IoT Now: ISSN 2397-2793

2026 • VOLUME 16 • ISSUE 1

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

floLIVE's Nir Shalom has one simple question for AI-led IoT success - What's your network plan?

CONNECTIVITY
Understand how connectivity leaders should approach the market. Read the IoT Now Report at **www.iot-now.com**

IoT SECURITY
Why enterprises need IoT security-as-a-service. Read the IoT Now Report at **www.iot-now.com**

TRANSPORT
Expanded use cases and new connectivity needs. Read the IoT Now Report at **www.iot-now.com**

UTILITIES
Learn how to deliver smart metering for a changing world in out latest Market Report inside

IoT GLOBAL NETWORK
Log on at **www.iotglobalnetwork.com** to discover our portal for products, services and insight

PLUS: Exclusive MWC26 Barcelona event preview • Get in the check-out queue for frictionless IoT connectivity • Aeris exceeds 100 million connections • Hyundai partners with Vodafone IoT in Middle East • Inside Thingsdata's global expansion • How LionsBoT autonomous robots achieved global connectivity • Giesecke+Devrient demystifies SGP.32 • Transforma Insights on how SPoG techniques can de-risk SGP.32 SIM adoption • Three key questions to ask connectivity providers - and their answers • How to ensure resilience for your critical IoT deployments • Read the latest News, Features and Interviews at **www.iot-now.com**

MWC GSMA | 4YFN

THE IQ ERA HAS BEGUN – IS YOUR BUSINESS READY?

MWC BARCELONA | FIRA GRAN VIA | 2–5 MARCH 2026

Join us at MWC26 Barcelona as we usher in The IQ Era – a new age of connected intelligence where human-centred thinking drives transformative change.

Through targeted thought leadership themes we'll explore the rapid growth and development of the connectivity ecosystem under the all-encompassing influence of AI and other game-changing technologies.

Don't miss it.

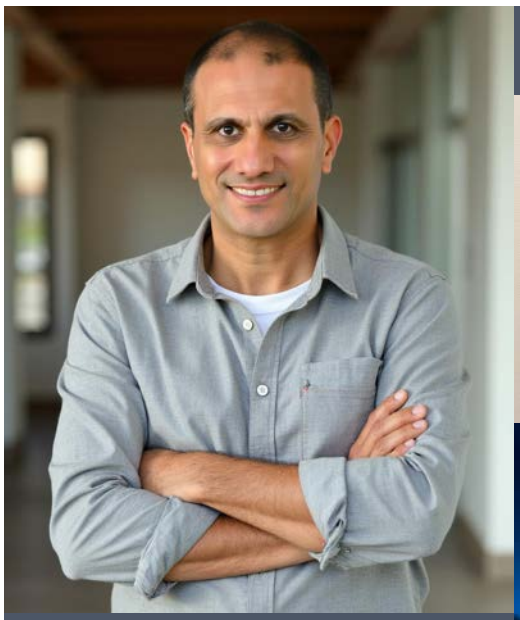
Register now to get your pass at **mwcbarcelona.com/passes**

Theme sponsors

INTELLIGENT INFRASTRUCTURE
CONNECT AI
AI 4 ENTERPRISE
AI NEXUS
TECH 4 ALL
GAME CHANGERS

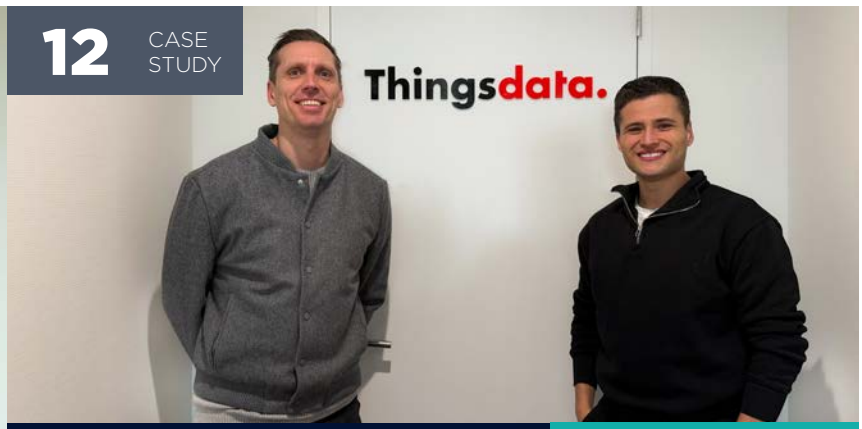
snowflake
HONOR
CSG
KPMG
Infosys Navigate your next
taara

CONTENTS



08 INTERVIEW
Nir Shalom, chief executive floLIVE

12 CASE STUDY



Connecting smart meters
A guide to long battery life, wide coverage and secure deployments with cellular LPWA

35 MARKET REPORT

IN THIS ISSUE

Long-expected items in basket

Simplification of cellular IoT connectivity is finally here. Innovation on the specification front has delivered SGP.32, the IoT-specific SIM framework from GSMA. For the first time this puts in place a foundation for enabling IoT connectivity, radically streamlining the process of connecting devices. This enables greater efficiency from the factory to the deployment site, improved flexibility to support decreased downtime and faster, easier device deployments across the globe

SGP.32 isn't the only driver behind these benefits. IoT solutions providers have been working to make connectivity simpler for more than a decade and we're now getting to the point where cellular SIMs can be bought off-the-shelf from service providers' stores. The next step is to ride the embedded wave and adopt technologies to orchestrate connectivity capabilities in devices from the point of manufacture, throughout the entire in-service life of a product.

In this issue, the experts at **Giesecke+Devrient** point out that connectivity should be viewed as a flexible resource – a lifecycle capability, not a one-time configuration choice. The **Wireless Broadband Association** states that connectivity must be effortless and trustworthy in an AI era and, on the opposite page, we report on **AT&T** going even further to offer an off-the-shelf end-to-end IoT solution on the **AWS Marketplace**.

Connectivity has been a barrier to IoT innovation for too long. It has demanded complex skills for organisations to pick their way through carriers' unique processes, it has required IoT enterprises to devote resources to configuring their device connectivity at the point of deployment and there has been limited flexibility to adjust parameters even during the decade-or-more lifespan of some IoT applications.

It's time to strip away the complexity, limit the friction and empower IoT innovators to get on with their core business of creating compelling new use cases that transform how we live, work and play. Being able to go to a store and select a portfolio of connectivity, foundational technologies and secure, cloud infrastructure seems an obvious step that has taken until now to happen. I'll see you in the check-out queue.

George Malim, managing editor

Enjoy the magazine

George Malim

MANAGING EDITOR
George Malim
Tel: +44 (0)7930 301 841
g.malim@wkm-global.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: +44 (0) 1732 808690
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: +44 (0) 1732 807410
c.jameson@wkm-global.com

DESIGN
Jason Appleby
The Ark Design Agency
Tel: +44 (0) 7801 817 139

PUBLISHED BY
WeKnow Media Ltd. Suite 138,
80 Churchill Square, Kings Hill,
West Malling, Kent ME19 4YU, UK
Tel: +44 (0) 1732 807410

AT&T launches first end-to-end IoT solution on the AWS Marketplace with Connected Spaces

AT&T has announced that its Connected Spaces solution is now available as its first end-to-end Internet of Things (IoT) offering listed on the **AWS Marketplace**, marking a significant step in simplifying smart business operations for small and medium-sized enterprises (SMEs). AT&T Connected Spaces is a plug-and-play IoT solution designed to help businesses monitor and manage their environments in near real-time. The solution combines pre-integrated wireless sensors and a secure cloud platform with intuitive dashboards to deliver actionable insights without requiring in-house IT expertise.

