IOT ANALYTICS

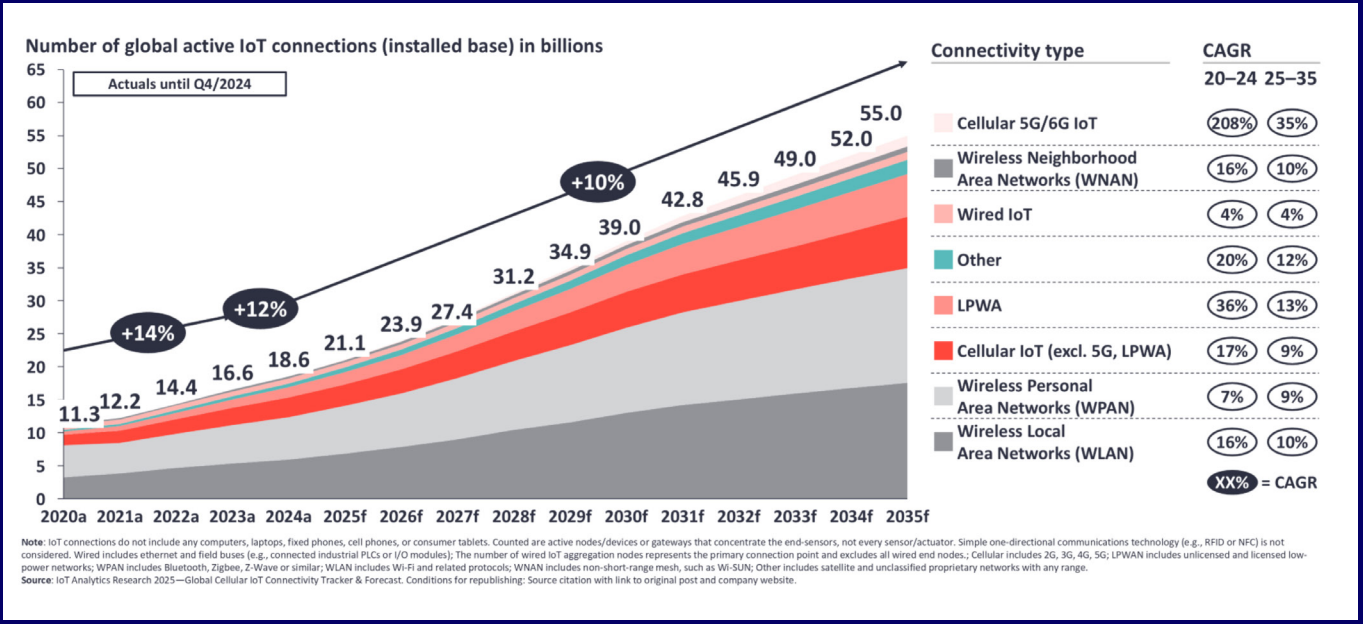
Giesecke+Devrient

Navigate connectivity barriers with eSIM, RSP, and SGP.32 to scale cellular IoT securely

Executive Summary

Cellular IoT adoption is accelerating, but scaling globally has long been hindered by roaming limits, fragmented provisioning, and security concerns. These challenges are now being addressed through eSIM, iSIM, and Remote SIM Provisioning (RSP), enabling secure, flexible, and automated connectivity across borders. The new GSMA SGP.32, for which Giesecke+Devrient (G+D) received the first GSMA eSIM Compliance and eUICC Security Assurance certifications in April 2025, and In-Factory Profile Provisioning (IFPP) standards make large-scale deployments practical, simplifying activation, reducing SKU complexity, and ensuring devices connect reliably from day one. With centralized orchestration platforms, device makers can manage profiles, automate switching, and maintain continuous service worldwide. As a result, connectivity in industries like transport and logistics is becoming simpler, more scalable, and more resilient, marking a decisive shift from connectivity challenges to connectivity readiness.

