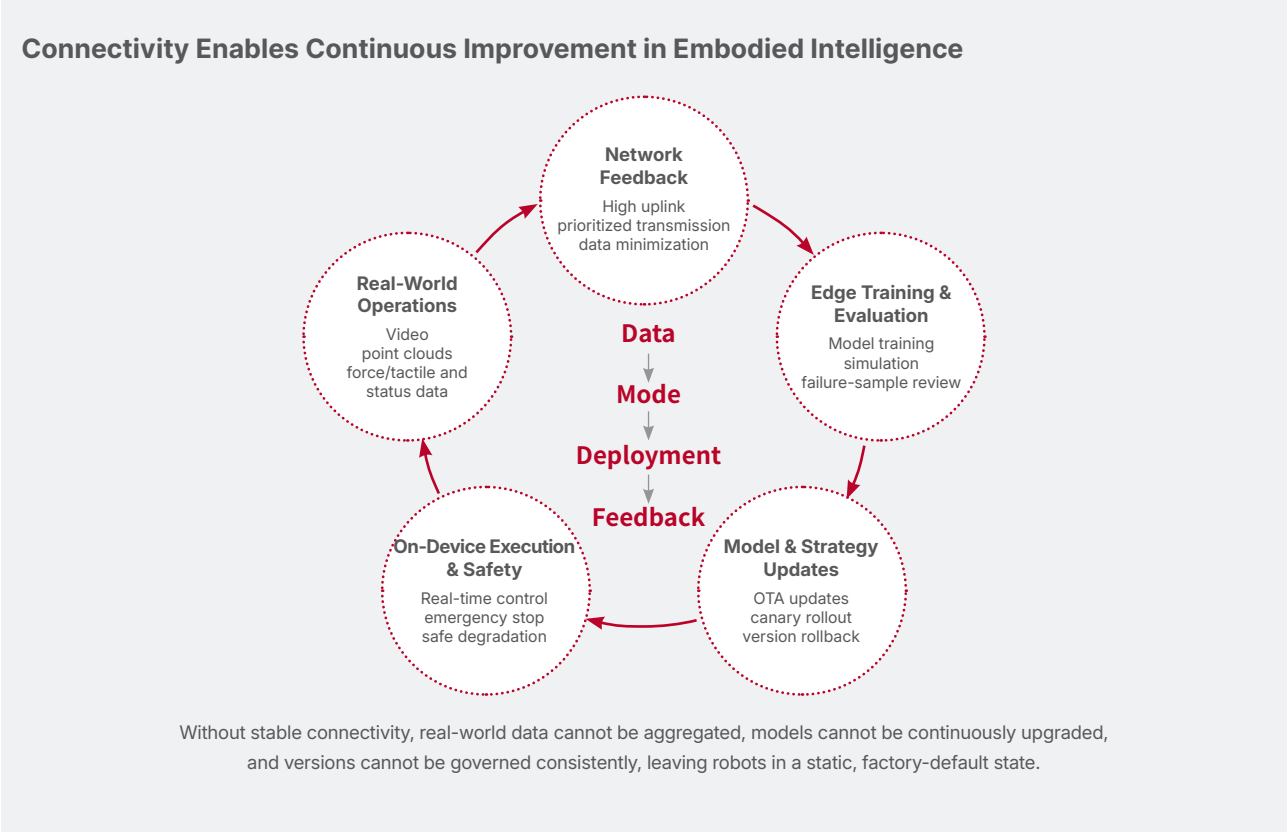

Figure 1. Connectivity Supports the Continuous Improvement Loop for Embodied Intelligence

Source: Prepared by the research team based on public industry information

Chapter 2.

Single-Robot Limits and the Role of Connectivity:
Connectivity as a Key Path to Operating Embodied Intelligence at Scale

As robots move beyond pre-programmed behaviour into dynamic, open real-world environments, the robot itself still faces four major bottlenecks: compute, data, battery endurance and cost.

2.1 Four Coupled Constraints on the Robot:
Computing, Data, Endurance, and Cost

Computing power ceiling

The size, weight, power consumption and heat dissipation of the robot body impose hard constraints. The power budget available for computing chips on a humanoid robot typically ranges from several tens of watts to around 100 W, whereas a single GPU used for cloud-based large-model training typically consumes several hundred watts. High computing capacity brings significant power consumption, which reduces the endurance of embodied intelligence robots and increases cooling requirements.

Data silos

Without connectivity, each robot is a data silo. What it sees, the scenarios it experiences and the mistakes it makes cannot be shared with other robots. The model cannot keep improving: without new data, it remains at the level it had when it left the factory.

Endurance constraints

Computing power and endurance constrain each other. Adding high-performance chips means shorter operating time. In industrial settings, insufficient endurance directly prevents a robot from completing a full shift.

Cost pressure

If every robot is equipped with its own high-performance computing chip, the unit cost rises to a level that makes scaling difficult.

2.2 Four Structural Gaps on the Network Side:
Conventional Connectivity Is Not Yet Fully Adapted to Robot Services

Although embodied intelligence depends on networks, today's networks are not yet fully adapted to its needs. Four gaps remain:

The device-side connectivity gap

Although China has built the world's largest 5G network, connectivity at the robot end has not yet been fully established. Most robots do not ship with a cellular module as standard; many rely on Wi-Fi or local links only, and wide-area cellular connectivity is an optional feature rather than a default one.

Insufficient adaptation to the service model

The service model of embodied intelligence differs markedly from that of smartphones: it is uplink-heavy (smartphone traffic is mainly downlink), bursty (rather than continuous streaming) and has high determinism requirements (most consumer mobile services are delivered on a best-effort basis). The adaptation of existing networks to robot services is still at an early stage.

Lack of unified standards

Robot communication protocols are fragmented, and there are no unified standards for interoperability across brands and models. As a result, even where network connectivity exists, robots from different vendors find it difficult to collaborate. A technical system and standards framework for embodied intelligence robots and mobile communications needs to be developed, with a focus on key areas such as agent connectivity, agent collaboration and device-network coordination.

Cost concerns

Enterprises are concerned that adding communication modules will increase hardware costs, that moving to the cloud will create ongoing operating expenses, and that connectivity will introduce cybersecurity risks. Current deployment volumes are too low for the cost of communication modules, chips and other hardware to be spread effectively, which further limits enterprises' willingness to invest in adding communication capabilities to robots.

2.3 Root Cause:
Robots Are Still Treated as Isolated Endpoints Rather Than System Nodes

Insufficient computing, closed data, difficult collaboration, and difficulties in remote management and security governance may appear to be separate problems, but they largely stem from the same architecture: robots are designed as isolated devices expected to perform all perception, decision-making, and execution on their own. In this architecture, external computing resources cannot be called on demand, other robots cannot share perception or task states, and operations platforms cannot centrally manage identities, versions, and permissions.

Optimising the robot body can ease single-robot performance bottlenecks, but it cannot solve system-level problems. Higher-performance chips can increase a robot's inference speed, but its experience still cannot be shared with other devices. Larger batteries can extend a robot's operating time, but task allocation and path conflicts among multiple robots still require external coordination. Stronger on-board models can increase autonomy, but operators still cannot audit the robot's behaviour remotely or take over safely when necessary. Data sharing, multi-robot coordination and remote governance all depend on connections between devices, and between devices and platforms. For embodied intelligence to move from individual prototypes to large-scale production systems, an architectural shift is needed.

2.4 The Way Forward:
From Standalone Intelligence to Connected Intelligence

A core aspect of connectivity is placing each task at a suitable computing location according to its timeliness and computing requirements, and linking these locations into a coordinated loop through the network. For example, hard real-time safety functions such as joint servo control, balance control and emergency stop must remain on the robot body; visual fusion, local planning and on-site task orchestration can be deployed at the edge; large-model training, knowledge bases, long-horizon planning and cross-regional scheduling can be deployed in the cloud; and identity, permissions, logs and version management, together with operational functions such as billing, can be handled by an operations management platform. This is a logical allocation of functions; actual deployments may be distributed or shared across multiple platforms.

Single-Robot Problem	Connected Solution	Expected Outcome
Insufficient compute	Use edge/cloud resources on demand for complex inference and training	On-demand access to complex inference, with safety and real-time loops kept on the robot body
Model stagnation	Real-robot data backhaul, failure analysis and phased model rollout	A close loop of data–model–deployment–feedback is established
Single-robot isolation	Share maps, locations, task states, and capability descriptions	Multi-robot collaboration and orchestration of heterogeneous devices are supported
Inadequate security and safety control	Digital identity, access authentication, behavior auditing and remote takeover	High-risk and sensitive scenarios become controllable and traceable
Difficulty of operation and maintenance at scale	Remote monitoring, OTA updates, alarms, and version rollback	Per-device maintenance costs are reduced and replication at scale is supported

Source: Compiled by the research team

Network dependence increases significantly when services require remote supervision, multi-robot collaboration, cross-site operation and maintenance, continuous updates or unified governance. The case for connectivity therefore lies primarily in system-level operations, not in replacing real-time control on the robot. By degree of network dependence, embodied intelligence capabilities can be divided into three categories:

Network-dependent cross-site operations, remote supervision and takeover, multi-robot scheduling, centralized maintenance, model and credential lifecycle management, and cross-party collaboration. These are often a key foundation for deployment at scale.

Network-enhanced external knowledge access, on-demand computing offloading, shared learning, high-precision positioning assistance and non-real-time model updates. These can add value, but their use should be decided according to scenario, cost, and data boundaries.

Local autonomy required joint servo control, balance, collision detection, emergency stops, basic obstacle avoidance and a safe state upon loss of connectivity. These must not depend on any external network connection or remote inference.

2.5 Communications Infrastructure Is Becoming Ready to Move from Connectivity to Enablement

5G deployment is maturing, led by large-scale markets. 5G networks are now commercially deployed in many markets worldwide, although coverage, standalone (SA) deployment and network capabilities vary significantly between markets. China currently has the largest deployment: as of the end of April 2026, it had 5.009 million 5G base stations and 1.262 billion 5G mobile subscribers [3], and by June 2026, 5G applications had been adopted in 91 of the 97 major categories of its national economy, with more than 182,000 application cases [4]. Where such wide-area coverage exists, it provides the basic connectivity needed for robots operating across campuses, across cities and outdoors.

5G-Advanced is at an early stage of rollout

Operators in a number of markets have begun commercial 5G-A deployments, with China again the most extensive: according to MIIT's interpretation of its 2025 Statistical Bulletin on the Communications Industry, 5G-A covered more than 330 Chinese cities by the end of 2025 [5]. Under specific deployment and test conditions, 5G-A can provide hundreds of Mbps of uplink capacity, millisecond-level latency within local areas, and high reliability. For embodied intelligence, these capabilities, combined with edge computing, can provide a network foundation for multimodal data backhaul, mobile operations and remote collaboration. In most markets, however, they are not yet widely available, and deployments should be planned against the capabilities actually offered by local operators.

Chapter Takeaway

Operating embodied intelligence at scale increasingly depends on connectivity. This is not because the robot body is no longer important, but because its physical limits prevent it from handling complex cognition, continuous learning, collective collaboration, and full-lifecycle governance all at once.

Chapter 3.

Connected Embodied Intelligence: Concept and Technical Architecture for Device-Edge-Network-Cloud Collaboration

Chapter 2 set out the case for connectivity. Connecting embodied intelligence, however, is not simply a matter of fitting a communication module to a robot. It involves rethinking the architecture, the connectivity options, and the technology stack. This chapter sets out what connectivity means and the technical architecture it requires, covering the definition, the layers of connectivity and the technical architecture.

3.1 Connectivity Means Redistributing Intelligence, Not Just Adding a Communication Module

Connected embodied intelligence keeps real-time control and safety autonomy local. On that basis, it links the robot body, edge nodes, communication networks, cloud-based models, other agents, people and business systems through cellular mobile communications, Wi-Fi, industrial Ethernet, mesh networking and other connectivity options, forming an intelligent system based on

Typical Architecture for Connected Embodied Intelligence: End-Edge-Network-Cloud Collaboration

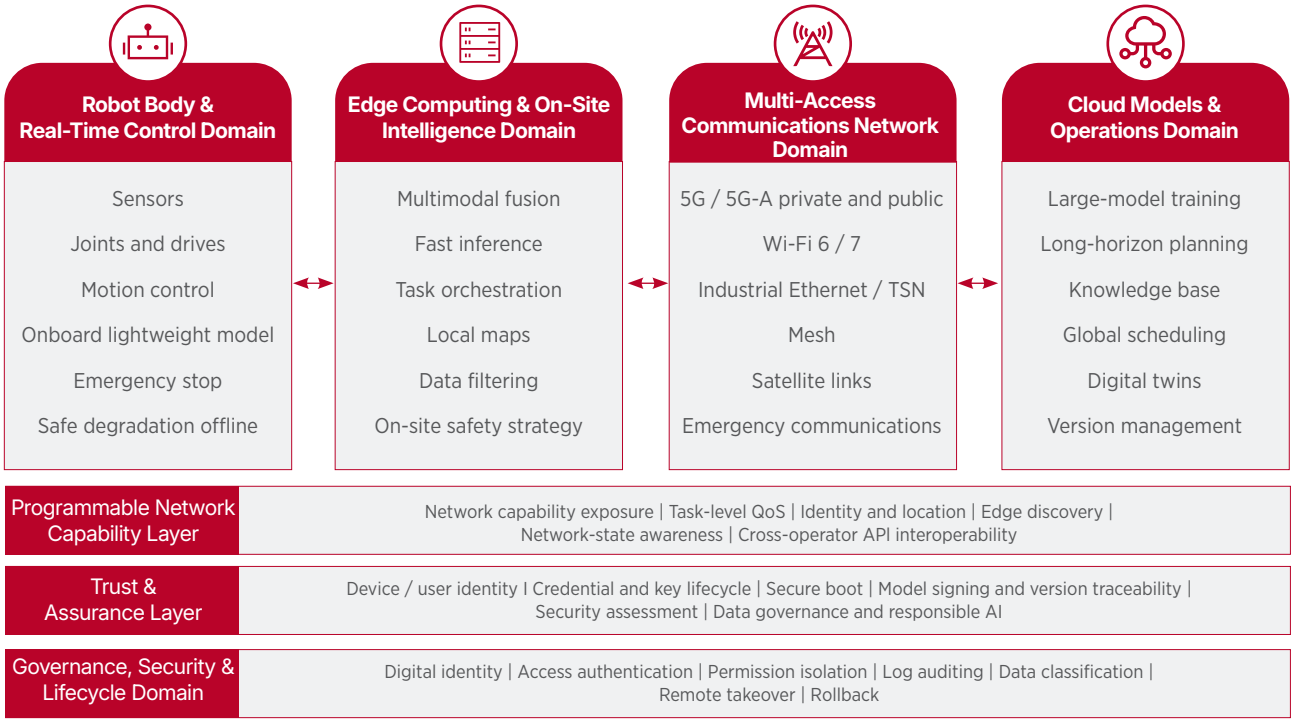

Figure 2. Device-Edge-Network-Cloud Typical Architecture for Connected Embodied Intelligence

Source: Prepared by the research team

device-edge-network-cloud collaboration. Its core is not to send all data to the cloud. Instead, it applies tiered collaboration, dynamic scheduling, continuous iteration and security governance across the device, edge, network and cloud, according to task timeliness, safety level, data sensitivity and computing requirements.