Businesses can track critical metrics such as temperature, humidity, motion, energy usage and security, enabling them to optimise resources, reduce downtime and enhance customer experiences. By joining AWS Marketplace, AT&T is making it easier than ever for businesses to discover, purchase and deploy Connected Spaces through a trusted cloud commerce platform. This listing streamlines procurement, accelerates time-to-value and provides a scalable, data-driven solution that can support a wide range of industries such as retail, hospitality, healthcare, warehousing and property management.

Mike Van Horn, AT&T

"Connected Spaces is about giving businesses the tools to make smarter decisions, faster," said Mike Van Horn, the associate vice president at AT&T Connected Solutions. "Bringing our first end-to-end IoT solution on AWS Marketplace reinforces our commitment to innovation and accessibility for businesses of all sizes."

Connected Spaces offers a range of features designed to simplify IoT adoption. Businesses benefit from easy installation with pre-staged sensors and dashboards, near real-time monitoring of environmental conditions, and customisable alerts when thresholds are exceeded. The solution is built for scalability, allowing organisations to add sensors as their needs evolve, and offers extended range and long battery life for reliable performance. With data encrypted end-to-end, businesses can trust that their information is protected.

Aeris exceeds 100 million connected devices, delivering nearly 90% growth and outpacing IoT market

Aeris has surpassed 100 million connected devices worldwide. This landmark achievement is a result of nearly 90% growth in additional device connections since the 2023 acquisition of the **Ericsson** IoT Accelerator Platform.

According to a report from **Berg Insight**, global cellular IoT connectivity grew by approximately 30% over the same period, making Aeris' expansion nearly three-times the industry average. The company says this growth validates its commitment to simplifying global deployments through AI-driven connectivity management platform innovation, IoT cybersecurity and automotive leadership, and a strong partner ecosystem.

"This milestone validates our vision of providing the world's most trusted end-to-end solution for cellular devices," said Aziz Benmalek, the chief executive and board director at Aeris. "Reaching 100 million connections is not merely scale — it's evidence of how rapidly we're transforming business outcomes. By using agentic AI, we will continue to elevate our capabilities to protect data and ensure reliability in the highest stakes environments, from connected vehicles to lifesaving medical devices."

Aziz Benmalek, Aeris

News in Brief

Telenor IoT passes 30 million connected units

Telenor IoT has reached more than 30 million connected units deployed worldwide. This achievement reflects Telenor IoT's continued commitment to innovation, customer success, expanded partnerships and global expansion.

"Surpassing 30 million connected units is a testament to the trust our customers place in us and the strength of our global IoT strategy," said Mats Lundquist, the CEO of Telenor Connexion and the head of Telenor IoT. "We will continue to innovate and invest in technologies that help enterprises scale connected solutions securely and efficiently. Our goal remains clear: to be the first choice for IoT."

Netmore acquires Actility to lead global transformation of massive IoT

Netmore Group, a network operator for massive IoT, has announced its acquisition of Paris-based **Actility**, a pioneer in low-power wide-area network (LPWAN) solutions with a presence across Europe, North America, the Middle East and Australia – along with its subsidiary **Abeeway**, a contributor in ultra-low power multi-technology geolocation. Benefiting from synergies across commercial markets, this transaction strengthens Netmore's leadership in its primary vertical segments including utilities, buildings and smart cities, while expanding reach into the enterprise, industrial, asset tracking and operator sectors.

One of the original authors of the LoRaWAN specification and a founding member of the **LoRa Alliance**, Actility brings Netmore thousands of LoRaWAN project deployments across more than 100 countries, partnerships with over 50 LoRaWAN network operators, and a customer base that includes Tier-1 operators and global utility and manufacturing leaders. Contracted IoT devices now under Netmore management total over 14 million.

Hyundai Motor Group partners with Vodafone IoT to deploy connected cars in the Middle East

Hyundai Motor Group has partnered with **Vodafone IoT** to deploy regulatory-compliant in-car connectivity to Bahrain, Kingdom of Saudi Arabia (KSA), Kuwait, Qatar and the United Arab Emirates (UAE) in the Middle East. In collaboration with Vodafone IoT's network partners in the region – such as **e& UAE** – Hyundai Motor Group will receive reliable and secure in-car connectivity that is compliant with local laws.

Vodafone IoT provides Hyundai Motor Group with seamless in-car connectivity in the Middle East, thanks to its Global SIM+ solution – which dynamically turns its Global IoT SIM into a local SIM. This offers local network credentials, data routing, compliance with national laws and seamless cross-border connectivity – making it easier and more efficient for carmakers and manufacturers to launch services in regulated countries, as well as giving them global access to connected services.

Combined with Vodafone IoT's managed connectivity platform which integrates directly into the local network partner's infrastructure, manufacturers can manage their global IoT estate from a single platform – giving them truly global reach and centralised control over their operations.

Erik Brenneis, the CEO of Vodafone IoT, said: "As manufacturers look to deploy connected vehicles in diverse geographies, it is vitally important that they are provided with connectivity that's reliable, secure and compliant with national regulations. We are proud to partner with Hyundai Motor Group to deliver innovative in car connectivity powered by our Global SIM+ which provides local credentials and a seamless cross border service. It turns vehicles into secure connected platforms – keeping drivers and passengers safe, informed and connected." ■

Erik Brenneis, Vodafone IoT

News in Brief

Phoenix and Disruptive partner to accelerate building automation

Phoenix Energy Technologies, a contributor in lifecycle asset optimisation for multi-site commercial buildings, has announced a partnership with **Disruptive Technologies (DT)**, a pioneer in delivering ultra-reliable wireless data insights for the healthcare and food retail sectors. Together, the companies are combining Phoenix's expertise in HVAC, refrigeration and lighting optimisation with DT's data to deliver richer insights, better benchmarking and more automated workflows for national and global portfolios.

Phoenix Energy Technologies specialises in integrating and optimising HVAC, refrigeration and lighting systems across large, distributed commercial building fleets such as retail, grocery, C-store and outpatient healthcare. Through its EnterpriseDX platform, Phoenix connects to enterprise HVAC and lighting control systems as well as a wide range of IoT devices. This provides customers with a centralised view and a single point of control across many different building systems, vendors and software components, both at the individual site level and across the entire enterprise. ■

New deal will track containers

WiseTech Global and Hapag-Lloyd launch IoT container tracking pilot

WiseTech Global, a developer of logistics execution software and supply chain technology solutions, has announced a new partnership with **Hapag-Lloyd**, one of the world's largest container shipping lines and a first mover in equipping its two million container fleet with smart devices, to trial the integration of Internet of Things (IoT) technology for real-time global container visibility, tracking and data collection.

Through this initiative, Hapag-Lloyd's fleet is equipped with IoT devices that frequently transmit location updates directly to WiseTech's ecosystem of platforms for the logistics, global trade and supply chain industry. This pilot specifically tests the ability to ingest and process millions of data points daily, applying advanced algorithms to transform the IoT data into meaningful products used to drive decision-making.