Figure 1: Global IoT market forecast (in billions of connected IoT devices)
Source: IoT Analytics



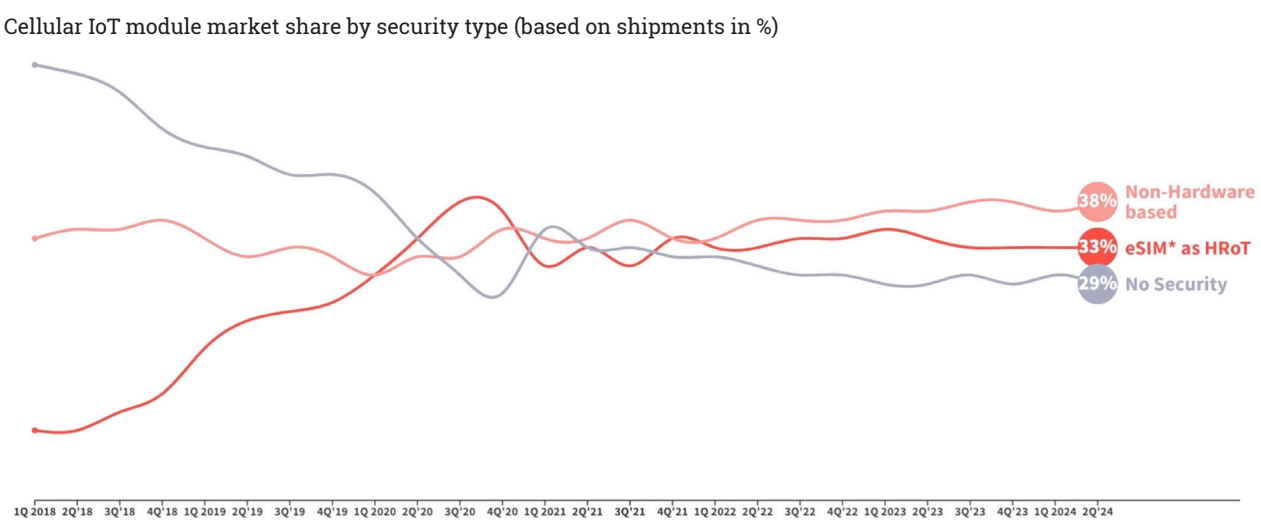
1. Accelerated growth of cellular IoT presents challenges for device makers

Connected IoT devices projected to reach 40 billion. According to IoT Analytics, there were 18.6 billion connected IoT devices worldwide by the end of 2024, a 12% increase from 2023. The total number of connected IoT devices is forecast to grow at 14% CAGR, reaching 39 billion by 2030.

Global cellular IoT connections are set to more than double. Global cellular IoT connections accounted for 22% of these overall IoT connections, reaching 4.1 billion by the end of 2024. Cellular IoT connections are projected to grow at a 14% CAGR, reaching 9.1 billion by 2030, aided by ongoing deployments of LTE Cat 1 bis, LPWA, and 5G technologies. As cellular IoT is ideal for mobility and long-range coverage applications, the transportation, supply chain, and logistics industries led adoption in 2024, collectively accounting for 35% of global cellular IoT connections.

Cellular IoT faces scaling, security, and interoperability challenges as adoption accelerates. As discussed in the next section, device makers face several persistent challenges in not only scalability but also security, lifecycle management, global interoperability, regulatory compliance, and connectivity management. Traditionally, cellular IoT connections relied on physical SIM cards, which were often locked into specific providers. These typically required swapping when entering new regions, countries, or even coverage areas within countries, making deployments difficult to scale, costly, and labor-intensive. Additionally, cellular IoT devices that leverage traditional SIM cards often ship without dedicated hardware-based security, relying instead on weaker software protections or none at all.

Figure 2: Growth trend for eSIMs/iSIMs vs other SIM types
Source: IoT Analytics



eSIMs and iSIMs help streamline and secure cellular IoT deployments. eSIMs and iSIMs have offered device makers solutions to at least connectivity management challenges, such as remote SIM provisioning (RSP), remote profile management, dynamic subscription switching, and lightweight, secure methods for device deployments. As the names suggest, eSIMs and iSIMs are either embedded in a cellular IoT module or integrated into the cellular IoT chipset of the IoT device. They are unique and programmable, allowing for remote network profile management, eliminating the need for users to swap physical SIM cards. Furthermore, these SIMs include embedded secure elements, which serve as unique elements of cellular IoT modules and chipsets, thereby enhancing the integrity of the IoT devices into which they are integrated.

Adoption of eSIM/iSIM technology has grown in recent years. In 2024, 32% of shipped cellular IoT modules were eSIM/iSIM-capable, and 17% of cellular IoT connections were eSIM/iSIM-capable devices. Driving their adoption is their ability to help device makers address security hardening, large-scale remote provisioning, carrier switching, SIM logistics, and small-form-factor and power-constrained devices.

2. Broad context: Foundational challenges for device makers

Scaling cellular IoT deployments has long posed challenges for device makers, largely due to security, device lifecycle management, interoperability, regulatory compliance, and connectivity management.