Connectivity is therefore not simply the addition of a communication module, but an architectural shift from standalone intelligence to connected intelligence. The local "cerebellum" handles immediate perception and execution, the edge- or cloud-based "brain" handles complex decision-making, and the communication network provides connectivity and service assurance between the two. ("Brain" and "cerebellum" are used here only as explanatory metaphors.)

3.2 Key Characteristics of Connected Embodied Intelligence: From Transferring Data to Assuring Tasks

The network requirements of embodied intelligence services can be summarised in six characteristics. These characteristics mean that network architectures designed mainly for smartphone services need targeted enhancement.

First, uplink-heavy traffic. A robot is a mobile sensor platform that continuously generates multiple streams of video, point clouds, speech, tactile and status data, so uplink capacity is often more critical than for conventional smartphone services.

Second, traffic bursts. Data volumes are manageable during routine patrols but rise sharply when the robot encounters anomalies, is teleoperated or performs high-precision grasping.

Third, heterogeneous multimodal traffic. High-definition video, point clouds, small control packets, logs and model files share the same network, with significant differences in packet size, periodicity and priority.

Fourth, complex mobility and obstruction. Robots move among metal shelving, robotic arms, people and equipment, and channel conditions change rapidly with the robot's posture, position and obstructions.

Fifth, sensitivity to tail latency. Low average latency does not guarantee stable task performance; 99th- and 99.9th-percentile latency (P99/P99.9) and jitter better reflect occasional stalls.

Sixth, task-dependent information value. Remote emergency-stop commands and safety-status reports are more valuable than routine logs (local emergency stop is always handled on the robot body), and key frames and anomalous point clouds are more valuable than large volumes of repetitive raw data.

How do sensor configurations translate into network requirements? The network load of embodied intelligence is determined first by how many sensors a robot carries, which data needs to be uploaded from the robot body, and at what frequency and compression it is transmitted. At the planning stage, bandwidth should be derived from the service data sources. The figures below are illustrative assumptions for planning estimates only; final values should be based on device encoding parameters and on-site measurements.

Data Source	Typical Configuration / Assumption	Implications for Network Planning
RGB Video	Four 1080p video streams; assume approximately 4–8 Mbps compressed bitrate per stream	Sustained uplink of approximately 16–32 Mbps; with multiple robots operating concurrently, loads must be aggregated and congestion at P95/P99 considered
Depth / Stereo Vision	One or two depth/stereo streams, with raw, feature, or event streams selected according to the task	Uploading raw data to the cloud greatly increases bandwidth; feature extraction on the device or at the edge is preferred
LiDAR / Point Clouds	One or two point-cloud sensors; whether full point clouds are uploaded depends on localisation, mapping and remote diagnostics requirements	Full backhaul is sensitive to uplink capacity and jitter; edge fusion and upload of key frames and anomalous segments can be used instead

Data Source	Typical Configuration / Assumption	Implications for Network Planning
Status and Control	High-frequency small packets for joint, location, health, and task status	Low bandwidth usage, but determinism, tail latency, packet loss and priority assurance are more important
Model / Log Files	Model packages, replay logs and batch uploads of failure cases	Higher latency is tolerable; this traffic should be isolated from real-time control traffic and transmitted during off-peak periods

3.3 Three Layers of Connectivity:
Robot-to-Cloud, Robot-to-Robot and Robot-to-Human

Robot-to-cloud connectivity addresses how single-robot capability can be continuously extended. The robot uploads selected perception data, task context and operational logs to the edge and cloud, where large models, knowledge bases and compute pools perform complex inference, training and global optimisation. Models, skills or task-level instructions are then delivered back to the robot.

Robot-to-robot connectivity addresses how multiple robots can complete a task together. Multiple robots share environmental perception, location and intent over the network and negotiate tasks through a scheduling platform or peer-to-peer communication, moving from individual operation to coordinated fleet operation. The key to collective intelligence is not merely that devices are online at the same time, but that state semantics are consistent, clocks are synchronised, conflicts can be resolved and faults can be isolated. In emergency command or large-scale public security operations, robots of different types can form coordinated groups based on their specialised capabilities, communicate in real time, share environmental information and task status, and negotiate and divide tasks within the scope authorised by commanders.

Robot-to-human connectivity addresses how robots can be supervised, taken over and worked with. In high-risk scenarios such as power, firefighting and mining, operators need high-definition video, depth information and equipment status, and must be able to take over remotely when necessary. Here the network simultaneously carries sensor backhaul, control commands, identity authentication and operation auditing, and is a key factor in whether teleoperation can be introduced safely and reliably into production processes.

3.4 Four Networking Tiers:
Different Scenarios Require Diverse Communication Networks

Network Tier	Typical Technologies	Main Tasks	Design Priorities
In-Robot Network	EtherCAT, CAN/CAN FD, TSN, ROS 2/DDS, etc.	Hard real-time communications among joints, drives, sensors, and controllers	Strictest latency and smallest range; must support offline operation
On-Site Local Network	Industrial Ethernet/TSN, Wi-Fi 6/7, 5G private networks	Edge inference, task scheduling, and data loops in factories, warehouses, and campuses	Determinism, keeping data within the local domain, and manageability
Wide-Area Public / Private Network	5G/5G-A public networks, industry private networks, APN/DNN-based access, dedicated fibre lines (site-to-cloud backhaul)	Cross-campus management, mobile operations, cloud-based models, and remote maintenance	Continuous coverage, mobility and security isolation

Network Tier	Typical Technologies	Main Tasks	Design Priorities
Weak-signal/no-network ad hoc networking	Mesh, direct device-to-device links, temporary base stations, satellite links, public-safety emergency networks (e.g. TETRA)	Field exploration, emergency rescue, disaster sites	Rapid deployment, autonomous coordination and graceful degradation upon loss of connectivity

Source: Compiled by the research team from industry reports and publicly available standards, including 3GPP TS 22.104 [36], 3GPP TS 22.261 [37] and 5G-ACIA [39]

These networks are not mutually exclusive alternatives but form a layered combination. For example, an automotive factory may use industrial Ethernet for fixed-equipment control, a 5G private network to connect mobile robots, Wi-Fi for non-critical O&M terminals, and a dedicated line to connect to a cloud-based training platform. An emergency scenario may use a 5G public network, a temporary private network, mesh networking and satellite links at the same time. The key to selecting networks for a scenario is not to pursue the most "advanced" technology, but to meet the requirements of end-to-end task completion, data boundaries, coverage continuity and cost.

The table below gives reference network requirements for typical scenarios. These are initial planning assumptions for typical scenarios, not unified standard requirements.

Scenario	Primary Network Tasks	Reference Uplink Bandwidth	Reference Latency	Reliability Focus	Typical Combination
Industrial assembly / fine manipulation	Robot control kept local; edge-based vision and task planning	10–100 Mbps per robot (depending on video and point-cloud configuration) [37][38]	20–50 ms at task level; lower for on-board control [36][39]	99.99% or higher; redundancy required for critical tasks [36]	Industrial Ethernet/ TSN + 5G private network / Wi-Fi 7
Warehousing and logistics / multi-robot collaboration	Location, routes, task status, video	1–50 Mbps per robot [39][40]	20–100 ms for coordination [36]	99.9–99.99% for status and video; safety-related control loops may require more than 99.9999% [36]	5G private network, Wi-Fi 6/7, edge scheduling
Energy inspection / teleoperation	HD video, meter reading, remote fine manipulation	20–100 Mbps per robot [37][38]	20–50 ms for teleoperation; less stringent for status monitoring [37][38]	99.99% or higher [36][37]	Wide-area 5G-A coverage + edge UPF / dedicated line [39]
Emergency rescue	Video, thermal imaging, gas detection, maps, control	20–200 Mbps per robot [15]	20–50 ms for critical control [37]	High reliability; multi-link / ad hoc networking required [37]	5G/5G-A + mesh + temporary base stations / satellite
Commercial / home services	Voice, video, orders, cloud-based skills	5–50 Mbps per robot	100–300 ms for interaction	Around 99.9%; safety-related actions kept local	Wi-Fi + cellular backup / secure public-network tunnel
Data collection and training	Multiple raw video streams, point clouds, logs	50–500 Mbps per robot, or offline batch transfer [11][38]	Second-level latency acceptable [38]	Data integrity and cost	High-uplink private network / fibre / edge caching

Source: Compiled from the Research Report on Embodied Intelligence Robots and Mobile Communication Technologies (2025 Edition) [2], 3GPP TS 22.104 [36], 3GPP TS 22.261 [37], 5G-ACIA white papers [38][39][40], public case studies [11][15] and engineering experience. Values without a citation are planning assumptions of the research team. Values are planning references and must be calibrated against on-site measurements. Reliability refers to the end-to-end transmission success rate within the latency budget.

Commercial and home service scenarios can be further divided into commercial, hotel, hospital and home settings.

Home settings place greater emphasis on privacy, local safety and low cost. The network mainly carries voice and video interaction, model invocation, remote O&M and authorised data loops, and robots must be able to operate autonomously and locally when the network is unavailable. Hotel settings place greater emphasis on movement across floors, coordination with access-control, lift and guest-room control systems, and multi-robot scheduling, requiring continuous coverage, identity authentication and cross-device interfaces. Hospital settings involve patient privacy, delivery of medicines and supplies, and human-robot coexistence. In addition to continuous coverage, they require stronger data minimisation, tiered permissions, audit trails and human confirmation of high-risk actions.

3.5 5G, 5G-A, and 6G

Dimension	5G	5G-A	6G (Vision / Research Stage)
Standardisation stage	IMT-2020; 3GPP Rel-15 to Rel-17	3GPP Rel-18 and subsequent 5G evolution	As of November 2026: ITU-R WP 5D has developed draft IMT-2030 technical performance requirements, subject to approval by Study Group 5; 3GPP 6G work is in the Release 20 study phase, with normative specifications planned for Release 21 (from March 2027)
Core focus	Enhanced mobile broadband, massive connectivity, ultra-reliable low latency	Enhanced uplink, determinism, positioning, sensing, network intelligence and multi-link coordination	Deep integration of communication, sensing, computing, AI and ubiquitous connectivity
Peak data rate (reference)	ITU minimum requirements: 20 Gbps downlink, 10 Gbps uplink (ideal conditions)	No single globally unified "peak target"; focus on enhancing live-network capability and scenario-specific assurance	ITU vision examples: 50/100/200 Gbps; final values still being developed
Air-interface latency (reference)	eMBB 4 ms, URLLC 1 ms (unloaded, small packets, air interface only)	Tail latency and jitter reduced through enhanced scheduling, deterministic networking and edge deployment	Vision research target 0.1–1 ms (air interface); not equivalent to application end-to-end latency
Reliability (reference)	Success probability of $1\text{-}10^{-5}$ for 32 bytes within 1 ms (ITU minimum requirement)	Enhanced reliability, redundancy and fault recovery for industrial and mission-critical use	Vision research target $1\text{-}10^{-5}$ to $1\text{-}10^{-7}$
Main value for embodied intelligence	Wide-area access, mobile connectivity, baseline low latency	High uplink capacity, mobility continuity, differentiated QoS, positioning and edge collaboration	Integrated communication, sensing, computing and intelligence; AI-native networks; agent communication

Source: ITU-R M.2410, ITU-R M.2160, and progress on IMT-2030 technical requirements and evaluation as of 2026 [6][7][8]. The 5G-A column summarises evolving capabilities; vendor marketing figures are not treated as unified standards.

5G already provides mobile connectivity, QoS and edge support. 5G-A continues to enhance these capabilities in Rel-18 and subsequent releases, but availability depends on network and device deployment. As of November 2026, IMT-2030 is still in the research and standards development stage. The 6G values in the table are vision targets or draft requirements and should not currently be regarded as commercial commitments or network performance indicators.