WiseTech can then distribute the location and positioning data to Hapag-Lloyd's customers via a range of channels such as the CargoWise Cargo Tracker and Container Automation solutions. More distribution channels are planned, including via GLO, INTTRA and Neo.

By unlocking richer visibility and smarter forecasting, WiseTech and Hapag-Lloyd are setting the stage for a new era of data-driven logistics execution, empowering customers with unprecedented accuracy and control across global supply chains.

Zubin Appoo, the chief executive officer of WiseTech Global, said: "The shipping industry has long relied on discrete and often inaccurate event updates that may lag by hours or even days. By bringing IoT-driven live container data and tracking into CargoWise, we're revolutionising supply chain visibility. This collaboration with Hapag-Lloyd harnesses data at significant scale to turn it into intelligence that customers can act on, to reduce uncertainty, improve efficiency and make smarter decisions." ■

TRANSFORMA

INSIGHTS

Global Advisors on IoT, AI and Digital Transformation

Every year Transforma Insights publishes its list of IoT 'Transition Topics' highlighting where we expect to see seismic change occurring during the year. This year the list focuses on the intersection of AI and IoT, the persistent challenge of regulation, greater localisation, and the impact of a shifting connectivity technology landscape.

IoT Transition Topics 2026

- AI-enabled IoT video analytics poised for explosive growth
- IoT vendors use AI to optimise and differentiate their offerings
- A shake-out is on the cards for cellular network technologies
- The rise of the Single Pane of Glass platform
- Continued geopolitical challenges and polarisation of markets
- The increasing requirement for localisation
- The rubber hits the road for SGP.32
- How to sell more IoT?
- Hardware innovations driving growth
- The implications of the evolution to software-defined vehicles

To learn more about the Transition Topics, you can find more details in our press release: transformainsights.com/news/iot-transition-topics-2026

The Transition Topics will form the basis of a significant part of the research agenda for the Transforma Insights Advisory Service in 2026, as well as sponsored Position Papers and Virtual Briefings. To learn more about our 2026 Research Agenda, or to discuss sponsorship opportunities, please contact us at enquiries@transformainsights.com

The overlooked question in AI-led IoT is the simplest one - What is your network plan?

As enterprises roll-out AI across connected devices, attention often focuses on value, use cases, governance, deployment and compliance. Yet many organisations overlook a more fundamental dependency. If the network cannot deliver the required coverage, performance, intelligent routing, local behaviour and sovereign data handling, AI workloads will struggle to scale.

Nir Shalom, the chief executive of floLIVE, tells IoT Now that the most overlooked question in AI-led IoT is also the simplest: What is your network plan?

Our network is global in reach, yet hyperlocal in operation

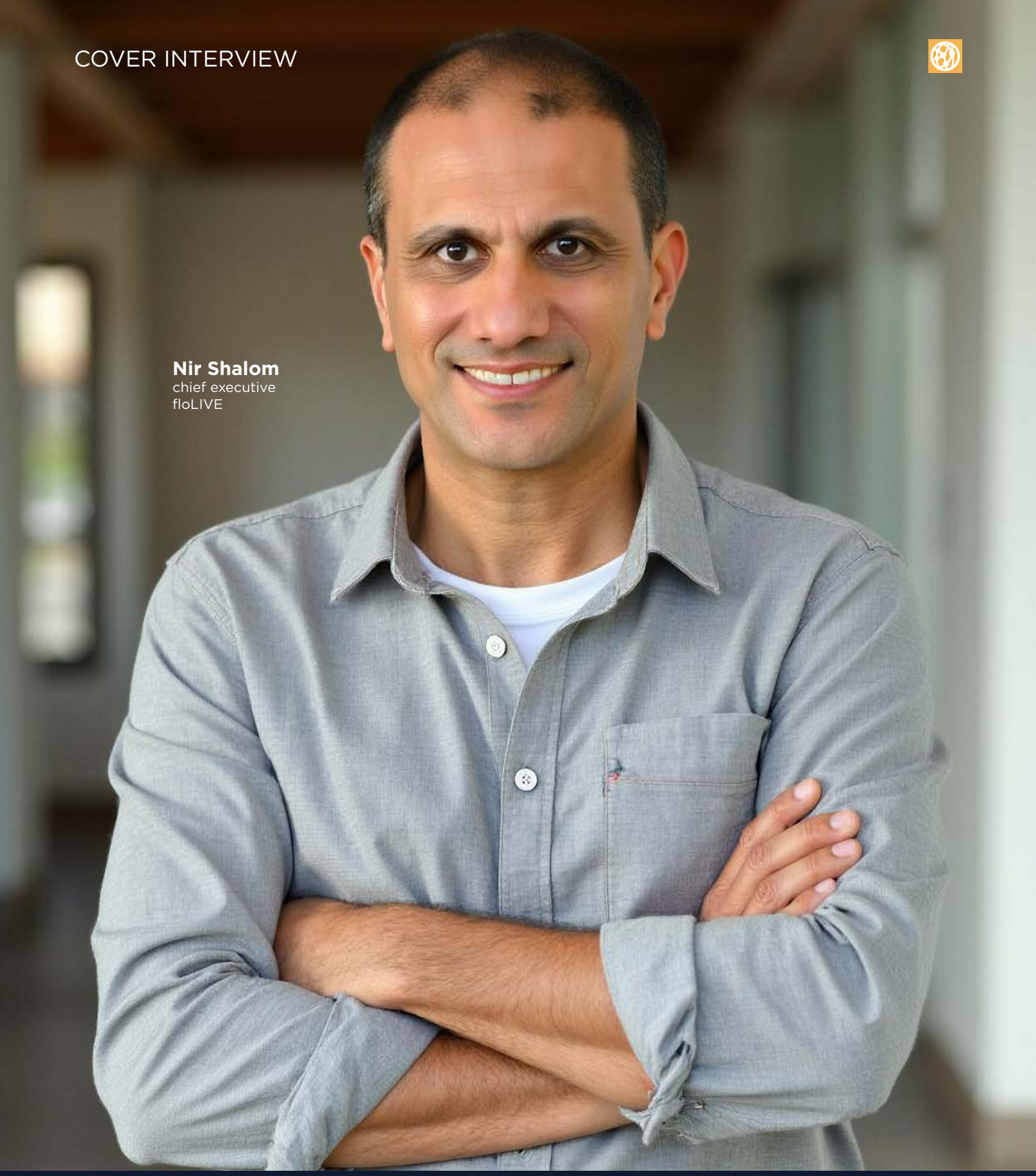
IoT Now: Nir, for readers who may not know you or floLIVE, what problem are you solving in the IoT connectivity market, and what is floLIVE's mission?

Nir Shalom: We connect any device, anywhere in the world. Unlike traditional IoT connectivity solutions that rely heavily on roaming agreements and legacy technologies, we make use of the world's largest purpose-built global cellular network for devices. Our network is global in reach, yet hyperlocal in operation – connecting devices locally across regions worldwide. This approach eliminates common challenges such as data sovereignty risks and high latency, while still providing enterprises with a unified, global view of all their connected assets.

In addition, our platform delivers extensive real-time visibility and control over network behaviour, enabling customers to actively monitor, manage and optimise connectivity performance across their entire device fleet.