Security

As billions of devices come online, attackers are targeting weak trust anchors and fragmented provisioning processes. Many IoT devices still rely on physical SIMs without embedded secure elements, leaving authentication dependent on weaker methods. Even when secure elements are present, large-scale deployments face key management challenges across fragmented supply chains.

Recent attacks underscore the risks:

- **Maersk's NotPetya attack:** In June 2017, Maersk suffered a NotPetya cyberattack that disrupted shipping operations for weeks, causing $200–300 million in losses across key logistics business units.
- **Raptor Train Botnet:** In 2024, the Raptor Train Botnet compromised over 200,000 IoT devices, including routers and IP cameras, exploiting vulnerabilities to maintain large-scale control and posing significant risks to logistics network security.

Device lifecycle management

Cellular IoT devices often remain in service for many years, sometimes decades. This requires reliable over-the-air (OTA) updates and proper end-of-life decommissioning. Each stage poses operational and security risks.

OTA updates

OTA updates must be delivered securely throughout the device's lifespan, yet bandwidth limits, intermittent connectivity, and diverse hardware capabilities can make consistent patching and feature upgrades difficult.

Example: In January 2024, during Tesla's Autopilot recall rollout, some owners reported failed OTA updates that disabled driver-assist features, and in isolated cases, required service visits; the recall remedy itself was an OTA change, as per US NHTSA (National Highway Traffic Safety Administration) filings.

Decommissioning

Decommissioning is often neglected. It is the process of revoking credentials, removing device identities from networks and platforms, wiping local data, updating inventories, and disposing of hardware to eliminate latent risk.

Example: In the UK, millions of smart meters are expected to lose functionality when 2G and 3G networks are switched off by 2033. The Public Accounts Committee estimates 7 million meters will need costly hardware upgrades, showing how long lifespans, network sunsets, and weak forward compatibility can trigger replacement programs.

Interoperability

The cellular IoT ecosystem is highly fragmented, featuring diverse device types, varying connectivity standards, network operator requirements, and proprietary platforms. This means devices must be customized for different regions, operators, or vertical markets, leading to increased complexity, reduced scalability, and higher support costs. Examples of these interoperability issues include:

- **Diverse device types:** Fleet telematics vendors like **Samsara** and **Geotab** often require their sensors to pair only with their own proprietary gateways, meaning devices must be customized for different regions and platforms, increasing complexity and reducing scalability.
- **Standards:** India's Department of Telecommunications recently mandated that IoT device makers adopt oneM2M standards for M2M and IoT deployments. While this ensures interoperability within India, other markets continue using proprietary or fragmented protocols, creating additional engineering work and certification costs for device makers.
- **Proprietary platforms:** Proprietary telematics platforms like **Verizon Connect** and **Trimble** rely on vendor-specific data schemas and integration models. Migrating from one vendor to another can incur high costs, including data migration, retraining staff, and reworking integration points, which limits flexibility and increases the lifecycle cost of devices.

Regulatory compliance

Device makers must be aware of and comply with national and regional regulations in several areas:

- **Data sovereignty:** These laws, such as the GDPR in Europe and India's new Data Protection Act, compel device makers to manage region-specific cloud and data architectures.
- **Cybersecurity:** Device makers must demonstrate security-by-design and ongoing lifecycle management, as exemplified by the EU Cyber Resilience Act.
- **SIM registration:** These rules add a further burden. For example, Nigeria's 2022 biometric registration drive disrupted IoT connectivity when unverified SIMs were deactivated.
- **Telecom rules:** Rules placed on telecommunications companies, such as Brazil's restrictions on permanent roaming, require local agreements, while operator-specific certifications, like Verizon or China Mobile approvals, further fragment the market. This patchwork of compliance obligations hinders deployment, increases certification costs, and makes global scaling more challenging.

Connectivity management

While IoT device makers design devices to be secure, manageable, interoperable, and compliant with various regulations to bring them to market, managing connectivity once deployed presents its own set of challenges.

The cellular IoT ecosystem is highly fragmented, featuring diverse device types, varying connectivity standards, network operator requirements, and proprietary platforms

3. Connectivity context: Cellular IoT connectivity management challenges and solutions (deep dive)

Connectivity remains one of the most persistent hurdles in IoT. Device makers must overcome core obstacles such as roaming restrictions, inefficient provisioning, unreliable first-boot activation, inconsistent regional coverage, and legacy provisioning standards that were never designed for IoT.

Emerging solutions are beginning to address these barriers. eSIM and iSIM technology, together with Remote SIM Provisioning (RSP), enable dynamic operator switching and large-scale automation. The GSMA's new SGP.32 standard further adapts these capabilities for constrained, headless IoT devices, making provisioning more reliable and scalable.