It should be emphasised that the air-interface latency, peak data rate and reliability values in the standards are theoretical values defined under specific test conditions. They are not equivalent to the end-to-end performance of a robot, from sensor capture, network transmission and model inference through to action execution. Embodied intelligence projects should take task success rate as the ultimate objective, measure communication, computing, control and application latency separately, and avoid adopting standard values directly as requirements for all robot scenarios.

5G-A capabilities are being deployed progressively based on Release 18 and subsequent releases. Available features and commercial maturity vary by market, network and device ecosystem. Key capabilities for embodied intelligence may include:

Network Capability	Role in Embodied Intelligence	Key Application Metrics
High uplink capacity	Supports backhaul of multiple video streams, point clouds and data from physical robots	Peak / guaranteed uplink rate; P95 throughput under congestion
Low latency and low jitter	Supports teleoperation, task-level inference and multi-robot synchronisation	End-to-end P50/P99/P99.9 latency; jitter
High reliability	Reduces loss of critical control and status messages	Packet loss rate; continuous task success rate; fault recovery time
Continuous coverage and mobility	Maintains connectivity as robots move across campuses, roads and sites	Handover success rate; number of short interruptions; coverage gaps
Edge computing and local breakout	Shortens the inference path and keeps data within the local domain	Edge computing latency; compute utilisation; reduction in backhaul traffic
Differentiated QoS	Tiered assurance for control, video, logs and model files	Effectiveness of critical-service pre-emption; congestion isolation
Enhanced positioning and sensing	Assists robot localisation, trajectory tracking and environmental perception	Positioning accuracy; update rate; stability under obstruction

Source: Compiled by the research team

5G-A is an evolutionary stage of 5G, not a separate network deployment mode. Its specific capabilities depend on SA deployment, spectrum, device capabilities, the core network, RAN configuration, edge deployment and the operator's commercial offering. Robot projects should not be accepted on the basis of the "5G-A" label alone, but against end-to-end KPIs/SLOs and on-site testing.

3.6 Layered End-to-End KPIs: From Network Metrics to Task Metrics

Embodied intelligence projects should not use a single air-interface metric as a substitute for overall system performance. We recommend dividing measurement into six layers: radio access, transport and core network, edge and cloud, robot system, task, and operations. Correlation analysis should be established to trace network anomalies through to task outcomes. Every metric should have a defined measurement point, statistical window, percentile, concurrent load and anomaly condition.

Layer	Suggested Metrics
Radio access	RSRP/RSRQ/SINR, uplink throughput, air-interface latency, packet loss, handover interruption
Transport and core network	RTT, jitter, path availability, UPF and edge path latency
Edge and cloud	Queuing time, inference time, resource utilisation, cold-start time
Robot system	Perception-to-decision latency, decision-to-action latency, state synchronisation error
Task	Task success rate, human takeover rate, safe-stop rate (share of tasks in which a safe stop is triggered by network or system anomalies), cost per task
Operations	Fault recovery time, version release success rate, cross-site replication cycle, SLO attainment rate

Chapter 4.

Core Value of Connected Embodied Intelligence

The device-edge-network-cloud architecture provides the technical foundation for connected embodied intelligence, but its real industrial value lies in translating that foundation into concrete productivity gains. This chapter sets out four core values that connectivity brings to embodied intelligence.

4.1 Core Value 1:

Layered Coordination Between the "Brain" and the "Cerebellum" Enables Continuous Upgrades of Complex Intelligence

The role of connectivity is to link the "brain" and the "cerebellum" into a layered, coordinated system, not to replace the robot body with the cloud. The cerebellum resides on the robot body and is responsible for motion control, safety state and protection upon loss of connectivity. On-site edge nodes handle multimodal fusion, local mapping, visual inference and low-latency task planning. The cloud-based brain handles large models, knowledge bases, long-horizon planning, model training and global optimisation. The robot sends task-relevant status and perception data upstream; the edge and cloud return task-level policies, target poses or skill invocations; and the local controller converts these into continuous motion.

From an industry perspective, brain-cerebellum coordination means that robot capabilities are no longer permanently locked to a given generation of on-board hardware. Models and knowledge can be iterated continuously at the edge and in the cloud, with the robot body accessing new capabilities through interfaces. The same brain capabilities can also be adapted to different forms, such as wheeled, dual-arm and humanoid robots, reducing duplicated development costs. Above all, it establishes an engineering path for continuous capability upgrades, turning robots from equipment delivered once into production tools that can evolve over the long term.

As set out in Section 2.4, safety-critical closed loops must never depend on external networks. When the network is interrupted, the robot should slow down, pause, return to base or enter a safe posture, rather than continue unsupervised high-risk actions.

4.2 Core Value 2:

On-Demand Compute Offloading Optimises Device Cost and Energy Use

Connectivity does not simply mean moving computing to the cloud. It enables tiered offloading according to task timeliness and data sensitivity, following the allocation set out in Section 2.4. The network can also support model partitioning, feature transmission, caching and dynamic scheduling, so that the computing location can adjust to network conditions, task load and battery level.

The economics must be assessed on a total cost of ownership (TCO) basis. Compute offloading can reduce peak on-board

configurations, increase hardware reuse and extend product lifecycles, but it also adds costs for network deployment, edge servers, cloud computing, data traffic and O&M. Projects should compare cost per task, effective robot working hours, human takeover rates and downtime losses. Connectivity forms an economic basis for mass deployment only when the gains in utilisation and operational efficiency from shared computing exceed the additional network costs.

TCO Dimension	Main Components	Optimisation Through Connectivity
Robot body cost	Chips, memory, thermal management, batteries, structural reinforcement	Reduce peak configurations while retaining computing for safety and basic autonomy
Network cost	Modules, private/public networks, APs, data traffic, dedicated lines	Tier by scenario; avoid applying the highest assurance level to all services
Edge and cloud cost	Edge servers, GPUs, model invocation, storage	Shared pooling, elastic scheduling, hot/cold data tiering
Operational benefits	Effective working hours, task success rate, staff savings, reduced downtime	Validate through cost per task and payback period

Source: Compiled by the research team

4.3 Core Value 3:
Multi-Robot Collaboration and Collective Intelligence

Connectivity turns multiple robots from merely co-existing into working together. The technical chain includes: unified identity and capability descriptions, so that the platform knows what each robot can do; shared maps, locations and task status, reducing duplicated perception and path conflicts; task orchestration for role allocation and dynamic replanning; time synchronisation and priority mechanisms to assure critical coordination messages; and task handover and local isolation when faults occur. Collective intelligence is therefore not simply a matter of adding more devices, but of forming system-level perception and decision-making through the network.

Value for Industry

Connectivity raises the unit of value in embodied intelligence from the individual robot to the entire operational system. When perception, tasks and capabilities can be shared, information collected by one robot can serve multiple devices, and when one device fails, others can take over. System resilience and asset utilisation improve as a result.

4.4 Core Value 4:

Trusted Connectivity, Trustworthy AI and Functional Safety Together Form the Foundation of Trust for Deployment at Scale

As embodied intelligence robots move from laboratories and showcase settings into industrial manufacturing, energy and power, emergency rescue, healthcare, commercial spaces and homes, safety and security issues are no longer limited to collisions and mechanical failures of the robot body. They extend to device identity, network access, data flows, model decisions, permission control and remote operation. Once a robot becomes an agent that can perceive, decide and act on the physical world autonomously, its security boundary expands from single-device security to system-level security spanning devices, networks, models and platforms.

Deploying embodied intelligence at scale first requires robots to be identifiable, constrainable, able to be taken over and traceable. Trusted connectivity addresses who is allowed to connect and whether data has been tampered with in transit; it cannot guarantee that the data was accurate at the source. Trustworthy AI constrains model decisions and autonomous behaviour. Functional safety ensures that the robot body can still enter a controlled, safe state when the network, models or platforms behave abnormally.

Trusted connectivity uses device digital identity, mutual authentication, encrypted transmission, integrity protection and permission isolation to prevent unauthorised devices and personnel from entering the control chain. It should be stressed that authentication is not authorisation: a device that successfully connects to the network does not thereby gain permission to perform actions such as opening doors, operating high-voltage equipment or taking over a robot. Trustworthy AI requires that, in high-risk tasks, model outputs are checked by rules, safety controllers or action-feasibility validation, and that a pause, re-perception or human takeover is triggered when confidence drops, the scenario falls outside the training distribution or execution fails repeatedly. Functional safety requires that hard real-time safety loops, such as joint servo control, collision detection, emergency stop, speed limits, spatial limits and loss-of-connectivity protection, remain on the robot body. The safety design and validation of robot bodies should follow applicable robot and machinery safety laws, standards and scenario requirements. Industrial robot scenarios can be assessed with reference to ISO 10218-1:2025 and ISO 10218-2:2025 (the latter incorporates the requirements for collaborative applications formerly set out in ISO/TS 15066). These standards mainly address industrial and collaborative robot applications and should not be generalised as unified safety standards for home, public-service, healthcare or other non-industrial robots. This paper does not replace any applicable functional safety standard.

Safety and security capabilities should be built into the architecture of the robot body, network, edge, cloud and operations platform from the system design stage. In high-risk scenarios, the priority among autonomous execution, platform scheduling, human takeover and safe stop should be clearly defined.

Chapter Takeaway

The four values are not independent of one another; together they form the system capabilities needed to scale embodied intelligence. Layered brain-cerebellum coordination extends the boundaries of single-robot intelligence; on-demand compute offloading improves resource utilisation; multi-robot collaboration moves robots from standalone devices to operational systems; and trusted connectivity, trustworthy AI and functional safety together establish the foundation of trust for deployment at scale. All four rely on coordination among communication networks, computing, data and operations platforms, and ultimately aim to make embodied intelligence usable, replicable, operable and governable.

Chapter 5.

Industry Case Studies

Building on the four dimensions of value set out in Chapter 4, this chapter uses industry case studies to examine how these values materialise in real-world settings. It should be noted that the contribution of connectivity to final business outcomes varies across cases. This chapter therefore classifies cases into three categories according to the degree of attributability.

A Category Connectivity capabilities have a relatively direct, measurable relationship with business outcomes, and both network metrics and task results have been published.

B Category The connected system is a necessary component, providing backhaul, supervision, scheduling and communication assurance, but its contribution is difficult to quantify separately.

C Category The case mainly demonstrates on-device perception, inference, motion control and algorithmic capabilities, and its relevance to connectivity lies mainly in the requirements it reveals.

The A/B/C classification reflects the degree to which business outcomes can be attributed to connectivity; it is not a rating of source reliability. Case data are drawn from the cited public reports or from disclosures by project participants and have not been independently verified by GSMA. The measurement start and end points, network load, number of devices, percentiles and statistical windows of all metrics are as defined in the original sources. Inclusion of a case does not constitute an endorsement by GSMA of any company, product, service or solution; company and product names are used only to identify the cases described in the cited sources.

Category B

5.1 Case Study 1:

5G-A Multi-Robot Private Network, Supporting On-Demand Offloading with Edge Computing

Item	Details
Project Name	EasyOn·Robot 5G-A Multi-Robot Private-Network Solution
Participants	China Telecom, ZTE, DroidUp, and AgiBot
Connectivity	5G-A private network on site, with ZTE NodeEngine edge computing boards; robots upload sensor, location and status data to the on-site edge for positioning and task orchestration.
Public Release	December 2025, published as a GSMA Foundry case study
Deployment / Validation Format	Multi-robot entertainment collaboration, unmanned convenience stores, and other scenarios
Case Source	GSMA Foundry official case study [11]

Project Overview and Challenges

GSMA Foundry has published the EasyOn·Robot 5G-A multi-robot private network case study. The solution was developed jointly by China Telecom, ZTE, DroidUp and AgiBot and, according to the case study, has been piloted in scenarios such as multi-robot entertainment collaboration and unmanned convenience stores. These scenarios require multiple robots to continuously upload high-definition visual, positioning and status data, with an on-site platform performing inference, positioning and task orchestration. Relying entirely on on-board computing would require each device to be equipped with higher peak computing capacity, and would make it difficult to build a data and task flow shared across devices [11].

Connectivity and Edge Collaboration Solution

EasyOn·Robot uses a 5G-A private network to connect different types of robots and uses ZTE NodeEngine edge computing boards to combine the necessary 5G functions with on-site edge computing. Robots upload high-resolution sensor data, location and operational status to the on-site edge, where the edge platform performs high-precision positioning, task orchestration and data processing before sending task and coordination information back to the robots. High-traffic, low-latency services can therefore form a short closed loop within the campus, with complex computing handled by shared edge resources, while joint control, balance and safety protection remain on the robot body. This creates a layered structure in which the robot body handles real-time functions and the edge supplements computing capacity.

Published Results

Metric Category	Published Results
Technical performance	Maximum aggregate uplink throughput of 2 Gbps; guaranteed uplink of 200 Mbps per robot; air-interface latency below 10 ms; network availability of 99.99% (as reported by the vendor) [11][12]
Service capabilities	Supports multi-robot entertainment collaboration and unmanned convenience store processes including customer entry, product recommendation, self-checkout and product delivery

Metric Category	Published Results
Deployment value	As described in the case study, edge boards combine network capabilities with on-site edge computing, shortening the processing path for high-traffic, low-latency services
Architectural value	The robot body retains real-time and safety loops, while complex perception, positioning and task orchestration can use shared edge computing

Lessons Learned

This case shows that compute offloading for embodied intelligence is not simply a matter of moving models to the cloud, but of placing computation at different timescales in the most suitable location. The robot body retains hard real-time and safety loops; the edge handles high-bandwidth perception processing, positioning and task orchestration; and the cloud handles longer-cycle model training and operational analytics.