AI accelerates the need for such advanced networks. As AI moves into connected devices ▶

SPONSORED INTERVIEW

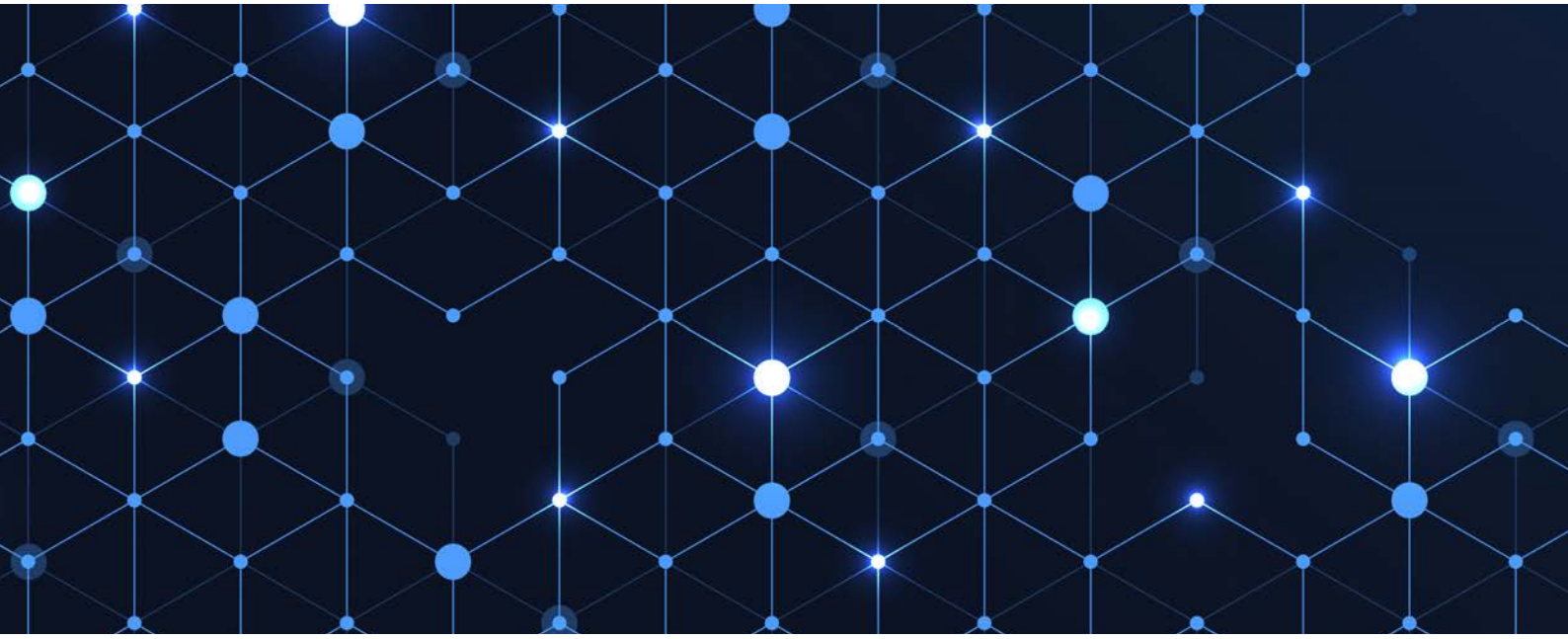


Nir Shalom
chief executive
floLIVE

and edge environments, enterprises want to operationalise models using their own data within secure and compliant architectures. Our focus at floLIVE is on providing a global network infrastructure built for those requirements, allowing IoT deployments to scale globally while behaving locally everywhere, with performance and sovereignty supported by design.

IoT Now: When you speak with enterprise leaders planning AI across connected devices, what questions are they asking today? And what is the one question you rarely hear but believe should be asked early?

NS: Enterprise leaders I speak with are primarily asking how to generate real business value from ▶



The first pillar is control and compliance, allowing customers to shape network behaviour so data remains local and aligned with the AI architecture

AI across connected devices. Once they identify the opportunity, their focus shifts to architectural questions: should intelligence sit at the edge or in the cloud, how does data gravity influence deployment, and how do they manage complexity while balancing security, data sovereignty and cost?

The question I rarely hear early enough - but believe is essential – is: What should the network look like to support this AI strategy? Global AI deployments, network topology, latency, sovereignty and control become foundational constraints that must be designed intentionally from the start. A deliberate network plan is required to ensure that the network topology supports data gravity needs; otherwise, the benefits of local storage are lost to high latency and poor routing

IoT Now: Many enterprises assume that choosing a strong operator in a mature market is enough. How reliable is that assumption in practice?

NS: In practice, that assumption is often unreliable. While traditional operators may offer strong local coverage in mature markets, they are generally not equipped to support the architectural requirements of enterprise AI deployments.

Legacy operator networks are not designed to be flexible around AI needs. If an enterprise wants to run inference at the edge, the network architecture must support that, meaning core functions and breakout points need to sit closer to the inference point. Operators typically won't adapt their topology or routing behaviour to match a customer's AI workload.

IoT Now: If that is the reality domestically, what happens when organisations scale globally across dozens of countries and regulatory environments?

NS: Now you multiply the problem.
Every assumption is multiplied across different networks, performance characteristics and regulatory frameworks. Connectivity models based on roaming or centralised hubs introduce unpredictability from one market to the next.

For AI-driven systems, that unpredictability is a serious constraint. Latency, throughput and routing behaviour directly affect performance and compliance. Enterprises need global consistency combined with local behaviour everywhere, delivered through a single, coherent network architecture. Without that, large-scale AI-led IoT becomes difficult to govern and optimise.

IoT Now: Many organisations treat data sovereignty as a storage problem. What are they missing?

NS: They are missing everything that happens between the device and the application. While storage location (aka: 'data gravity') matters, sovereignty also depends on how data moves, where it exits the network, which jurisdictions it traverses and where processing and inference occur.

AI makes this far more sensitive. Data flows become continuous and decisions happen in real time. If connectivity routes data out of the country and back again, organisations can breach requirements without intending to. At that point, sovereignty becomes an architectural concern, not a policy checkbox.

IoT Now: Many AI teams say they will run inference at the edge for privacy. Why is that not automatically a sovereignty solution?

NS: Because 'edge' describes where inference runs, not how data moves.

Even when inference happens locally, devices still exchange telemetry, receive updates and send insights back into central systems. If the network routes that traffic through distant or uncontrolled jurisdictions (like roaming), the expected sovereignty benefits disappear.

Edge AI reduces exposure at the endpoint, but true sovereignty requires a network architecture that keeps data local throughout its entire journey.

IoT Now: How do you design a network that behaves locally everywhere?

NS: You move away from roaming-based thinking and focus on topology. Most global connectivity ▶

relies on centralised logic, where traffic is often routed through distant hubs regardless of where devices operate.

A network that behaves locally everywhere must be distributed, with control over where data exits the network and how it enters applications. For AI in particular, that local behaviour must extend into the cloud layer, allowing data to move directly into local environments without unnecessary detours.

IoT Now: How do you describe floLIVE's approach to AI-led IoT? What are the main building blocks?

NS: We use a three-pillar framework because AI fundamentally changes what the network needs to do. Traditional networks were designed to connect devices; AI-driven systems require the network to play a more active role.

The first pillar is control and compliance, allowing customers to shape network behaviour so data remains local and aligned with the AI architecture. The second is intelligence inside the network, using AI to improve security, operations and efficiency. The third is data enrichment, using network-level insight to provide AI systems with richer real-world context.

IoT Now: Let's unpack the first pillar. What does it mean, in practical terms, to shape the network for AI?