The following sections examine core connectivity challenges in detail, along with the technologies and deployments shaping the next phase of global IoT connectivity.

eSIM and iSIM technology, together with Remote SIM Provisioning (RSP), enable dynamic operator switching and large-scale automation

Challenge A: Roaming barriers

Roaming is both expensive and restricted: Cellular IoT devices must operate across hundreds of networks worldwide; however, international roaming rules vary significantly by country and operator. Some markets ban or restrict permanent roaming altogether, and often, IoT devices pay two to five times more for roaming than local connectivity. Enterprises are forced into fragmented contracts that raise costs and complicate scaling.

Challenge example – Regional barriers: Brazil and Turkey ban permanent roaming outright, while China imposes strict controls on international SIM cards. In the US and Canada, there are no regulatory bans; however, operators frequently restrict long-term roaming in commercial policies.

Solution – eSIM/iSIM with remote profile management: eSIM and iSIM, combined with RSP, allow devices to download and switch to local operator profiles over the air dynamically, ensuring compliance and lowering roaming costs. By supporting dynamic network switching, eSIM/iSIM with RSP eliminates the need for separate SIM-related stock-keeping units (SKUs) and directly addresses the barriers of expensive and restricted roaming.

Solution example – G+D's AirOn360® IoT: G+D's AirOn360® IoT platform enables remote profile download and activation, allowing devices to shift from roaming to local operator profiles seamlessly. This ensures compliance with local regulations, eliminates the burden of long-term roaming, and provides enterprises with centralized orchestration to manage operator onboarding and connectivity policies across multiple countries.

Migrating hundreds of thousands of vehicles would have been unmanageable for automotive manufacturers with manual SIM swaps or factory preloading

Challenge B: SIM provisioning at scale

Manual provisioning is inefficient and costly: Provisioning millions of IoT devices cannot be done reliably with manual activation or pre-provisioned SIMs. Manual onboarding is too costly, while preloaded single-operator profiles lock devices to one network, limiting flexibility and increasing long-term costs. Further, GSMA's current SIM provisioning standard, SGP.22, was designed for smartphones and struggles with constrained IoT devices, often leading to failed profile downloads during initial activation.

Challenge example – Automotive OEMs: Migrating hundreds of thousands of vehicles would have been unmanageable for automotive manufacturers with manual SIM swaps or factory preloading. Manual updates across global fleets were too costly, while single-operator profiles would have locked vehicles to a single network, limiting flexibility and increasing long-term costs.

Solution – RSP with SGP.32: eSIM and iSIM, enabled by RSP, allow operator profiles to be securely downloaded and switched over the air. The new SGP.32 specification is optimized for the requirements of the broader IoT ecosystem, from low-power, low-memory environments to the automotive sector—making large-scale provisioning more reliable than legacy approaches.

Solution example – G+D and BMW: Since 2016, BMW has used G+D's AirOn360® solution to manage remote eSIM provisioning. Instead of loading country-specific SIMs at the factory, BMW downloads and activates local operator profiles over the air, supporting multiple operators with a single embedded SIM and avoiding costly manual updates.

Challenge C:
Bootstrapping failures and SKU fragmentation due to manual provisioning

Establishing reliable first-time connectivity remains a persistent hurdle in large-scale IoT deployments. Many IoT devices ship without active profiles, forcing manual or post-deployment provisioning. In constrained environments, limited memory, intermittent connectivity, or a lack of user interfaces often cause first-boot attempts to fail, leaving devices inactive in the field. Manual methods also drain battery life in devices such as smart meters and trackers.

Without secure in-factory provisioning, manufacturers face further inefficiency. Devices must be activated after deployment, which slows production cycles and increases logistics costs. To cope, many resort to SKU fragmentation, producing operator- or region-specific hardware variants, which adds inventory complexity and slows global scaling.

Challenge example – Taiwan Mobile and **Able Device:** In a smart meter deployment, devices shipped with only default passcodes and required credentials to be pushed post-deployment via SIM applets and binary Class-2 SMS. Because the meters left the factory without secure profiles, they could not establish reliable first-time connectivity. This post-factory provisioning created operational burden and highlighted the inefficiency of workflows that rely on in-field activation instead of secure in-factory profile loading.

Challenge example – SKU fragmentation: Quectel RM5xxQ series lists separate "Carrier Certification" tracks (Verizon, AT&T, T-Mobile, Telstra, Deutsche Telekom) alongside "GL" vs "AE" models, creating distinct variants that OEMs must manage as different SKUs.