Category B

5.2 Case Study 2:

5G-A Embodied Intelligence Robots for Power Grid Inspection, End-to-End Demonstration of Remote Safety Control and Efficiency Gains

Item	Details
Project name	5G-A Embodied Intelligence Robot Power Grid Inspection Application Demonstration [14]
Participants	Guangdong Power Grid, China Mobile, Leju Robotics, Beijing Institute for General Artificial Intelligence (BIGAI)
Connectivity	China Mobile 5G-A covering the operational substation, carrying HD video and status uplink and VR-based remote control. The deployment model (standalone private network, network slice or shared public network) is not disclosed.
Launch date	Publicly announced in November 2025
Application scenarios	Inspection at operational power grid substations; operation of 110 kV bay control cabinets; voltage verification on 10 kV feeder cabinets
Core operations	Outdoor equipment temperature measurement; backhaul of meter and switch status; VR-based remote fine manipulation

Project Overview and Challenges

In November 2025, Guangdong Power Grid, China Mobile, Leju Robotics and BIGAI jointly announced a 5G-A embodied intelligence robot application demonstration for power grid inspection. The robots entered operational substations and carried out tasks including outdoor equipment temperature measurement, operation of 110 kV bay control cabinets and voltage verification on 10 kV feeder cabinets. Conventional manual inspection requires staff to enter high-voltage equipment areas, while relying solely on the robot's local autonomous judgement cannot cover all complex equipment states. What the scenario really needs is real-time supervision and fine-grained takeover capability, with the machine at the front line and people at a safe distance.

Connectivity and Remote Takeover Solution

The robot body handles movement, perception and action execution. 5G-A provides continuous connectivity across the substation, stable high uplink capacity, and what the project participants describe as millisecond-

level low-latency, high-reliability links. Head- and wrist-mounted cameras send first-person views of meter readings, switch status and other information back to the operations side, where operators use VR equipment for remote verification and fine manipulation. During operations such as 110 kV bay cabinet operation and 10 kV feeder cabinet voltage verification, the robot replicates the operator's remote actions on a 1:1 basis. The network therefore does more than upload video: it links status backhaul, human judgement, control commands and operation records into a single safety loop.

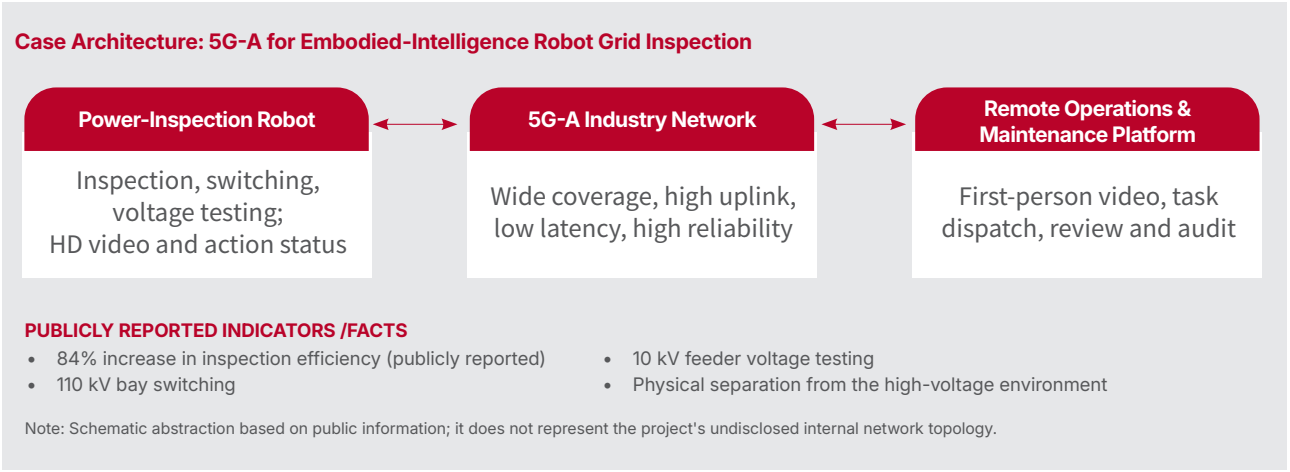

Figure 3. Abstracted Architecture of the 5G-A Power Grid Inspection Case

Source: Prepared based on public reporting by Xinhua Finance[14]

Published Results

Metric Category	Published Results
Technical performance	The project participants report stable high uplink capacity, millisecond-level low latency and high reliability; remote actions are replicated by the robot on a 1:1 basis
Service efficiency	The project participants report an 84% year-on-year increase in inspection efficiency (public materials do not specify the baseline, observation period or sample) [14]
Safety value	As described by the project participants, operators complete 110 kV bay cabinet operation and voltage verification on 10 kV feeder cabinets from a safe distance, physically separating people from the high-voltage environment
Operational value	High-definition video backhaul, remote review and fine-grained takeover are intended to enable robots to take on high-risk, repetitive tasks

Lessons Learned

In high-risk scenarios, the goal should not be to pursue fully unmanned operation indiscriminately, but to prioritise a safe operating model in which robots work at the front line, staff supervise from a safe location and remote takeover is available when anomalies occur. When this approach is replicated, site-wide coverage mapping, QoS for critical tasks, tiered handling of video and control traffic, operation logs, safe actions upon loss of connectivity and two-step confirmation for high-risk operations should be designed together, so that remote takeover becomes an auditable operating procedure rather than a demonstration feature.

Category B

5.3 Case Study 3:

China Mobile 5G-A Firefighting and Rescue Demonstration, Remote Safety Loops in Extreme Environments

Item	Details
Project name	"Industry-First 5G-A Embodied Intelligence Humanoid Robot Training Ground and Firefighting and Rescue Application Demonstration" (title as announced by the project participants) [15]
Participants	China Mobile Research Institute, China Mobile Jiangsu, Wujiang District Fire and Rescue Bureau (Suzhou), Huawei, Leju Robotics
Connectivity	China Mobile 5G-A at the training ground, with separate uplink channels for real-time video and full datasets, uplink enhancement (multi-carrier aggregation, supplementary uplink) and priority-based assurance. Reported as end-to-end dedicated communication assurance; whether the underlying network was public or private is not disclosed.
Launch date	June 2026
Location	Wujiang District, Suzhou, Jiangsu Province
Core tasks	Fire-source identification, obstacle clearance, valve operation, remote control
Source	Public materials from China Mobile Research Institute; Suzhou Daily reporting [15][16]

Project Overview and Challenges

On 22 June 2026, China Mobile, the Wujiang District Fire and Rescue Bureau in Suzhou and industry partners launched a 5G-A embodied intelligence humanoid robot training ground and firefighting and rescue application demonstration in Suzhou.

According to the project participants, Wi-Fi in conventional firefighting and emergency scenarios suffers from high interference, limited uplink bandwidth, high transmission latency and limited concurrent capacity, making it difficult to support large-scale, synchronised data collection by multiple robots. Reinforced concrete, dense smoke and dust can cause video stalls and control delays, and may even lead to loss of connectivity.

Connectivity and Network Assurance Solution

The training ground deployed a 5G-A network solution with dual transmission channels for real-time video and full datasets, integrating data collection, storage and real-time backhaul. The project participants report approximately 24 Mbps of uplink per video stream at the training ground, up to 150 Mbps of uplink for non-real-time data, and more than 600,000 training data records from physical robots. During the firefighting drills, uplink was approximately 15–20 Mbps, used for on-site video, status backhaul and remote operation [15]. These metrics come from a specific demonstration environment; the measurement endpoints, statistical windows and the network's independent contribution to task success have not been published.

According to the project participants, the 5G-A network provided end-to-end dedicated communication assurance for the firefighting robots during the drills, based on three network capabilities:

First, enhanced uplink.

Techniques such as multi-carrier aggregation and supplementary uplink meet the bandwidth requirements of machine-vision recognition and detailed operational assessment.

Second, real-time monitoring of network conditions and service demand.

Traffic fluctuations and changing transmission requirements are monitored in real time, so that network resources can be scheduled on demand and assurance targeted where it is needed.

Third, priority-based network assurance.

The network distinguishes service priorities and gives precedence to low-latency, high-reliability transmission of critical data, supporting a 1:1 mapping between the robot body and remote operation.

Lessons Learned

Where environments involve high temperatures, dense smoke, obstructed visibility and sudden obstacles, the network needs to help ensure that operators can see, that control remains effective and that the system can degrade safely upon loss of connectivity. For firefighting, mining, hazardous chemicals and disaster rescue, what can be replicated is not a particular bandwidth figure, but a closed-loop design of robot reconnaissance, multimodal data backhaul, remote assessment, remote takeover and on-board safety fallback.

Category B

5.4 Case Study 4:

Kuafu 5G-A Robot Torch Relay at the 15th National Games, Demonstrating Layered Brain-Cerebellum Coordination

Item	Details
Project name	5G-A Humanoid Robot Torch Relay at the 15th National Games
Participants	China Mobile, Leju Robotics; technical support from ecosystem partners including Harbin Institute of Technology and the Beijing Institute for General Artificial Intelligence (BIGAI)
Connectivity	China Mobile's in-service 5G-A network along the relay route (dual-band 2.6 GHz + 4.9 GHz, more than 20 sites optimised), with service-aware scheduling, priority protection for critical packets and local breakout. No separate private network was reported.
Launch date	2 November 2025
Deployment scale	More than 20 5G-A sites optimised along the route; one Kuafu robot completed a relay leg of approximately 100 metres
Application scenarios	National sporting event; dynamic outdoor mobility; human-robot torch handover
Source	Public materials from China Mobile and China Mobile Research Institute [9][10]

Project Overview and Challenges

The task took place in an open outdoor environment. The robot had to rely on its on-board motion "cerebellum" for gait, balance, payload and joint posture, while continuously sending back first-person video and operational data and receiving task decisions and anomaly handling from the cloud or the control centre. The task therefore tested both on-board autonomy and wide-area mobile connectivity.

Coordination Solution: On-board "Cerebellum" + 5G-A + Cloud-Based "Brain"

The project did not move running and balance control to a remote system. Instead, the upgraded on-board motion-control "cerebellum" handled real-time gait and posture loops. On the network side, 5G-A used dual-band 2.6 GHz + 4.9 GHz deployment, with more than 20 sites along the route optimised section by section to carry high-definition video, joint posture, control commands and other data types [9][10]. According to the project participants, mechanisms including service-aware traffic identification, intelligent resource scheduling, local breakout and priority protection for critical packets were used to provide a stable channel for task-level information exchange and remote assurance.

The completion of the torch relay resulted from on-board control, on-site tuning, task orchestration and network assurance working together; available public materials are insufficient to quantify the network's independent contribution to gait stability or task success rate [9][10].

Published Results

Metric Category	Published Results
Basic facts	No technical staff running alongside and no handheld remote control following on site; the robot completed a torch relay of approximately 100 metres while continuously carrying a 1.6 kg torch
Network deployment	Dual-band 2.6 GHz + 4.9 GHz deployment; more than 20 5G-A sites along the route optimised section by section [9][10]
Service results	Completed a continuous sequence of starting, running, waving and handover, with real-time backhaul of first-person ultra-high-definition video
System value	The on-board motion "cerebellum" maintained real-time closed loops, while 5G-A carried multimodal data and delivered cloud-based decisions, forming layered coordination

Lessons Learned

The torch relay shows that brain-cerebellum coordination is first and foremost an appropriate division of labour within the system, not a matter of handing all control to the cloud. For scenarios such as outdoor inspection, campus delivery and cultural tourism services, the structure of real-time on-board autonomy, continuous network coverage, cloud-based task capabilities and remote assurance can be reused. Coverage, handover and congestion testing should be completed before route deployment, and actions upon loss of connectivity, such as slowing down, pausing or entering a safe posture, should be defined in advance.

Category B

5.5 Case Study 5:

China Telecom "Lingsi Brain", Coordinated Scheduling of Heterogeneous Robots

Item	Details
Project name	"Lingsi Brain" Robot Collective Intelligence Scheduling Service [13]
Participants	China Telecom Tianyi IoT and ecosystem robot vendors

Item	Details
Connectivity	Robots connect to the Tianyi IoT AIoT and RaaS platforms, which carry event reporting, location and status synchronisation and task dispatch for "Lingsi Brain" scheduling. 5G-connected service robots were shown in public demonstrations; the access technology and network topology at commercial deployment sites are not disclosed.
Publication date	December 2024
Deployment scope	Campus enterprises in Guangzhou (Guangdong), Dazhou (Sichuan), Suzhou (Jiangsu) and elsewhere
Platform architecture	Tianyi IoT AIoT platform + RaaS service platform + TeleChat (Xingchen) AI large model + "Lingsi Brain"
Application scenarios	Coordinated delivery, patrol and cleaning in large buildings, hospitals, core equipment rooms and similar settings

Project Overview and Challenges

In December 2024, China Telecom Tianyi IoT publicly launched the "Lingsi Brain" robot collective intelligence scheduling service, which, according to the company, has been deployed in campus enterprises in Guangzhou (Guangdong), Dazhou (Sichuan), Suzhou (Jiangsu) and elsewhere. The problem it addresses is that campuses, buildings and hospitals often procure delivery, cleaning, patrol and other robots of different brands and types, each with its own maps, interfaces and back end, which tends to result in a separate system for each type of robot. The more devices there are, the more complex cross-task collaboration and operational scheduling become.