NS: Practically, it means you stop treating connectivity as one size fits all.

Instead of deploying devices and accepting whatever routing and behaviour you get, you define it. By geography, by device group, by workload. If you need data to stay local for sovereignty, you set it that way. If you need low latency to a specific compute environment, you optimise the route to that destination. If different regions have different requirements, they follow different policies by design.

The point is simple: the network behaves the way your AI system needs it to behave, so performance and compliance are built-in from day one.

IoT Now: Let's move to pillar two. You said this is about using intelligence inside the network. What does that include?

NS: Pillar two is where the network shifts from passive connectivity to an operational layer that helps you run the service. In most IoT deployments, connectivity just transports data and when something breaks you find out late, usually through a ticket.

By applying AI to network signals and events, you can improve two things at scale: security and operations. On security, you can enforce policy and detect anomalies at the network layer, before issues spread. Operationally, you can quickly separate a device fault from a local network condition or a configuration problem, which cuts false alarms and speeds up root-cause.
The network becomes an active operational layer, not just infrastructure you hope behaves.

IoT Now: And the third pillar, as you describe it, is about using the network's intelligence as an input to enterprise operations and AI. What does that mean in practice?

NS: Pillar three is about turning the network into a source of intelligence.

Most enterprises never see what's happening inside the network. With standard connectivity, the network is effectively a black box, providing usage and availability, but little insight into signaling behaviour, performance patterns or real-world operating conditions. Because we operate the network core, we can expose that deeper layer of network intelligence and feed it into customers' own systems and models. For AI teams, this matters because models are only as good as the data they ingest. Network-level insight adds real-world context that application data alone can't provide, transforming the network from a passive pipe into an active data source that strengthens the entire AI value chain.

IoT Now: Can you give a concrete example of how network intelligence translates into business insight?

NS: Take an automotive use case such as ADAS. Under normal conditions, vehicles generate relatively consistent connectivity patterns in terms of volume, destination and protocol usage. If those patterns change, the network can detect it without inspecting the data itself. Once correlated with a known malfunction, the network can flag similar behaviour across the fleet in real-time, enabling earlier intervention and reducing operational and compliance risk.

IoT Now: Finally, what should enterprises do differently this year if they want to scale AI across connected devices successfully?

NS: They should add one line to the checklist early: What is my network plan?

Before deciding on edge or cloud strategies, enterprises need to ensure the network can deliver local performance and local data handling, with compliance supported by design. Getting that right makes everything else easier.

By applying AI to network signals and events, you can improve two things at scale: security and operations

flo. LIVE

www.flolive.net

How Thingsdata scaled up from regional provider to global enabler

Thingsdata is a specialist in global cellular IoT connectivity that delivers a turnkey solution combining hardware, connectivity and data processing. The company's mission is to make complex global IoT connectivity accessible and actionable — helping clients modernise operations, gain real-time insights and scale globally with ease. It turned to mobile virtual network enabler (MVNE) floLIVE to support its needs for seamless international connectivity

Thingsdata supports the entire IoT lifecycle enabling selection and provisioning of devices and sensors, providing multi-network cellular and LPWAN connectivity, and enabling advanced analytics through customisable IoT dashboards. This integrated approach allows organisations across logistics, energy, fintech and other sectors to focus on outcomes, not infrastructure.

Key performance indicators

- 10x increase in SIMs deployed globally
- Triple-digit growth in new customer onboarding
- Significant reduction in connectivity costs through international mobile subscriber identity (IMSI) optimisation
- Achievement of seamless cross-border IoT deployment across 190+ countries ▶

SPONSORED CASE STUDY

The company's mission is to make complex IoT technologies accessible and actionable — helping clients modernise operations, gain real-time insights and scale globally with ease

Address coverage gaps, high costs and operational burdens

As Thingsdata expanded globally, its reliance on several mobile network operators (MNOs) revealed key challenges:

- Coverage gaps outside the EU made it difficult to support global connectivity at a consistent service level.
- Roaming costs and charges for idle SIMs made international rollout financially unsustainable.
- Each MNO operated different platforms, SLAs and support systems — increasing operational complexity for provisioning, diagnostics and support.

"With MNOs, the further you go from the home country, the more expensive it gets," explains Jochem Koppes, the managing director of Thingsdata. "Global roll-out becomes really challenging with a consistent price level and that's what we needed to solve. That's why we looked into MVNEs like floLIVE, to support global connectivity with local pricing through a multi-IMSI setup."

A unified, scalable IoT ecosystem built for global reach

To address these challenges, Thingsdata modernised its infrastructure to enable seamless international performance through a fully integrated platform.

The solution includes:

- Global coverage in 190+ countries with access to multiple networks
- A centralised connectivity management platform (CMP) for SIM provisioning, real-time diagnostics and remote management.
- A multi-IMSI architecture allowing SIMs to switch automatically to the best local network.
- Local packet gateways (PGWs) for low-latency performance and regulatory compliance.
- SLA-backed, 24/7 technical support from telecoms and IoT specialists.

"We are really happy that floLIVE is adopting a lot of new innovations," adds Koppes. "It's a highly technical market, and we really like that floLIVE is on top of all the new developments, picking out the smart ones and then deploying those into the market."

By transitioning to a scalable and globally consistent IoT solution, Thingsdata accelerated international expansion and improved customer outcomes:

- **Global customer growth**
  Achieved rapid growth with 100+ new global customers.
- **Expanded market reach**
  Deployed IoT solutions beyond the EU into North America, South America, Africa and Asia.
- **Improved coverage performance**
  Eliminated coverage blind spots and improved connectivity in hard-to-reach regions.
- **Reduced operational costs**
  Avoided roaming surcharges and eliminated charges for inactive SIMs.
- **Consistent global experience**
  Delivered reliable, high-performance connectivity with automatic IMSI switching and local breakout.

"In the two years that we've had this relationship, we gained a lot of very nice business cases and extremely nice customers that we're rolling out at high volume," says Koppes. "floLIVE has supported us across performance, security and operations helping us and our customers win in their markets."

www.flolive.net
www.thingsdata.com

LionsBot unlocks seamless global connectivity for autonomous robots with floLIVE

The business impact of floLIVE

Reduced deployment complexity
SIMs installed and pre-configured at manufacture

Consistent coverage and reliability
Autonomous switching, even in remote regions

Strengthened operational efficiency
Teams can focus on fleet performance

LionsBot is a global robotics company specialising in autonomous cleaning solutions for large commercial and public environments. Founded in Singapore, the company designs and manufactures intelligent cleaning robots used by facilities management providers, property operators and enterprises to maintain high-traffic spaces such as airports, hospitals, office buildings, shopping centres and industrial sites

LionsBot was looking for a way to install SIM cards directly during robot production and ship devices pre-configured for global use

LionsBot's robots are designed to operate continuously while being managed through a centralised cloud platform, enabling remote monitoring, performance optimisation and proactive maintenance across entire fleets. Today, LionsBot robots are connected via cellular networks and deployed across more than 30 countries worldwide. Deployments range from single buildings to complex, multi-site environments managed by international facilities management companies.

As LionsBot's customer base expanded globally, reliable, always-on cloud connectivity became essential to ensure consistent service delivery, efficient fleet management and scalable operations across diverse geographies. The company was looking for:

SIMs installed at the point of manufacture: LionsBot was looking for a way to install SIM cards directly during robot production and ship devices pre-configured for global use. This would also remove the need for dealers to open robot panels or perform manual, country-specific setup such as access point name (APN) settings, SIM PINs and personal unblocking key (PUK) codes.