Solution – In-factory profile provisioning (IFPP): The GSMA's IFPP (SGP.41/42) allows secure operator profiles to be loaded during manufacturing. Devices leave the factory ready for connectivity, ensuring reliable first boots while preserving battery life. IFPP also supports late personalization, enabling a single global hardware SKU to be adapted for multiple markets and operators.

IFPP also delivers additional benefits: by digitizing profile injection during manufacturing, OEMs can reduce logistics complexity, avoid the need for GSMA SAS accreditation in their factories, and support sustainability by eliminating the plastic and CO2 impact of physical SIM cards.

Solution example – G+D's AirOn360® In-Factory eSIM: With its IFPP solution, AirOn360® In-Factory eSIM, G+D has provisioned over 100 million profiles for a leading OEM. Devices left the factory "connectivity ready," reducing SKU fragmentation, accelerating time-to-market, and avoiding costly post-deployment activation.

Challenge D:
Ensuring reliable connectivity across regions

Challenge scenario – Insights from G+D

"Whether it's a logistics enterprise moving goods across European borders or a utility enterprise managing smart meters in remote U.S. regions, relying on a single carrier can lead to blind spots, service disruptions, and costly delays. Inconsistent roaming agreements or local network limitations not only disrupt delivery schedules but also complicate compliance with cross-border data and transport regulations. For critical infrastructure, even short lapses in connectivity can have serious operational and regulatory consequences. This is a clear reminder that regional diversity in mobile networks demands a smarter, more flexible connectivity strategy. With intelligent connectivity management, devices can switch profiles dynamically—across borders or within a country—ensuring continuous service, faster recovery, and giving enterprises full control over network connectivity wherever their assets operate."

Alistair Elliott, Head of Connectivity Portfolio, Giesecke+Devrient

Solution – Dynamic subscription switching and centralized orchestration: With eSIM or iSIM, devices can automatically switch to a different operator profile when coverage or performance drops. Centralized orchestration platforms allow enterprises to define switching policies, automate provisioning, and monitor all devices through a single interface, ensuring consistent service quality across borders.

Solution example – G+D's IoTgo® Suite: A global logistics operator uses G+D's IoTgo® Suite to enforce policy-based dynamic switching. When devices detect coverage loss or regulatory restrictions, the platform triggers a remote profile download to a local operator. From a single console, the enterprise manages onboarding, policies, and monitoring—reducing downtime, site visits, and operational overhead while maintaining continuous service worldwide.

Challenge E: Pre-SGP.32 provisioning limitations

Before SGP.32, enterprises relied on earlier GSMA standards: SGP.02 for M2M and SGP.22 for consumer devices. Both were poorly suited to IoT. SGP.02 demanded complex, carrier-to-carrier integrations that slowed projects and raised costs. SGP.22 eased some workflows but was designed for smartphones with powerful hardware, stable LTE/5G connections, and user interfaces. IoT devices, by contrast, are headless, power-constrained, and often operate with intermittent coverage.

As a result, deployments faced multiple barriers:

- **High integration effort:** Each new operator required bespoke backend projects, including SM-DP or SM-SR connectivity, APN setup, IPsec tunnels, and market-specific acceptance testing.
- **Unreliable provisioning:** SGP.22 assumed the presence of a Local Profile Assistant (LPA) with user interaction. Without a UI, IoT devices could not recover from failed downloads, leaving many stranded in the field.
- **Inefficient protocols:** Reliance on HTTPS and SMS created heavy signaling overhead, draining batteries and reducing reliability for NB-IoT and LTE-M devices.
- **Poor scalability:** Workflows were designed for individual devices rather than fleets of millions, limiting adoption in logistics, utilities, and industrial IoT.

Challenge scenario – Insights from G+D:

"Before SGP.32, IoT provisioning was a patchwork of consumer-grade workflows and costly backend integrations. Enterprises had little control, relying on carrier-driven processes that didn't scale. A European automotive OEM had to build custom tunnels for every operator just to get vehicles online across markets. Meanwhile, a U.S. utility company struggled with headless devices going offline due to failed profile downloads. SGP.32 changes that—putting control back in the hands of users with seamless, automated provisioning, lower costs, and freedom to define connectivity on their terms."