Unified AIoT, Large-Model and RaaS Scheduling Solution

According to the company, "Lingsi Brain" provides unified robot management, customisation and collective intelligence scheduling, with a "Kuaishan" delivery system to support deployment. In public demonstrations, a delivery robot that detects a cleanliness issue located it and called a cleaning robot to handle it. In hospital settings, patrol robots carry out security patrols while delivery robots transport medicines and supplies. The network carries event reporting, location and status synchronisation and task dispatch, enabling different robots to "discover" and "call on" one another within the same workflow.

Reported Deployment

According to public materials, "Lingsi Brain" has been deployed in campus enterprises in Guangzhou, Dazhou, Suzhou and elsewhere, suggesting that the combination of a unified connectivity foundation, unified capability management and collective scheduling has begun to move from exhibition concept into campus operations. This case most directly supports the third core value, multi-robot collaboration: collective intelligence does not require every device to have the same hardware and models, but requires different robots to share events, locations, tasks and capability status, with a common platform orchestrating tasks across devices. Large buildings, hospitals, core equipment rooms and similar settings can use this approach to combine individual capabilities such as delivery, cleaning and patrol into continuous workflows [13].

Lessons Learned

The real bottleneck in multi-robot collaboration is often not just wireless data rates, but whether robots can understand one another: identity, capabilities, maps, events, tasks and status must share common semantics. The next stage of connectivity should therefore focus on establishing, beyond connectivity itself, cross-brand capability descriptions, task interfaces, event models, status codes and permission systems, so that the platform can determine who can do what, where each robot currently is and whether it is authorised to accept a task. Only then will a growing number of robots translate into system-level productivity.

Category C

5.6 Case Study 6:

Robotera at China Post and SF Express Logistics Sites, Flexible Parcel Induction and the Path to Scale

Item	Details
Project name	Robotera Embodied Intelligence Robot Application for Logistics Sorting and Parcel Induction
Participants	Robotera, China Post, SF Express and other logistics companies
Connectivity	Not disclosed. Public materials describe coordination with on-site systems and operational data collection, but not the robot access technology, network topology or measured uplink, latency or reliability; no specific dependence on 5G is established.
Location	China Post Guangzhou Mail Processing Centre and logistics sites of China Post, SF Express and others
Deployment scope	According to public materials, the cooperation covers more than 10 logistics centres in North, East and South China and other regions
Typical tasks	Parcel picking, flipping, label orientation adjustment, sorting and induction
Source	Robotera public disclosures, Haidian News and Xinhua public materials [17][18]

Project Overview and Challenges

Parcel induction in express logistics involves high operating frequency, intensive repetitive labour and wide variation among parcels. Soft packages, cartons and other items differ in size, material, shape and label position, requiring equipment to identify, pick, reorient and accurately place items during continuous operation. Conventional automation is efficient at handling standardised items, but still requires manual support for non-standard parcels and complex operations.

According to public reporting, at the China Post Guangzhou Mail Processing Centre the Robotera M7 robot picks, flips and inducts parcels, turning labels face up before placing parcels onto conveyor equipment, exploring how flexible manipulation can complement existing automation systems.

Embodied Manipulation and On-Site System Coordination Solution

For applications at scale, the value of connectivity lies in linking robots, on-site logistics equipment and operational systems. The path involves three aspects. First, operational coordination: exchanging device status, induction cadence and anomaly information to improve coordination between robots and conveying and sorting equipment. Second, the data loop: using data on complex parcel handling, picking failures and anomaly handling for model optimisation, and deploying improvements to on-site devices after testing and validation. Third, operation and maintenance at scale: supporting unified maintenance and capability iteration across devices at multiple sites through device status monitoring, fault diagnosis and version management.

This scenario reflects a gradual path from autonomous single-robot manipulation towards system-level coordination on the production line. At present, robots are already performing autonomous parcel induction in real logistics environments, while data interoperability and operational linkage across the full equipment system remain a future direction. As on-site interfaces, data loops and operations management capabilities mature, robots could integrate further into logistics production systems, which would support cross-site replication and deployment at scale.

Published Results

Metric Category	Published Results and Scope
On-site operations	Continuous operations including parcel picking, flipping and face-up label placement have been demonstrated at the Guangzhou China Post site
Operational efficiency	Public reporting on the Guangzhou China Post case states a maximum induction rate of up to 1,200 items per hour [17]

Metric Category	Published Results and Scope
Deployment scope	Public materials state that cooperation with China Post, SF Express and others covers more than 10 logistics centres [18]
Basis for scaling	Public materials indicate expansion from a single site to multiple logistics sites; replicability across sites has not been independently assessed

Lessons Learned

As these links are gradually connected, capability gains at a single workstation can translate into shared benefits across multiple sites, allowing expansion in scale and system optimisation to reinforce each other.

5.7 Case Study 7:

(Data Governance Case; Not Rated for Network Attributability)

Privacy-First Design for Commercial Service Robots, Data Protection Practices Described by the Company

Item	Details
Project name	Privacy and data protection practices for commercial service robots, as described by the company
Participants	YUNJI Technology
Deployment scope	Hotels and other commercial service scenarios; localised overseas services and on-premises LAN deployments for customers with high confidentiality requirements [19]
Connectivity	On-premises customer LAN for high-confidentiality customers; separate regional or locally operated servers for some overseas deployments. Robot-side access technology is not disclosed; these are data-hosting arrangements, not access-network design.
Application scenarios	Service operations in highly private spaces such as hotel guest rooms; cross-border, multi-jurisdiction data protection requirements

Project Overview and Challenges

When commercial service robots operate in private spaces such as hotel guest rooms, guests may be concerned that navigation cameras are recording them or that data will be uploaded and misused; overseas operations must also meet the data protection requirements of different jurisdictions. In a public interview, YUNJI Technology described its approach to these issues [19].

Privacy Measures Described by the Company

According to the company, its measures operate at three levels. On the device, camera angles are designed to limit capture, cameras turn away or switch off when a guest-room door opens or in sensitive areas, and data is encrypted in transit. For the data lifecycle, de-identified environmental logs are kept for short periods and deleted periodically. For cross-border operations, some overseas markets use independent regional cloud servers; according to the company, these deployments are designed to keep relevant operational data within the local deployment environment rather than routinely transferring it back to a central overseas platform, and customers with high confidentiality requirements can run the system within their own LAN [19]. These descriptions come from the company's public disclosures. They do not constitute independent verification that any product meets the regulatory requirements of a particular jurisdiction, and the case does not assess the contribution of network performance to task outcomes.

Lessons Learned

The approach described by the company illustrates a privacy-first design sequence for connected service robots: first define what is not collected, then define how data is transmitted, stored and deleted. Physical constraints on capture, data minimisation with periodic deletion, and localised deployment for cross-border operations are practices that other deployments may consider, subject to verification against local requirements.

Category C

5.8 Case Study 8:

The MWC Shanghai Football Penalty Shootout: a Showcase of Embodied Intelligence System Capabilities in a Dynamic Setting and Its Implications for Network Requirements

Item	Details
Project name	MWC26 Shanghai Humanoid Robot Football Penalty Challenge
Organisers	Hosted by GSMA; AI 100, the Artificial Intelligence Industry Alliance (AIIA) and Xinhuanet participated in the organising committee
Connectivity	Perception, inference and motion-control loops ran on board, and remote operation was prohibited. Public event materials do not show 5G/5G-A use by competing robots or reliance on mobile networks for competitive control.
Dates	24–25 June 2026
Venue	Hall N4, Shanghai New International Expo Centre
Scale	8 participating teams; the main competition took place on 24–25 June [20][21]
Source	GSMA official announcements; Xinhua public reporting [20][21][22]

Project Overview

MWC26 Shanghai featured a Humanoid Robot Football Penalty Challenge for the first time on 24–25 June 2026, with eight Chinese embodied intelligence teams competing in autonomous shooting and goalkeeping under a World Cup-style penalty format. Robots had to observe the environment, track targets, judge positions and act autonomously, without on-site remote control or pre-set motion paths [20][21][22]. According to media reports, China Mobile's Lingxi CM-H2-A won the championship [23]. Hong Liu, Head of Technology at GSMA Greater China, likened the event to the starting point of a "Turing test" for embodied intelligence.

Observations and Lessons

GSMA positions the challenge as a system-level demonstration of how connectivity, AI, real-time decision-making and motion control work together [22]. The results mainly reflect perception, decision-making, motion control and system integration; public information does not show that the competitive loops of participating robots depended on mobile networks. For this paper, the event is best seen as a stress test of embodied systems in a dynamic physical setting, and as a signal that the mobile industry regards embodied intelligence as an emerging application area. Operators are working with industry partners to support robots, drones, connected vehicles and AI applications [24]. GSMA Director General Vivek Badrinath noted that such robots are being built not to replace humans on the pitch but to serve factories, hospitals, homes and streets, and that the convergence of connectivity, AI and physical action is opening up "the IQ Era".

Category C

5.9 Case Study 9:

2026 World Humanoid Robot Games, Competitive Capability and Connected Robot Management

Item	Details
Project name	Tennis Exhibition Match and Table Tennis Competition at the 2nd World Humanoid Robot Games (2026)
Organisers	Hosted by the Beijing Municipal People's Government, China Media Group, the World Robot Cooperation Organization and the Asia-Pacific RoboCup International Council
Connectivity	China Unicom deployed isolated robot networks at the venue: a dedicated 100 MHz 5G-A carrier at 3.3 GHz (of 300 MHz, the rest serving the public) and a physically separate Wi-Fi 7 network for the competition, with a reported robot-control latency target of 30 ms end to end (18 ms measured at the opening ceremony) [49]. A management platform handled robot identity, access authentication and status and location monitoring; competitive control loops stayed local, as cloud control was prohibited.
Dates	22–26 August 2026
Venue	National Speed Skating Oval ("Ice Ribbon"), Beijing
Scale	666 teams from 16 countries and 2,056 robots [25]
Source	Public reporting by Beijing Daily, Xinhua, CCTV.com and others

Project Overview

The 2nd World Humanoid Robot Games, held in Beijing on 22–26 August 2026, brought together 666 teams from 16 countries and 2,056 robots [25]. At the opening ceremony, a Galbot robot played an autonomous tennis rally with former world champion Zheng Jie; according to the company, the longest rally exceeded 130 shots [26]. Table tennis debuted as a formal event, the HOPE (Hitch Open Ping-Pong Embodied) AI Autonomous Decision-Making Robot Table Tennis Challenge, in which 12 teams used the AgiBot Yuanzheng A3 platform. Robots could receive data from the event's standard motion capture and refereeing systems, but teleoperation, remote control and cloud-based "remote brains" were prohibited [28].

Sources of Competitive Capability

Galbot coordinated task decisions with whole-body motion control through its AstraBrain system [26]; the Peking University and BAAI team combined spiking and fast-slow vision with rapid trajectory prediction and imitation learning [27]; and the University of Hong Kong's SMASH team relied on on-board perception alone [29]. These hard real-time loops ran on the robot or on site, and the rules excluded cloud-based control, so public information does not show that connectivity improved competitive performance (Category C).

The Role of Connectivity: Robot Management Platform

Connectivity contributed to event operations. China Unicom built a robot management platform for the event. The platform registered each robot's model, team and network address with access credentials, monitored device health in real time and retained link and location records for troubleshooting. According to the operator, it supported 2,056 robots and collected 1.56 million operational data records [30].

Lessons Learned

Real-time motion control should stay local, and connectivity should not be presented as a prerequisite for competitive performance. At scale, however, a key question is whether each robot can be identified, monitored and traced. The platform's identity registration, access authentication, status monitoring and record retention illustrate, at event scale, several elements of the lifecycle trust framework discussed in Section 6.4, and it is this management capability, rather than any network metric, that factories and campuses can draw on.

Chapter 6.

Development Path and Policy Recommendations: Building the Infrastructure for Connected Embodied Intelligence

Deployment at scale is not just a matter of procuring communication modules and connecting robots. It should start from scenarios, end-to-end task requirements and safety accountability, and establish a mechanism in which robots, networks, computing, platforms and users all take part. In his opening keynote at MWC Shanghai, John Hoffman, Executive Chairman and Director of GSMA Ltd, noted that the next phase of the mobile industry is no longer only about connecting people and devices, but about connecting "intelligence" through mobile networks, AI, open interfaces and global standards; intelligence at this scale cannot be achieved by any single country or company alone, and requires collaboration across industries, companies and borders. This chapter sets out a development path covering scenario tiering, infrastructure, interface standards, a full-lifecycle trust framework, Responsible AI, testing and validation, and commercial models. Except where published GSMA positions are cited, the content of this chapter reflects industry research findings and opinions. It does not represent a formal GSMA public policy position, nor does it constitute GSMA technical recommendations or specifications.

6.1 Define Networks by Scenario Tier, Rather Than Looking for Scenarios to Fit Network Capabilities

Scenarios should be tiered according to task risk, range of movement, data volume and degree of external dependence. Low-risk, low-interaction tasks can use ordinary Wi-Fi or best-effort public cellular connectivity. Scenarios requiring continuous mobility, high-definition video and remote takeover should be equipped with 5G/5G-A with assured quality (for example a private network, a network slice or a QoS-assured public network service) and edge nodes. High-precision industrial control should retain industrial Ethernet/TSN and local safety loops. Emergency scenarios should be equipped with multi-link and ad hoc networking. Scenario tiering helps avoid a one-size-fits-all approach of building the highest-specification network everywhere, reducing deployment costs.