Reliable coverage without SIM swaps or downtime: The company needed consistent connectivity across regions, including in remote or low-coverage environments, with the ability to automatically switch networks when performance is poor so deployments would not be delayed by replacing SIM cards or dealing with prolonged connectivity issues. The business also required compliance with GDPR, making local data governance critical.

Always-on cloud access without reliance on customer Wi-Fi: LionsBot wanted a connectivity model that avoided building-specific IT approval processes and coordination with local facility teams, and that was not affected by Wi-Fi blind spots. This would also ensure uninterrupted access to the cloud for monitoring, diagnostics, and fleet management.

"Wi-Fi just wasn't a reliable fallback for us with our commercial buildings," says Mullapudi Sai, the head of the Robot Service Team at LionsBot. "Building-specific IT policies slowed deployment, network blindspots disrupted operations and we rely on significant coordination between facility IT teams and our operators. We needed a better way." ▶

Global, multi-network coverage

LionsBot selected **floLIVE** after evaluating connectivity providers that could support four key drivers:

1. A solution that could be embedded directly into robots, supporting simple SIM installation at the point of manufacturing.
2. The removal of country-specific complexity, providing reliable global coverage across diverse deployment regions.
3. Continuous cloud connectivity to support fleet management and remote diagnostics in real-time.
4. A robust networking infrastructure capable of supporting the continuous evolution of its proprietary AI.

floLIVE was chosen because of its global, multi-network coverage, the reduced installation and configuration efforts, and improved uptime and connectivity reliability. floLIVE delivers a cloud-native solution combining global international mobile subscriber identities (IMSIs), multi-network access and centralised connectivity management, allowing devices to connect seamlessly to local mobile networks anywhere in the world.

By partnering with floLIVE, LionsBot replaced fragmented local SIM management with a single, standardised cellular solution across its global robot fleet.

Key elements of the solution include:

Multi-network connectivity

LionsBot's robots generate significant cellular usage, typically more than 1GB per robot each month, so both reliability and cost control matter at scale. Robots automatically connect to the strongest available network in each location, removing dependency on a single provider and eliminating SIM replacements when coverage is poor, even in remote or challenging environments. With access to 90 networks across more than 30 countries and a multi-IMSI approach, LionsBot can steer traffic to available yet affordable networks in each region, driving significant connectivity cost savings.

Independent cloud access

Consistent cellular connectivity removes the need to integrate robots into customer Wi-Fi networks, avoiding delays caused by local IT security policies and ensuring reliable access for monitoring, diagnostics, and fleet management.

Reduced security and infrastructure dependency

Cellular connectivity avoids direct integration into building IT networks, reducing security concerns and ensuring LionsBot does not depend on the quality or reliability of local infrastructure.

Through its collaboration with floLIVE, LionsBot has significantly improved the efficiency and reliability of its global deployments. Key results include:

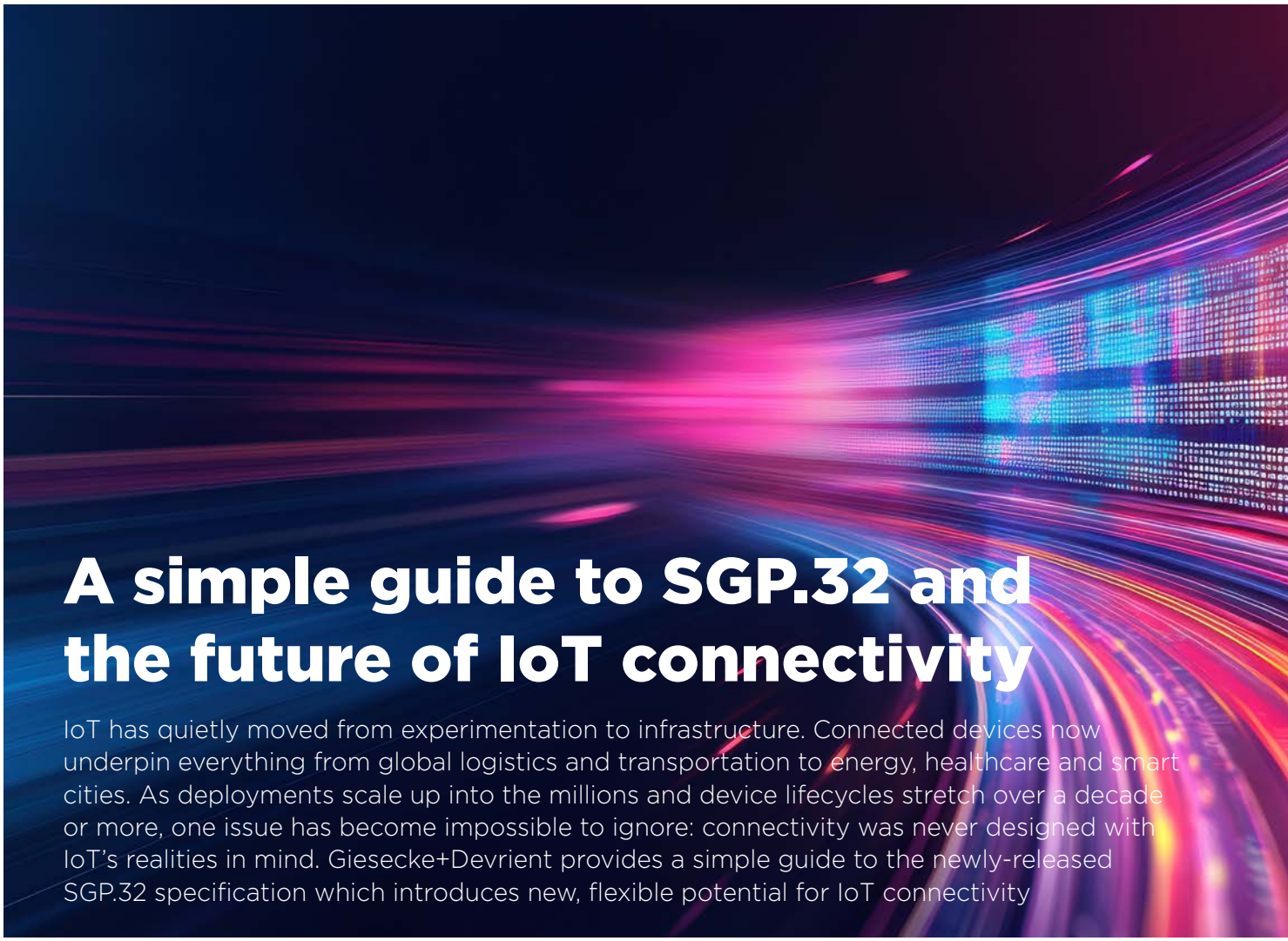
- **Faster, more consistent deployments:** Connectivity issues are no longer a deployment blocker, as robots arrive pre-configured and ready to connect immediately, regardless of country or site.
- **Improved uptime and reliability:** Automatic network switching ensures stable and cost-effective connectivity across regions, even in low-coverage environments.
- **Stronger focus on fleet performance:** With connectivity largely removed as a day-to-day concern, LionsBot and its customers can focus on fleet analytics, performance optimisation and remote troubleshooting instead of basic connectivity management.
- **Connecting the human and the machine:** As well as back-office data collection and software updates, users can utilise floLIVE connectivity to control robots directly from their mobile app, including setting cleaning schedules and troubleshooting issues, giving ultimate control.