Sam Colley, Senior Product Strategist, Giesecke+Devrient

Challenge E: Pre-SGP.32 provisioning limitations

Solution – SGP.32 for IoT-optimized provisioning: The new SGP.32 standard was designed specifically to address these shortcomings. It is part of the common GSMA eSIM ecosystem used for both consumer and IoT devices. It builds on, and is integrated with, the SGP.22 ecosystem (SM-DP+ model) but introduces IoT-specific components: the IoT Profile Assistant (IPA) within the device and the eSIM IoT Remote Manager (eIM) in the network. Together, these enable automated provisioning and lifecycle management across entire fleets, triggered by events such as first activation or coverage changes.

Key improvements include:

- **Lower integration cost:** Enterprises integrate once with SM-DP+, eIM, IPA, and SM-DS. New operators can be added simply by loading profiles, removing the need for bilateral backend projects.
- **Efficient, scalable workflows:** Lightweight protocols such as CoAP, MQTT, and LwM2M, along with a minimal IoT profile just a few hundred bytes in size, enable secure provisioning even on constrained networks and support parallel activation of millions of devices.
- **Stronger security and discovery:** SGP.32 integrates SM-DS with IPA for autonomous profile discovery and uses DTLS-based mechanisms aligned with 3GPP IoT security requirements, ensuring resilience even in low-bandwidth environments.

Solution example – G+D and Murata: In April 2025, G+D received the first GSMA eSIM Compliance and eUICC Security Assurance certifications for an SGP.32 IoT eUICC. SGP.32 v1.2 with GSMA test, compliance, and security schemes provides a certified, interoperable path for secure eSIM IoT deployments. G+D has integrated SGP.32 into its IoTgo® Suite platform, enabling automotive and industrial customers to provision and manage fleets automatically. In partnership with Murata, it also launched the first SGP.32- and iSIM-compliant connectivity module. The module combines Murata's hardware with AirOn360® IoT to deliver zero-touch provisioning and lifecycle management directly inside an iSIM. Targeted at smart metering, logistics, and automotive, it shows how SGP.32 enables power-efficient, large-scale connectivity for constrained devices—overcoming the one-device-at-a-time limitations of previous standards.

4. Vertical case examples: Transport & logistics

Connected operations in transport and logistics require continuous data from vehicles, cameras, and cargo. At a global scale, connectivity underpins safety, compliance, and efficiency. Yet, operators face recurring barriers, including roaming restrictions across borders, downtime caused by coverage gaps, and device fragmentation stemming from multiple SKUs or provisioning models. The use cases below are mapped to Challenges A–E, and each includes a concise example with clear roles.

Telematics and fleet tracking

How it works: On-board units collect GPS, vehicle health, and driver data via a cellular modem with eSIM. Policies govern operator profile selection and roaming behavior.

Challenges addressed: A, B, D

Example – U.S.-based fleet management provider with G+D eUICC: A fleet management enterprise uses eUICC with a multi-IMSI bootstrap, enabling over-the-air reconfiguration to different operators or core networks when coverage degrades. Policy triggers include roaming blocks and latency spikes. If a profile fails, the SIM reverts to the bootstrap, keeping telemetry online. Results include resilient cross-border uptime, faster recovery, and up to 70% fewer risky driving events.

Roles: The enterprise provides on-board units (OBUs) and telematics software; G+D provides eUICC connectivity and the fleet console.

Dashcams and driver monitoring

How it works: AI dashcams capture road and driver video, uploading critical clips over cellular. eUICC profile changes maintain connectivity across networks and borders.

Challenges addressed: A, B, D

Example – Global logistics technology enterprise with G+D's eUICC: The enterprise deploys AI dashcam cameras that record high-definition dual streams and preserve pre/post-incident video. Policy-driven profile changes ensure uninterrupted uploads for analysis and claims. Fleets report more than 50% lower risk and up to 70% fewer risky driving events.

Roles: The logistics enterprise provides dashcams and analytics; G+D supplies multi-operator eUICC connectivity.

Track and trace for cargo

How it works: Battery-powered trackers monitor container location and conditions, ensuring continuous connectivity as shipments cross borders.

Challenges addressed: A, D

Example – DB Cargo with G+D solar-powered tracking and connectivity: A leading European rail freight operator has deployed solar-powered IoT trackers to monitor cargo wagons across borders. The solution supports dynamic roaming based on location, ensuring reliable connectivity even in regions with limited mobile network access. The trackers operate autonomously for years without battery replacement, enabling real-time location and condition monitoring while reducing maintenance costs and environmental impact.

Roles: The rail operator deploys and manages the trackers; G+D provides the solar-powered tracking solution, connectivity, and orchestration platform.

Cold chain monitoring

How it works: Sensors feed temperature and power data to a cellular gateway, which streams readings for alerts and audit trails.