For scenarios with high continuity requirements, scenario tiering should also cover the choice of connectivity assurance approach. For embodied intelligence scenarios involving movement across campuses or regions, or with high service continuity requirements, connectivity assurance mechanisms combining multiple operators, multiple access networks or multiple links can be explored according to task risk, coverage conditions and operational needs. Where supported by device and network capabilities, the system can select connectivity paths, perform failover or degrade services, taking into account network availability, coverage and signal quality, latency and packet loss, service priority and operational policy. For services with high continuity requirements, such as remote operation and backhaul of critical status, mechanisms such as multiple modules, multiple links, edge state retention and application-layer session recovery can improve service availability under fault conditions. On-board safety control and loss-of-connectivity protection should still remain autonomous and local, so that safety-critical functions do not depend on successful network switching.

6.2 Build Integrated Infrastructure for Networks, Cloud–Edge Computing and Operations Platforms

Networks for embodied intelligence may need to be assessed on more than coverage and data rates. Depending on the scenario, edge computing, model services, device management and security auditing may also need to be considered alongside network deployment. For example, campus-level platforms can provide unified access, traffic breakout, inference services, maps and task scheduling, while the cloud handles cross-campus training, knowledge bases, model management and operational analytics. Platform-based capabilities reduce the need for each robot project to build its own private network, computing and back end.

Cloud-edge computing resource pooling and coordinated scheduling for embodied intelligence may be a topic for further study, including how workloads could be placed across cloud and edge nodes according to task requirements, network conditions and data boundaries.

Depending on their capabilities, operators can extend beyond cellular connectivity into edge computing, network APIs, identity signals, security, billing and O&M services, and develop solutions together with robot companies, cloud service providers and system integrators. The specific role depends on each operator's strategy, assets and partnership model.

6.3 Advance IoT Interoperability and Device-Edge-Cloud Interface Standards

The aim of standardisation for connected embodied intelligence is not to unify the internal implementation of robots, but to define the minimum common interfaces needed for cross-brand and cross-platform collaboration. Relevant areas include device identity and capability description; semantics for maps, location, tasks, status and events; device-edge-cloud model and data interfaces; service invocation and permission management; and joint network and task testing. These interfaces would also need to extend beyond robot-to-robot collaboration to on-site facilities such as lifts, access control, sensors and conveying equipment, while remaining compatible with existing protocols and installed devices. Standards bodies and industry organisations have begun work in some of these areas; in China, for example, MIIT/TC8 and the China Communications Standards Association (CCSA) are developing related standards [1].

On the network side, standardised network APIs offer an existing route for robots and their platforms to use operator network capabilities consistently across operators and markets. Interfaces for embodied intelligence could explore alignment with GSMA Open Gateway and CAMARA [31], which may be relevant in the following areas:

Robot Requirement	Relevant CAMARA/Open Gateway API Direction	Typical Use
Connectivity quality assurance	Quality on Demand / QoS Profiles / QoS Provisioning (availability not guaranteed in all markets)	Teleoperation; upload of critical video
Location and area verification	Location Verification (verifies whether a device is within a given area)	Supporting geofence alerts and site access checks (not the sole basis for safety-critical positioning)
Device and number signals	Number Verification / SIM Swap / Device Swap (subscription or anti-fraud signals, not robot asset identity)	Supplementary signals for access risk control (not a substitute for device identity or operator authentication)

Robot Requirement	Relevant CAMARA/Open Gateway API Direction	Typical Use
Network status awareness	Connectivity Insights (whether QoS thresholds are breached); Device Reachability Status (device online status)	Dynamic offloading; degradation upon loss of connectivity
Edge discovery	Simple Edge Discovery (discovers edge cloud zones close to the device)	Nearby inference and local breakout

The API names listed reflect GSMA Open Gateway/CAMARA materials as of November 2026. API names, market availability, authorisation methods and service levels depend on official GSMA Open Gateway/CAMARA releases and local operators' commercial offerings. CAMARA maturity classifications, the release status of individual APIs and operators' commercial availability are distinct and should not be equated.

Several further CAMARA APIs at an earlier stage of maturity could also be relevant and are worth tracking as they progress, for example: Device Identifier, which returns the device model and manufacturer based on the TAC [43]; Network Slice Booking and Dedicated Networks, which reserve network resources for a given area and time window, such as an event or a temporary operation [44] [45]; Optimal Edge Discovery, which identifies the most suitable edge cloud zone for a device and application [48]; and Traffic Influence, which routes device traffic to the optimal edge application instance [46]. Robotics companies and operators can contribute use cases to these work items so that robot requirements are reflected early.

Global standards and multilateral mechanisms are essential for scaling. International mechanisms such as spectrum harmonisation, 3GPP standards, the ITU and the WRC form the foundation for the cross-border development of 5G-A, 6G and AI. Connected embodied intelligence involves multiple standards systems. 3GPP mainly defines technical specifications for cellular network architecture, radio access, core networks, QoS and mobility; the ITU is responsible for the IMT vision, overall requirements and international coordination related to spectrum; robotics and industrial organisations are responsible for functional safety, control, data models and industry interfaces; and GSMA focuses on aggregating operator requirements and advancing cross-network and cross-operator implementation specifications, interoperability, certification, network APIs and commercialisation at scale. In this paper, the "GSMA perspective" mainly refers to mobile industry requirements, interoperability frameworks, network capability exposure, security and trust, and commercial scale, and does not replace 3GPP or robotics standards organisations in developing underlying technical standards.

6.4 Build a Full-Lifecycle Trust Framework

Connectivity transforms robots from relatively closed standalone devices into intelligent nodes continuously connected to networks, computing, models, platforms and business systems. In this process, security risks expand from conventional device security to full-lifecycle risks covering device identity, communication links, the software supply chain, model operation, data processing, remote operation and device decommissioning. The security framework for embodied intelligence should therefore not focus only on network access and transmission protection, but should span the full device lifecycle, from manufacturing, onboarding, operation, upgrade, maintenance and transfer through to decommissioning, forming a closed-loop trust framework covering identity, boot integrity, connectivity, software, models, operations, data and decommissioning.

Establish a Device Root of Trust and Trusted Identity Framework

Robots should support a verifiable device identity anchored, where appropriate to the risk level and device architecture, in hardware-backed security capabilities such as a secure element, hardware security module or other suitably assured root-of-trust mechanism. Trusted execution environments may complement this foundation by protecting sensitive runtime processing and supporting attestation. The device identity

should be bound to the robot's model, serial number, hardware and software versions, owning entity and authorisation status. Communication identities such as SIM, eSIM and iSIM mainly address device access to mobile networks and should not in themselves be equated with the robot's complete identity. In practice, mapping and binding mechanisms should be established between mobile network identity, device identity, device certificates and platform accounts, so that the network, platform and business sides can jointly confirm which robot is accessing the system, with which identity and in which scenario. When a device is transferred, repaired, has its communication module replaced or changes its operating entity, the identity binding should be reconfirmed, to avoid situations in which the network identity remains valid after the device's owner has changed. Specifically, mobile network subscription identity, robot device identity, robot business/asset identity, operator identity and platform service identity should be managed separately and coordinated through audited mappings and authorisation relationships; no single identity authentication automatically grants permission for high-risk actions. Solutions such as GSMA IoT SAFE can use the SIM as a hardware root of trust for secure device-to-cloud communication, but this likewise does not equate to complete business identity or action authorisation [32].

Device-model visibility for operators can also be improved. Robot makers that integrate cellular connectivity can register as manufacturers with the GSMA and obtain a Type Allocation Code (TAC) for each robot model, rather than relying only on the TAC of the embedded communication module [41]. The TAC forms the first eight digits of the IMEI and, through the GSMA Device Database, gives operators visibility of the make, model and capabilities of devices on their networks [42]; the CAMARA Device Identifier API can expose this information to authorised applications [43]. This would allow operators to recognise robots as a distinct device category for network planning, policy and security, similar to work under way for connected vehicles. As with SIM-based identity, the TAC identifies the device model, not the individual robot's business identity or its authorisation to act.

For robots using eUICC/eSIM, remote provisioning and changes of mobile network subscription profiles are also part of lifecycle management. The GSMA SGP.31/SGP.32 IoT eSIM architecture and technical specifications [34][35] can be used to explore remote provisioning, status management and full-lifecycle management of subscription profiles, supporting connectivity management for robots in different deployment regions and operating environments. Remote profile provisioning, network selection and service continuity should be distinguished: remote eSIM provisioning supports lifecycle management of subscription profiles, but network selection, switching policy and service continuity still depend on device and module capabilities, available networks, operator policy, roaming or commercial arrangements, and application-layer fault tolerance. A profile change alters the mobile network subscription identity, so the binding between subscription identity, device identity and platform accounts should be reconfirmed as described above. Cross-border deployments should also comply with applicable telecommunications, data protection and other regulatory requirements.

Establish Secure Boot and Firmware Integrity Mechanisms

During start-up, robots should verify the integrity of the bootloader, operating system, drivers, control software, middleware and key model components, to prevent unauthorised software or firmware from entering the runtime environment. For on-board controllers, edge servers and critical on-site nodes, mechanisms such as secure boot, measured boot with remote attestation, and code-signing verification can be applied according to risk level. If firmware, drivers or key components are found to have been tampered with, the robot should be prevented from entering normal task mode or should automatically switch to a restricted, safe mode, with the transition itself designed so that it does not compromise the safety of people, equipment or ongoing operations.

Establish Full-Lifecycle Management of Credentials and Keys

Authentication among robots, operators, platforms, edge nodes and cloud services should not rely on fixed passwords or static keys over the long term. Mechanisms should be established for credential and key enrolment, issuance, distribution, rotation, renewal, revocation and expiry. For long-running devices, critical keys should be rotated periodically according to risk level. When devices are lost, attacked, transferred

or decommissioned, the relevant certificates, tokens and network access permissions should be revoked promptly. At decommissioning, network identity deregistration, platform account removal, key destruction, API permission revocation and sensitive data clean-up should be completed together, to avoid the security risk of a digital identity remaining valid after the device has been taken out of service.

Strengthen Software Bill of Materials and Supply Chain Security Management

Embodied intelligence robots often integrate operating systems, ROS middleware, communication protocol stacks, AI inference frameworks, drivers, third-party libraries, edge software and cloud services, resulting in complex software dependencies. A software bill of materials (SBOM) should be established to record key software components, versions, sources and dependencies on an ongoing basis, with continuous vulnerability monitoring of core open-source components and third-party software. Robot vendors, platform providers and system integrators should establish vulnerability disclosure and response mechanisms, and define patch service level agreements (SLAs) for vulnerabilities of different severity, covering remediation timeframes, interim mitigations, rollback plans and the scope of affected devices.

Establish Cloud-Edge-Device Model Signing and Version Traceability

Cloud, edge and on-board models should each have a unique version number, digital signature, provenance record and release record. Before going live, models should undergo testing, approval and version registration, and deployment should support phased rollout, batch activation and rapid rollback. For critical production systems, it should be possible to trace the model version actually used by a robot at any given time, together with its source, release time, deployment targets and configuration parameters. Updates to models, skill packages, control policies and key parameters should also be brought under unified version management, so that unvalidated models or policies do not directly overwrite production devices.

Establish Clear Authorization Boundaries Across Human Operators, Platforms and Robots

Control relationships in embodied intelligence systems are no longer limited to a single operator-robot relationship, but also involve automatic platform scheduling, autonomous AI model decisions and human takeover by remote operators. Permission boundaries among the three parties should be clearly defined: what operators may do, what tasks the platform may dispatch automatically, which decisions robots may make autonomously, which operations require human confirmation, and which actions may under no circumstances be used remotely to override on-board safety mechanisms. The principle of least privilege should be applied according to task risk level. For high-risk tasks such as high-voltage electrical operations, hazardous chemical handling, medical assistance and public safety, dual approval, secondary confirmation or multi-factor authentication can be used.

Define Human Takeover Priority and Permission Conflict Handling

Once embodied intelligence enters autonomous operation, on-board autonomous decisions, platform-scheduled tasks and human remote commands may occur at the same time. Permission priority should be defined in advance: emergency stop and on-board safety protection have the highest priority; authorised human takeover takes precedence over routine automatic platform tasks; platform scheduling should not override on-board safety logic; and routine autonomous tasks must not bypass the safety controller. For critical actions, a closed-loop mechanism of human takeover, secondary confirmation, operation logging and automatic release on timeout can be applied, to prevent misoperation and prolonged occupation of control.

Strengthen Data Minimization, Purpose Limitation, and Cross-Border Governance

Embodied intelligence robots continuously collect data such as video, voice, maps, location, environmental information, human behaviour, device status and task logs, some of which may involve personal privacy, trade secrets or important business information. The principle of data minimisation should be followed, collecting only the data necessary to complete the task. The purpose and boundaries of data use should be clearly defined, so that data collected for one task is not used for other purposes without authorisation. Data that can be processed on the robot body should preferably be processed locally; data that can be analysed at the

edge should not be uploaded to the cloud by default; and, where business needs allow, features, event results or key segments should be transmitted in preference to complete raw data. For cross-regional, cross-entity or cross-border data processing, data classification, access permissions, retention periods, processing purposes and responsible parties should be defined, with assessment and authorisation carried out in accordance with applicable rules.

In addition, before deployment, the roles and responsibilities of the personal information handler (or controller), entrusted processor, data provider or other relevant parties should be defined in accordance with applicable law, together with the processing purpose and the applicable rules or lawful basis. Transparent notice should be provided to affected persons such as family members, employees, patients and visitors. It should be made clear whether training, evaluation and O&M data may be reused for other purposes, and mechanisms for deletion, anonymisation and responding to individuals' rights should be in place. Functions such as cameras, voice and mapping should preferably be designed for minimal collection by default. These requirements can draw on the GSMA Mobile Privacy Principles [33].