Together, the result is a connectivity layer that is simple to deploy, globally consistent and designed for scale, giving LionsBot a foundation to support growing multi-country deployments without increasing operational complexity. This foundation will support future initiatives including advanced fleet analytics, faster remote diagnostics and reduced downtime across the global robot fleet.

"Day-to-day operations are now far smoother," confirms Sai. "Connectivity-related incidents are significantly reduced, as floLIVE provides strong network availability with at least two IMSIs and two networks in all our operating regions. This allows us and our customers to focus on fleet performance, usage insights and remote troubleshooting, rather than basic connectivity issues."

floLIVE was chosen because of its global, multi-network coverage, the reduced installation and configuration efforts, and improved uptime and connectivity reliability

www.flolive.net
www.lionsbot.com



A simple guide to SGP.32 and the future of IoT connectivity

IoT has quietly moved from experimentation to infrastructure. Connected devices now underpin everything from global logistics and transportation to energy, healthcare and smart cities. As deployments scale up into the millions and device lifecycles stretch over a decade or more, one issue has become impossible to ignore: connectivity was never designed with IoT's realities in mind. Giesecke+Devrient provides a simple guide to the newly-released SGP.32 specification which introduces new, flexible potential for IoT connectivity

Traditional IoT SIM cards are typically provisioned with a single network profile before deployment

For years, the industry has tried to adapt traditional SIM technology to fit IoT use cases. While this approach enabled early growth, it has also introduced hidden costs, operational rigidity and long-term risk. SGP.32, the latest eSIM standard from the **GSMA**, represents a fundamental rethink of how cellular connectivity should work for IoT. Rather than being a marginal technical upgrade, it signals a shift towards a more flexible, resilient and future-proof IoT ecosystem.

The connectivity problem hiding in plain sight

Connectivity problems are often overlooked in IoT. Devices connect to cellular networks, data flows to platforms and applications deliver insights. In practice, however, connectivity decisions made at deployment can constrain an IoT solution for its entire lifetime.

Traditional IoT SIM cards are typically provisioned with a single network profile before deployment. Once the device is installed — whether on a vehicle, container, utility meter or piece of industrial equipment — changing that connectivity can be expensive or even impossible. For globally deployed devices, this often leads to complex logistics, costly on-site maintenance visits or the need to over-engineer connectivity contracts upfront in anticipation of unknown future needs.

Vendor lock-in compounds the issue. When connectivity is tightly coupled to a single operator or provider, businesses lose negotiating power and flexibility. Coverage gaps, pricing changes, regulatory shifts or service degradation can all become strategic risks over long device lifecycles. As IoT deployments scale, these constraints directly impact total cost of ownership and operational resilience.

Why earlier eSIM standards fell short for IoT

Embedded SIM (eSIM) technology has been around for a while. The M2M eSIM standard, SGP.02, found early success in automotive use ▶

SPONSORED ARTICLE

cases. It proved that remote SIM management could work with large device fleets, but the cost of integrating new mobile network operators and the reliance on SMS for provisioning and management made this a barrier to wider adoption.

On the other hand, consumer eSIM models assume the presence of a user interface, regular human interaction and relatively short device lifecycles. IoT devices, by contrast, often operate unattended, with limited processing power, constrained energy budgets and lifespans measured in years or even decades. Many are deployed in remote or inaccessible locations, where physical intervention is costly or impractical.

As a result, earlier eSIM implementations in IoT added complexity without fully solving the underlying problem. What the industry needed was a purpose-built standard, one that treated remote connectivity management as a core requirement rather than an adaptation. That's where SGP.32 comes in.

What is SGP.32, in simple terms?

SGP.32 is an eSIM standard defined by the GSMA specifically for IoT deployments. At its most basic level, it allows IoT devices to securely download, activate and switch cellular connectivity profiles over the air, without requiring costly physical SIM changes or user interaction.

The key difference lies in how SGP.32 is designed around IoT realities. It supports devices with no screens, no keyboards, minimal power availability and long operational lifetimes. Connectivity can be managed remotely at scale, across fleets of devices, using lightweight and efficient processes. In practical terms, SGP.32 separates the device hardware from a fixed connectivity decision. Devices can be manufactured, deployed and operated without being permanently tied to a single network or operator. Connectivity becomes a flexible resource that can evolve alongside the business and its operational needs.

How SGP.32 works behind the scenes

SGP.32-enabled SIMs can store and manage multiple connectivity profiles. Using a centralised remote SIM management system, operators can download new profiles to devices over the air. These profiles can then be activated, deactivated or replaced as needed, without physical access to the device. The process is designed to be efficient and secure, even for devices operating on low bandwidth or intermittent connections.

Once a profile is active, the device behaves like any other cellular-connected endpoint. The difference is that if coverage, pricing, regulatory requirements or business priorities change, connectivity can be updated remotely. This decoupling of hardware and connectivity is what makes SGP.32 such a powerful enabler for long-term IoT scalability.

However, to fully understand why SGP.32 matters, it is important to introduce other concepts that are often overlooked: the eIM and the IPA.

eIM: The invisible engine behind SGP.32

The eIM, or eSIM IoT Manager, is the operational layer that makes SGP.32 usable at scale. While SGP.32 defines how eSIM profiles can be securely provisioned and managed for IoT devices, the eIM defines who manages them and how those processes are orchestrated across large device fleets. In simple terms, if SGP.32 is the standard, the eIM is the system that brings that standard to life.

The eIM operates entirely in the background, acting as the central control plane for IoT connectivity. It manages the lifecycle of eSIM profiles on devices, handling tasks such as initial bootstrap connectivity, profile downloads, activations, deactivations and switching between operators. Crucially, it is designed for IoT-scale ▶

SGP.32-enabled SIMs can store and manage multiple connectivity profiles

SGP.32 is often described as a technical standard, but its real impact is felt at a business level

operations, where thousands or millions of devices may need to be managed with minimal human intervention. This makes the eIM essential for unattended, low-power and long-lived IoT deployments.

With SGP.32 and the eIM working together, connectivity becomes a software-controlled resource. Decisions about which network to use, when to switch or how to optimise coverage can be made throughout the device lifecycle, not just at the moment of deployment.

IPA: The hands-on assistant on your device

The IoT profile assistant (IPA) is a small software programme that helps IoT devices manage the SIM securely. It acts as a middleman, making sure the device can safely communicate with the eIM and carry out tasks like downloading new IoT profiles.

There are two ways the IPA can be set up, according to SGP.32:

1. IPAd – IPA on the device

- Runs directly on the device's operating system.
- Gives device manufacturers more control over how the IPA works.
- Requires the device manufacturer to handle testing and certification, which can take more effort.

2. IPAe – IPA inside the SIM

- Integrated with the SIM operating system.
- Often comes pre-certified, reducing the manufacturer's work.
- Can speed up product development and time-to-market.

The key difference between the IPA and the eIM is where they operate and what they control. The IPA runs on the device or SIM and acts as a local assistant, executing commands and managing profiles directly on the device.

In contrast, the eIM lives in the cloud or network and serves as the central manager, sending commands and controlling the lifecycle of embedded universal integrated circuit cards (eUICCs). Essentially, the eIM is the 'boss' giving instructions, while the IPA is the 'assistant' carrying them out on the device. Both elements are the core enablers of SGP.32.