Challenges addressed: A, B, D

Example – G+D and RemoteM: Multi-network SIMs fail over per policy when coverage drops, ensuring continuous data flow. Over-the-air control prevents site visits. Fleets gain reliable alerts for vaccines and other regulated goods, reducing spoilage incidents.

Roles: G+D supplies connectivity and monitoring; device partners supply sensors and gateways.

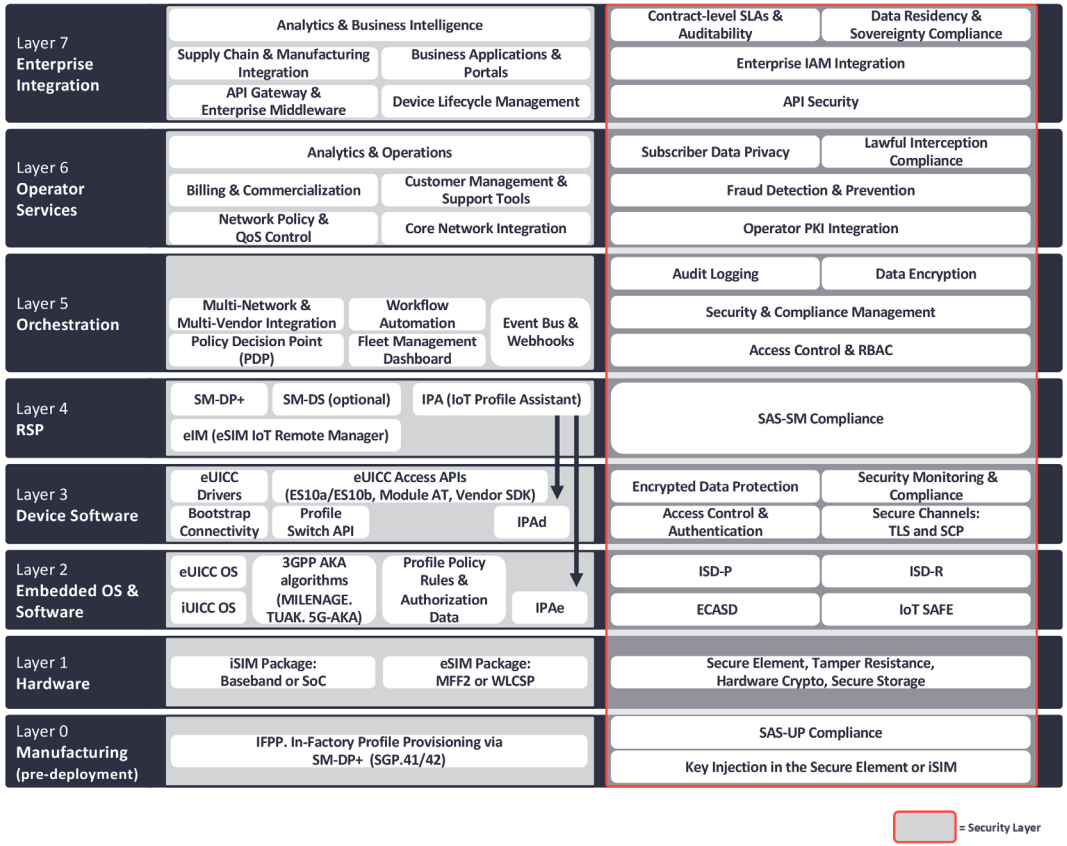
Implications for transport and logistics

- **Continuity:** Multi-operator access with policy switching reduces outages; deep indoor coverage can be improved by up to 40%. Firmware downloads fall from 63 hours to under 5 when multiple networks are used.
- **Scale:** RSP with profile swaps enables parallel rollouts without site visits. Fleets report up to 70% fewer risky driving events when telemetry and video stay connected across borders.
- **Compliance and cost:** Smart containers with local profiles meet roaming rules in restrictive markets, cutting SIM handling and exposure. IFPP and bootstrap connectivity support one global SKU with day-one connectivity, while SGP.32 scales to millions of constrained devices.

5. Industry landscape: Benefits of full-stack connectivity providers

Figure 3: Full tech stack of IoT eSIMs/iSIMs

Source: IoT Analytics



What "full stack" means

A full-stack provider covers the entire chain: SIM/eUICC [1]; RSP and discovery [2]; in-factory provisioning [3]; policy orchestration [4]; device-management hooks [5]; security [6]; analytics and operations [7]; integration, billing, compliance [8–10]; and supply-chain support for a global SKU [11].