Establish Threat Models for Connected Robots

Embodied intelligence systems should design security policies in advance for typical anomalies and attack scenarios, including degraded network quality or communication outages, GNSS spoofing and positioning interference, compromised edge nodes, robot identity spoofing, leaked communication credentials, unavailable model services, tampered models or control policies, falsified location and environmental information, anomalies in remote takeover links, and malicious devices joining multi-robot systems. Detection, isolation, degradation and recovery mechanisms should be defined for each threat. For example, upon loss of connectivity, the robot should automatically enter local autonomy or a safe state; positioning anomalies should be cross-checked against multiple sources such as vision and inertial navigation; and when an edge node behaves abnormally, its high-risk control permissions should be revoked promptly and critical tasks switched to trusted nodes.

Section Takeaway

The goal of a full-lifecycle trust framework is not to guarantee that the system will never experience faults or attacks, but to ensure that at every stage the system can identify entities, control permissions, detect anomalies, contain impact, recover quickly and trace accountability. For embodied intelligence, security capabilities are more likely to support deployment at scale when they are designed together with the device lifecycle, network connectivity, model operation and real-world business.

6.5 Integrate Responsible AI into Governance of Embodied Intelligence Systems

The risks of embodied intelligence arise not only from network outages, privilege abuse, device attacks and data breaches, but also from model misjudgement, distribution drift, data bias, incorrect generalisation, unexplainable decisions and unexpected actions in unseen scenarios. Compared with conventional generative AI, the outputs of embodied intelligence models may translate directly into mechanical motion, with physical effects on people, equipment and the environment. Responsible AI therefore needs to go beyond statements of principle and be embedded throughout model development, validation, deployment, operation and incident

investigation.

This section focuses on AI risks specific to connected embodied intelligence, including high-risk action validation, human escalation, model version control, continuous monitoring and joint incident investigation across network, model and robot body. It does not attempt to replace general AI governance frameworks or functional safety standards.

High-Risk Actions Must Not Be Executed Directly by Unvalidated Generative Models

For actions that may have a significant impact on people, equipment or the environment (such as those involving personal safety, equipment start/stop, high-voltage electrical operations, handling of hazardous materials, medical assistance or access-control release), the outputs of generative models that have not been validated for the scenario should not drive actuators directly, but should pass through validated rules, safety controllers, action constraints or human confirmation. Models can be responsible for understanding tasks, high-level planning and generating candidate strategies, but final actions should be checked by rules, safety controllers or action-feasibility validation.

Establish Model Output Validation and Safety Constraint Mechanisms

When large models or VLA models handle high-level semantic understanding and task planning, the on-board controller should retain an independent safety loop. Models can propose what to do, but should not directly determine every aspect of how to do it. Before execution, specific actions should be checked for collision risk, joint limits, workspace, tool status and the position of people, so that errors at the cognitive layer do not translate directly into dangerous actions.

Establish Confidence Thresholds and Human Escalation Mechanisms

When model confidence falls, perception information conflicts, a task falls outside the training distribution or execution fails repeatedly, the robot should not continue to execute on a best-guess basis. Mechanisms such as pausing, re-perceiving, switching models, reducing speed, requesting remote confirmation or human takeover should be configured according to task risk level. For high-risk tasks, clear human escalation thresholds should be defined in advance, with priority given to the safety principle of stopping when uncertain.

Document the Source, Licensing, Quality and Representativeness of Training Data

Embodied intelligence models depend heavily on real-world, simulated and synthetic data, and their performance is directly affected by data quality, scenario coverage and representativeness. The source, collection method, licence scope, data version, quality control method and applicable scenarios of training data should be recorded, and data bias across different populations, environments, devices and task types should be assessed. The effectiveness of synthetic and simulated data should be validated through testing on physical robots, rather than judging model safety in real production environments on offline metrics alone.

Establish End-to-End Model Auditability

Embodied intelligence systems should record model versions, key prompts or task instructions, tool calls, task inputs, key intermediate states, output actions and final task results. Where models call external tools, databases or industry systems, the call target, returned results and permission status should also be recorded. After an incident, it should be possible to reconstruct the complete chain of device state, network state, model input, model decision, platform command, human operation and final action.

Conduct Independent Scenario-Specific Evaluation

Recognition rates, grasping success rates or model benchmark results in the laboratory should not be equated directly with safety and reliability in real production environments. Each application scenario should be evaluated independently based on its environment, people density, task complexity and risk level. For example, even when hotel delivery, hospital delivery, industrial assembly and firefighting and rescue use the same robot and model, their acceptable error rates, human takeover conditions and safety boundaries should differ. After passing general testing, models should also undergo independent validation for the specific application scenario.

Establish Model Drift Detection and Continuous Monitoring

As robots operate over the long term, scenarios, equipment, people and task distributions change, and models may gradually drift from their original training distribution. Systems should continuously monitor task success rates, abnormal actions, human takeover rates, confidence changes and failure types, and trigger revalidation, model updates or version rollback when significant drift is detected.

Strengthen Data Governance and Purpose Limitation

Responsible AI and data governance should form a single closed loop. In sensitive scenarios such as homes, healthcare and public services, data minimisation, purpose limitation and tiered authorisation should be upheld, with clearly defined data retention periods, access permissions and cross-border processing boundaries. Training, evaluation and operational data should remain traceable in origin, explainable in use and auditable in access, to prevent unauthorised secondary use.

Define Accountable Parties and Incident Investigation Mechanisms

Embodied intelligence systems typically involve robot vendors, model providers, operators, platform providers, system integrators and end users. The responsibility boundaries of each party for devices, networks, models, data and operations should be defined before deployment. After an incident, investigation should be based on logs, model versions, network status and permission records, to avoid ambiguous accountability in which model problems are attributed to the device, device problems to the network and network problems to the platform.

Section Takeaway

Responsible AI is not a supplementary clause to the network security framework, but a distinct capability that embodied intelligence needs as it enters the real world. Trusted connectivity helps establish who can connect and whether data has been tampered with in transit, although it cannot vouch for the accuracy of the data at the source; Responsible AI provides governance and assurance mechanisms for how models are developed, validated, deployed and monitored, including when automated decision-making should be constrained or escalated; and functional safety is intended to keep the robot in a safe state even if the network or models fail. The three are complementary, cannot substitute for one another, and together form the foundation of trust for deploying embodied intelligence at scale.

6.6 Establish Joint Testing, Validation, and Third-Party Evaluation Mechanisms

Connected embodied intelligence can be validated under conditions close to real deployment, for example in shared test beds, industry test sites or on-site pilots. Test conditions could include typical challenges such as metal-rich workshops, dense shelving, outdoor mobility, weak coverage and high concurrency, and could cover single-robot to multi-robot, static to mobile, and normal to fault conditions, with network, system and business metrics recorded together. Where appropriate, independent third-party testing of key metrics reported in public case studies could improve comparability and credibility.

Test areas could include, for example: interoperability testing of cross-vendor device access, consistency of status and event semantics, service invocation and permission checks; task completion latency and fault recovery under network fluctuation and node failure; the success rate of coordination between robots and on-site equipment; and whether the robot degrades safely when connectivity is lost. Test methods and results should be comparable and reproducible wherever possible, so that different deployments can learn from one another.

6.7 Close the Commercial Loops Through Real-World Scenarios

In high-value scenarios such as manufacturing, logistics, energy, emergency response and commercial services, collaboration among multiple parties can help move connected embodied intelligence towards real deployment. For example, user organisations could define quantifiable task objectives, robot companies provide complete robots and models, operators provide network and edge capabilities, and platform companies handle system integration and operations; the exact division of roles will vary by project. On business models, individual companies may explore different approaches according to their own circumstances, for example combining equipment leasing with network services and model subscriptions, billing by effective working hours or task volume, or sharing edge computing resources. Within a given scenario, cost per task and payback period can serve as useful indicators. However, tasks vary widely in complexity and value and are not directly comparable across scenarios, so a more generic economic metric for connected embodied intelligence still needs to be developed.

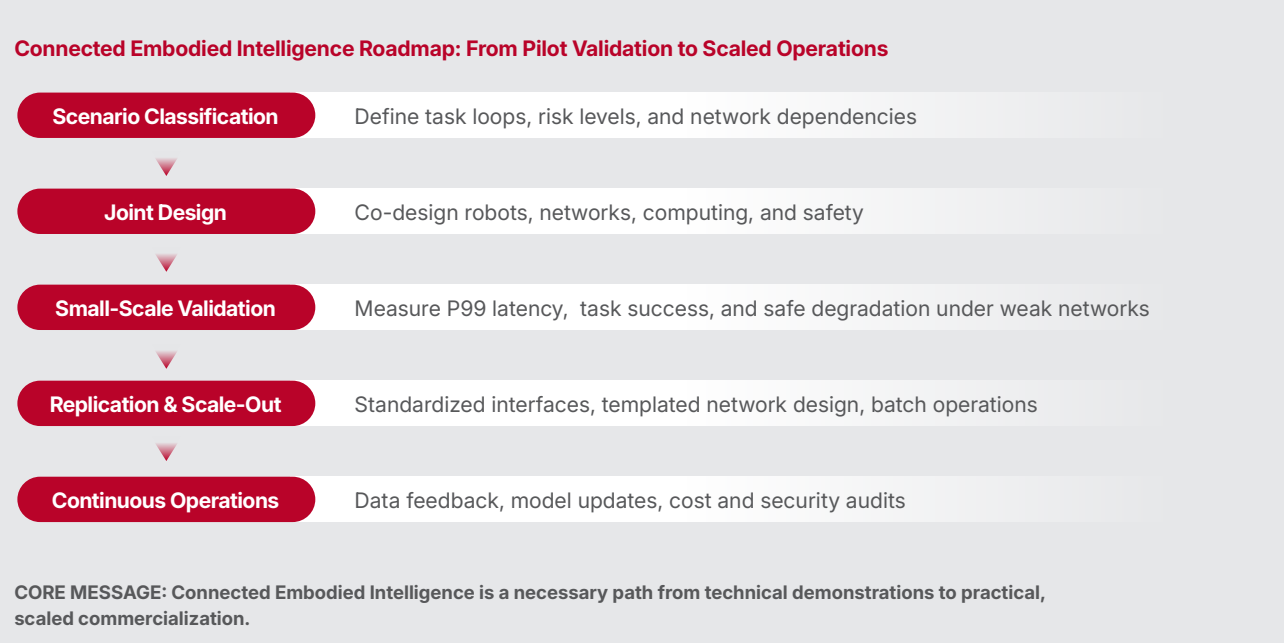

Figure 4. Roadmap for Building Connected Embodied Intelligence

Source: Prepared by the research team

6.8 Create an Enabling Policy Environment for Connected Embodied Intelligence

Connected embodied intelligence depends on sustained investment in mobile networks, edge computing and network capabilities that robots can use at scale. Operators, however, face rising costs and greater capital intensity due to shorter technology cycles, network densification and growing data demand [47]. In line with the GSMA's published policy recommendations on AI readiness [47], policymakers and regulators can consider the following measures as they apply to connected embodied intelligence.

Support sustainable network investment

Create an enabling economic environment for operators to invest, for example by rationalising sector-specific taxation, extending licence periods, enabling market-driven regulation, and prioritising efficient network deployment rules and spectrum management [47]. This helps 5G/5G-A and edge computing reach the factories, campuses, logistics sites and public spaces where robots operate.

Partner with industry to test and innovate

Collaborative governance mechanisms, such as time-limited regulatory sandboxes, allow new ideas and emerging technologies to be tested [47]. For connected robots, they can support real-world trials before wider rollout, together with R&D and ecosystem partnerships across operators, robotics companies and research institutions.

Keep the policy environment clear, consistent and harmonised

Governance frameworks based on internationally agreed principles, such as those developed by the OECD or UNESCO, and consistent terminology help solutions benefit from economies of scale across markets. Data privacy frameworks should be risk-based, horizontal and technology-neutral, and AI policies should be designed in conjunction with them [47].

Build skills and institutional capacity

Expand digital skills programmes for the workforce that will deploy, operate and maintain connected robots, and invest in capacity building so that policymakers and regulators have up-to-date knowledge of fast-moving technologies and global best practices [47].

Bringing operators and other industry participants into the rules-development process at an early stage can help ensure that governance remains effective and keeps pace with deployment [47].

Conclusion

As embodied intelligence moves from demonstrations into real-world operation, the challenge is no longer only to improve individual robot capabilities. Deployment at scale also requires robots, computing resources, communications networks, operational platforms and human operators to work together under clearly defined safety, security and governance boundaries. Connectivity can play an important role in this transition by supporting access to external computing and knowledge, multi-robot coordination, remote supervision, lifecycle management and continuous service.

Connected embodied intelligence should not be understood as moving all intelligence or control into the network or cloud. Hard real-time control and safety functions should remain local where required, while edge, network and cloud capabilities can complement on-device intelligence according to task latency, risk, data sensitivity and operational requirements. The appropriate architecture will therefore vary by scenario and should be assessed against end-to-end task outcomes rather than network performance alone.

This paper proposes Connected Embodied Intelligence as a research framework rather than a normative architecture or industry specification. Further work is needed on interoperable interfaces, lifecycle security and identity, Responsible AI, privacy and data governance, cross-vendor testing, network capability exposure and commercially sustainable deployment models. Collaboration among mobile operators, robotics companies, technology providers, industry users and standards organisations can help determine where connected capabilities provide measurable value and how they can be introduced safely and at scale.

Appendix: Glossary

Term	Description
Embodied Intelligence	An intelligent system with a physical embodiment that can perceive its environment, understand tasks, and affect the physical world through actions.
Connectivity (Connected Embodied Intelligence)	Connecting robot bodies, edge and cloud resources, other agents, people, and business systems through multiple communications technologies to form a collaborative system.
Brain-Cerebellum	The brain refers to complex cognition, planning, and knowledge capabilities; the cerebellum refers to onboard motion control, real-time execution, and safety loops.
Edge Computing	Computing resources deployed near an industrial park, base station, or worksite for low-latency inference, data processing, and task scheduling.
5G-A	5G-Advanced, an enhanced evolution of 5G based on 3GPP Release 18 and subsequent releases.
Task-Level KPI/SLO	Network, computing, control, and business metrics (KPIs) and target values (SLOs) defined around task success; they are called SLAs only when included in a contract.
Tail Latency	High percentiles of a latency distribution, such as P99/P99.9, used to capture occasional stalls and extreme delays.
Safe Degradation During Connectivity Loss	When the network is interrupted or degraded, the robot enters a predefined state such as slowing down, pausing, returning, or adopting a safe posture.

Terminology note: This white paper consistently uses “Connected Embodied Intelligence” as its English rendering of the concept of embodied intelligence connected through networks. This is a research term adopted in this paper and is not an established official GSMA term.

References

1. Ministry of Industry and Information Technology of China. Announcement of the Ministry of Industry and Information Technology (2025 No. 44) [EB/OL]. 2025-12-31. https://www.miit.gov.cn/jgsj/kjs/wjfb/art/2025/art_91588a03c1694803b04f6e7674ac973a.html
2. National Technical Committee for Robot Standardization. Research Report on Embodied-Intelligence Robots and Mobile Communications Technology (2025 Edition) [R]. 2025-12 (released publicly on 2026-05-06). https://mp.weixin.qq.com/s?__biz=MzkzMjMxMzg5NA==&mid=2247486341&idx=1&sn=e1f9d1b926b343d11e89557192763768
3. Ministry of Industry and Information Technology of China. Economic Performance of the Communications Industry in the First Four Months of 2026 [EB/OL]. 2026-05-25. https://www.miit.gov.cn/jgsj/yxj/xxfb/art/2026/art_a70719667cfe461fbd88a5f516d22706.html
4. China Academy of Information and Communications Technology, republished by Sina. Five Charts Illustrating Seven Extraordinary Years of 5G in China [EB/OL]. 2026-06. https://finance.sina.com.cn/wm/2026-06-06/doc-iniankfk1829355.shtml
5. Ministry of Industry and Information Technology of China. Interpretation of the 2025 Telecommunications Industry Statistical Bulletin: Stable Industry Performance and Accelerating Development of New Drivers [EB/OL]. 2026-01-28. https://www.miit.gov.cn/gxsj/tjfx/txy/art/2026/art_da754fe24a9347dc89bef9bf9c28528e.html
6. ITU-R. Report M.2410-0: Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s) [R]. 2017. https://www.itu.int/pub/R-REP-M.2410-2017
7. ITU-R. Recommendation M.2160-0: Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond [R]. 2023. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf
8. ITU-R Working Party 5D. IMT Towards 2030 and Beyond: Progress on Technical Performance Requirements and Evaluation [EB/OL]. 2026. Draft technical requirements from February 2026 and draft evaluation guidelines from June 2026 were proposed for consideration by Study Group 5 in December 2026. https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/IMT-2030/Pages/default.aspx
9. China Mobile, republished by C114. At the National Games Torch Relay, a 5G-A Robot Independently Runs the First Leg Worldwide [EB/OL]. 2025-11-04. https://www.c114.com.cn/news/118/a1299853.html
10. China Mobile Research Institute. China Mobile's 5G-A Innovations Support the National Games and Establish a New Model for Network Assurance [EB/OL]. 2025-11-17. https://mp.weixin.qq.com/s/ubA9j2sLjo0k-iTtRardjA
11. GSMA Foundry. 5G-Advanced Facilitates Multi-Robot Collaboration—ZTE and China Telecom [R]. Report dated November 2025; published online in December 2025. https://www.gsma.com/get-involved/gsma-foundry/wp-content/uploads/2025/12/5G-Advanced-Facilitates-Multi-Robot-Collaboration_Nov_25.pdf
12. ZTE. ZTE 5G-A EasyOn·Robot Private Network Facilitates Multi-Robot Collaboration at WAIC 2025 [EB/OL]. 2025-08-07. The latency cited is air-interface latency; 99.99% refers to network availability. https://www.zte.com.cn/global/solutions_latest/5g-advanced/solution-news/zte-5g-a-easyon-robot-private-network-facilitates-multi-robot-co.html
13. China Telecom Tianyi IoT. "Lingsi Brain" Empowers Robots to Move Toward Collective Intelligence [EB/OL]. 2024-12-17. https://www.chinatelecom.com.cn/ct/news/rgzn/154072.html
14. Xinhua Finance. Results Released for a 5G-A Embodied-Intelligence Robot Power-Grid Inspection Demonstration [EB/OL]. 2025-11-02. Efficiency improvement was disclosed by the project team; independent measurement of the network's contribution was not published. https://m.cnfin.com/hg-lb/zixun/20251102/4327817_1.html
15. China Mobile Research Institute, republished by Sina. China Mobile and Industry Partners Build What They Describe as the First 5G-A Embodied-Intelligence Humanoid-Robot Training Ground and Firefighting/Rescue Demonstration [EB/OL]. 2026-07-02. https://finance.sina.com.cn/wm/2026-07-02/doc-inifmmmu2670899.shtml
16. Suzhou Daily. Rescue Robots "Understand" Fire Scenes as 5G-A Embodied-Intelligence Humanoid-Robot Training Ground Opens [EB/OL]. 2026-06-26. https://news.2500sz.com/doc/2026/06/26/1216625.shtml
17. Haidian News. Humanoid Robots Take Up Parcel-Sorting Jobs [EB/OL]. 2026-05-18. Feeding efficiency was disclosed in an interview with the company. https://hdb.bjhdnet.cn/hdb/content/202605/18/c62088.html
18. Xinhua News Agency. China's Vibrant Economy in Focus: Leaving the Laboratory, How Do Robots "Go to Work"? [EB/OL]. 2026-06-12. https://www.news.cn/tech/20260612/128fdccbf5144235846fbfd1075e31a4/c.html
19. Xinhua News Agency, republished by Yunji Technology. Xinhua Interview with Yunji Technology CEO Li Quanyin: Connecting the Digital and Physical Worlds [EB/OL]. 2026-04-27. https://mp.weixin.qq.com/s/M6EU4pg0C03lLvgSOQuvBw
20. GSMA. Humanoid Robot Football Penalties Challenge [EB/OL]. Official MWC26 Shanghai event overview. https://www.mwcshanghai.com/exhibition/humanoid-robot-football-penalty-challenge
21. Xinhua News Agency. The "World Cup" of Humanoid Robots

at a Technology Showcase [EB/OL]. 2026-06-25. https://www.xinhuanet.com/20260625/109b3d2280ff470eaa23e0eab6d6d3f9/c.html

22. GSMA. GSMA Announces Humanoid Robot Football Penalties Challenge, Set to Debut at MWC26 Shanghai [EB/OL]. 2026-04-10. https://www.mwcshanghai.com/articles/humanoid-robot-football-penalties-challenge
23. PConline. China Mobile's Lingxi Humanoid Robot Wins the MWC26 Shanghai Robot Penalty-Shot Competition [EB/OL]. 2026-06-26. Technical and award information is based on China Mobile's public statements. https://news.pconline.com.cn/2177/21777637.html
24. GSMA. GSMA MWC26 Shanghai Opens Doors as AI, Robotics, and Drones Lead Packed Agenda [EB/OL]. 2026-06-24. https://www.mwcshanghai.com/articles/opens-doors-ai-robotics-drones-lead-packed-agenda
25. Beijing Daily. The Second World Humanoid Robot Games Open in Beijing, with 666 Teams from 16 Countries and 2,056 Robots Competing [EB/OL]. 2026-08-23. https://www.beijing.gov.cn/ywdt/gzdt/202608/t20260823_4833187.html
26. Xinhua Finance. Robots at Work, Industry Accelerates: Observations on Galbot's Scaled Deployment of Embodied Intelligence [EB/OL]. 2026-09-16. The longest rally of more than 130 shots was disclosed by the company. https://www.cnfin.com/cmjj-lb/detail/20260916/4470662_1.html
27. Peking University. Peking University's Table-Tennis Robot Wins the Championship! [EB/OL]. 2026-08-28. https://mp.weixin.qq.com/s/RT_Rovg9BwsaliK6aKAeYw
28. CCTV.com. HOPE AI Autonomous Table-Tennis Competition at the Second World Humanoid Robot Games Concludes; Joint Peking University–BAAI Team Wins Championship [EB/OL]. 2026-08-28. https://www.cctv.com/2026/08/28/ARTIGbZj5n4k3gXNeJq1QXNg260828.shtml
29. The University of Hong Kong. HKU SMASH Team Wins Silver at World Humanoid Robot Games with World-First Autonomous Humanoid Table Tennis System [EB/OL]. 2026-09-01. https://lead.hku.hk/en/article/2026/09/hku-smash-team-wins-silver-at-world-humanoid-robot-games-with-world-first-autonomous-humanoid-table-tennis-system/
30. Xinhua Net. Connecting Intelligence and a New Computing Ecosystem: China Unicom at the 2026 China International Fair for Trade in Services [EB/OL]. 2026-09-10. https://www.xinhuanet.com/info/20260910/055612f38adc445eb0761fb08b6d5eb2/c.html
31. GSMA. GSMA Open Gateway API Descriptions [EB/OL]. https://www.gsma.com/solutions-and-impact/gsma-open-gateway/gsma-open-gateway-api-descriptions/
32. GSMA. IoT SAFE (IoT SIM Applet For Secure End-to-End Communication) [EB/OL]. https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/IoT-SAFE/
33. GSMA. Mobile Privacy Principles [R/OL]. The principles were first published in January 2011; the resource page is dated 2016-02-05. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/gsma_resources/mobile-privacy-principles/
34. GSMA, SGP.31 eSIM IoT Architecture and Requirements, Version 1.3, May 2026.
35. GSMA, SGP.32 eSIM IoT Technical Specification, Version 1.3, May 2026.
36. 3GPP. TS 22.104: Service Requirements for Cyber-Physical Control Applications in Vertical Domains; Stage 1 (Release 19) [S]. https://www.3gpp.org/DynaReport/22104.htm
37. 3GPP. TS 22.261: Service Requirements for the 5G System; Stage 1 (Release 18) [S]. Clauses 6.9, 6.31, 6.42 and 7.4 cover relay UEs, disaster roaming, mobile base station relays and satellite access; Table 7.11-1 gives KPIs for remote-control robots. https://www.3gpp.org/DynaReport/22261.htm
38. 5G-ACIA. Architecture and Technology for Machine Vision in Industrial Applications with 5G [R]. 2025-03. https://5g-acia.org/whitepapers/architecture-and-technology-for-machine-vision-in-industrial-applications-with-5g/
39. 5G-ACIA. Industrial 5G Edge Computing: Use Cases, Architecture and Deployment [R]. 2023-02. https://5g-acia.org/whitepapers/industrial-5g-edge-computing-use-cases-architecture-and-deployment/
40. 5G-ACIA. A 5G Traffic Model for Industrial Use Cases [R]. 2019-11. https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_5G_A_Traffic_Model_for_Industrial_Use_Cases_22.10.19.pdf
41. GSMA. TAC Allocation [EB/OL]. https://www.gsma.com/services/device/tac-allocation
42. GSMA. Device Attribute Data: GSMA Device Database and GSMA Device Map [EB/OL]. https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-attribute
43. CAMARA Project. Device Identifier API [EB/OL]. https://camaraproject.org/device-identifier
44. CAMARA Project. Network Slice Booking API [EB/OL]. https://camaraproject.org/network-slice-booking/
45. CAMARA Project. Dedicated Networks API [EB/OL]. https://camaraproject.org/dedicated-networks/
46. CAMARA Project. Traffic Influence API repository [EB/OL]. https://github.com/camaraproject/TrafficInfluence
47. GSMA. Telco for AI: Policy Recommendations for AI Readiness [R]. March 2026. https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/gsma_resources/telco-for-ai-policy-recommendations-for-ai-readiness/
48. CAMARA Project. Optimal Edge Discovery API [EB/OL]. https://camaraproject.org/optimal-edge-discovery/
49. C114. From Supporting the 2026 World Humanoid Robot Games to Empowering Industry: How China Unicom Became the Operator That "Best Understands Embodied Intelligence" [EB/OL]. 2026-08-27. https://m.c114.com.cn/w119-1316470.html

Acknowledgements

This white paper was jointly initiated, organized, written, and published by GSMA and AI100.

The following organisations participated in the research, drafting, and review of this white paper. We sincerely thank them for their contributions:

Artificial Intelligence Research Institute, China Academy of Information and Communications Technology | China Mobile | China Unicom | China Telecom | Huawei | Robotera | Galbot | GigaAi | SpacemiT | Yunji Technology | Jiyuan Zhihang



GSMA
1 Angel Lane
London
EC4R 3AB
United Kingdom

Tel: +44(0)20 7356 0600
Fax: +44(0)20 7356 0601