Why it matters

- **Reduced complexity.** One architecture, API, and SLA across layers replace custom integrations.
- **Better management.** A single console correlates profile actions, device events, and network KPIs for faster troubleshooting.
- **End-to-end security.** SIM/iSIM hardware roots of trust enable IoT SAFE or PKI, combined with SBOM/VEX, cryptographic signing, and origin controls.
- **Faster time-to-market.** SGP.32 enables zero-touch activation for headless devices; SGP.41/42 supports the provisioning of global SKUs at the factory.

How it compares to limited offers (e.g., "SIM + platform")

Many offers stop at eUICC and SM-DP+. Device hooks, security, analytics, and policy orchestration are often left to third parties, resulting in handoffs, SLA gaps, and slower recovery times. Full-stack providers control the critical layers end-to-end, so incidents are routed to a single NOC and resolved more quickly. For example, **G+D offers a full-stack solution**.

Figure 4: G+D eSIM Technology Stack and Product Portfolio
Source: IoT Analytics

Case study – Scania connected trucks

Scania, one of the world's largest commercial vehicle manufacturers, operates trucks across more than 100 countries. Connectivity is now central to its business model: trucks need continuous links for telematics, safety functions like eCall, predictive maintenance, and compliance reporting. As the fleet expands globally, Scania faces operational complexity in managing connectivity across diverse regulatory regimes, mobile network operators, and RSP standards. The company's experience illustrates the structural challenges enterprises encounter when scaling IoT deployments in transportation.

Challenges (mapped to A–E)

A. Global network fragmentation & roaming complexity. Scania must keep trucks connected worldwide and manage multiple network profiles for eCall, telematics, and infotainment. Mixed standards (legacy and new) add complexity.

B. Provisioning at scale. A global OEM requires automated enrollment and a single interface to manage connectivity across various vehicle programs and markets. Manual processes do not scale.

C. SKU fragmentation. Scania operates mixed fleets across SGP.02 and SGP.32; tooling must handle both without creating variant SKUs or field rework.

D. Reliable connectivity across regions. Real-time diagnostics and policy automation are crucial for maintaining service continuity as vehicles transition between networks and countries.

E. Pre-SGP.32 provisioning limits. Managing two RSP generations is now a reality; the suite must support both and facilitate a smooth transition to SGP 32.

Solution

Scania adopted G+D's IoTgo® Suite for orchestration. Remote Profile Management ensures roaming compliance, while IFPP reduces SKU variants. This allows Scania to manage legacy and next-gen fleets in one platform, automate provisioning, and maintain global service continuity.

Benefits

Operational overhead fell, as fragmented operator processes were consolidated. Automated provisioning accelerated deployment, while diagnostics improved network visibility. Most importantly, Scania sustained reliable connectivity across borders while transitioning to SGP.32, ensuring continuity for legacy vehicles and readiness for future growth.

"With G+D's IoTgo® Suite, we've been able to smoothly transition to the new SGP.32 standard while continuing to maintain reliable connectivity for our existing fleet using SGP.02. The platform provides us with detailed diagnostic data and offers us an efficient, scalable solution to manage all our connected vehicles, ensuring seamless operations across both legacy and next-gen technologies."

– **Peter Vincent**, Head of Connected Systems at Scania

6. Conclusion: Enabling secure, scalable IoT for T&L and device makers

Cellular IoT is entering its scale phase, with 40 billion IoT devices expected by 2030, including 9.1 billion cellular IoT connections. Transport, supply chain, and logistics already represent 35% of that base. Growth is real, but so are the hurdles.

Cross-border fleets face roaming restrictions, first-boot often fails on constrained devices, provisioning remains manual, tools are fragmented, and security must endure for years. These frictions slow launches and raise costs.

A full-stack eSIM approach changes this. SGP.32 enables IoT-optimized remote provisioning for headless devices through eIM and IPA. IFPP (SGP.41/42) binds EIDs in the factory to support a single global SKU with day-one connectivity. Policy engines select compliant local profiles, while device hooks push APNs and trigger updates. Unified telemetry closes the loop from network to operations.

What to do now

- Build new programs on SGP.32 while maintaining SGP.02 for legacy fleets.
- Use IFPP at the factory to preload bootstrap profiles.
- Operate from one console for provisioning, policy, and incident response.
- Anchor identity in SIM/iSIM with PKI or IoT SAFE, protect transport with TLS/DTLS, and enforce SBOMs, signed updates, and key rotation.
- Track initial network attachment, profile swap success, incident repair times, and battery impact.

This path accelerates launches, reduces incident rates, and scales securely across borders.

For more information visit: www.gi-de.com