Benefits of SGP.32 for your business

SGP.32 is often described as a technical standard, but its real impact is felt at a business level. By changing how connectivity is managed over the lifetime of an IoT deployment, it delivers clearer control, lower risk and greater flexibility.

1. Connectivity that adapts as your business grows

With SGP.32, connectivity can evolve alongside the business. Devices operating across different regions can use the most appropriate local network without requiring new hardware variants or complex SIM logistics. When fleets expand into new countries or markets, existing devices can be adapted remotely rather than replaced.

This makes global growth simpler and faster, while avoiding the operational overhead traditionally associated with multi-country IoT deployments.

2. Lower operational costs and simpler fleet management

One of the most immediate benefits of SGP.32 is the removal of physical SIM handling. There is no need for SIM swaps, on-site visits or device recalls simply to change connectivity. This significantly reduces operational costs, minimises downtime and simplifies the management of large device fleets. For devices deployed in remote or hard-to-access locations, this benefit alone can have a major impact on total cost of ownership.

In addition, SGP.32 profiles are designed to be more readily integrated across operators and platforms, without the need for significant custom integration effort. This lowers the commercial and technical barrier to onboarding new connectivity providers, further reducing costs and improving flexibility over the lifetime of a deployment. ▶

3. Reduced vendor lock-in and stronger negotiating power

SGP.32 gives organisations greater independence from individual network operators or connectivity providers. Because profiles can be changed over the air, businesses are not locked into a single provider for the full lifetime of a device.

This flexibility allows organisations to renegotiate contracts, introduce redundancy or switch providers as coverage, pricing or service quality changes. Over long device lifecycles, this can translate into meaningful cost savings and improved resilience.

4. Future-proofing against regulatory and market change

Regulatory requirements around roaming, data residency and certification continue to evolve globally. SGP.32 provides a practical way to respond to these changes without disrupting deployed assets.

Instead of redesigning hardware or managing complex logistics, organisations can adapt connectivity remotely. This future-proofing is particularly valuable for IoT deployments expected to remain in service for many years.

Use cases where SGP.32 makes a tangible difference

The benefits of SGP.32 become most apparent in deployments where scale, mobility and longevity are critical. In automotive and telematics, vehicles routinely cross borders and operate in diverse network environments. SGP.32 enables seamless connectivity transitions without manual intervention, supporting applications such as real-time diagnostics, fleet optimisation and predictive maintenance.

Asset tracking and logistics provide another clear example. Containers, pallets and high-value equipment often move across regions and operators. With SGP.32, connectivity can follow the asset rather than being constrained by its original deployment location.

Industrial IoT and smart infrastructure deployments also stand to benefit. Devices monitoring utilities, environmental conditions or critical infrastructure may remain in place for decades. SGP.32 ensures that connectivity can evolve alongside technology roadmaps, business models and regulatory frameworks.

A foundation, not a feature

It is tempting to view SGP.32 as a feature of connectivity platforms or devices. In reality, it functions more like a foundational infrastructure. Much like how cloud computing simplifies hardware design for developers, SGP.32 removes connectivity constraints from IoT solution design.

This shift allows organisations to focus on data, insights and outcomes rather than the mechanics of keeping devices online. It also encourages healthier ecosystems, where hardware manufacturers, connectivity providers and application developers can innovate without forcing long-term lock-in.

Looking ahead: SGP.32 and the future of IoT

The purpose-built approach of SGP.32 reflects a broader industry shift towards treating connectivity as a lifecycle capability rather than a one-time configuration choice. From the beginning of 2026, this shift becomes fully tangible. Until now, **Giesecke+Devrient**'s (G+D) SIM hardware and management platforms were SGP.32-ready. Now, so is G+D's connectivity service, meaning all layers of our IoT connectivity stack are now aligned to the same GSMA standard.

This means that eSIM hardware, platforms and connectivity are now all natively built around SGP.32. Rather than operating a mixed or transitional setup, device makers and solution providers can work with a fully SGP.32-native IoT connectivity stack from end-to-end. And what's more, we own every layer of that stack, rather than being assembled from multiple vendors. This end-to-end ownership creates a more reliable and predictable foundation for customers, with fewer integration challenges, more consistent behaviour across the stack and clear accountability throughout the entire connectivity lifecycle.

It also enables a more flexible engagement model. Device makers can work with a single provider across the stack, selecting only the elements they need, while benefiting from consistent architecture and interfaces. Support for both IPAd and IPAe further extends SGP.32 connectivity to a broader range of devices, including more constrained IoT use cases. In addition, the IPAe is capability aware, so if a device enabled with IPAd is used now, or upgraded in the future, the IPAe disables itself. The solution is future-proofed.

Taken together, this marks an important step in the evolution of IoT connectivity. By aligning hardware, platforms, and connectivity around SGP.32, the industry moves closer to a future where connectivity is simpler to manage, easier to scale and better suited to the realities of long-lived, globally deployed IoT solutions. It also reinforces G+D's position as a specialised IoT MVNO focused on next-generation eSIM connectivity, built around standards that are designed for what IoT has become and where it is heading next.

This shift allows organisations to focus on data, insights and outcomes rather than the mechanics of keeping devices online

www.gi-de.com

Kaleido Intelligence

Mobilesquared
Decision ready data

NEW 2026 CONNECTIVITY DATA HUB UPDATE

Historical & Market Forecast Connectivity Database Covering 60+ Markets

New Key Findings

- Transport, Energy & Utilities, Smart Cities, Healthcare & Manufacturing use cases to account for **57%** of total connections by 2030
- **25%** of eSIM profiles for IoT will be deployed using the SGP.32 specification in 2029
- **146 million** connections across smart phones & IoT devices for direct-to-satellite (D2D, NTN) connectivity in 2030
- **11%** CAGR for cellular IoT with global connections reaching over 6.5 billion in 2030

Access the Full Report to **Inform Your 2026 Strategy**

✓ 500,000+ datapoints across the global cellular IoT market
✓ Accurately measure current & future market size
✓ Identify key growth areas across detailed segments & IoT verticals

kaleidointelligence.com

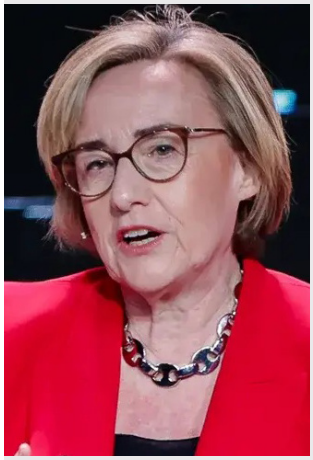
Movers and shakers are promising key tech progress at MWC26 Barcelona

Mobile World Congress Barcelona is back at the Fira de Barcelona Gran Via on 2-5 March, and this year is the 20th annual expo and conference in the city. The week-long gathering will attract global leaders, innovators and policymakers to explore the future of mobile and digital transformation, reports Antony Savvas

CEOs and leaders from the breadth of the global mobile and technology ecosystem and beyond are set to take to MWC stages, with keynotes from the likes of **AT&T** CEO John Stankey, **BT Group** CEO Allison Kirkby, **China Mobile** CEO He Biao, **Deutsche Telekom** CEO Tim Höttges, **Lumen** CEO Kate Johnson, **Nokia** CEO Justin Hotard, **NTT** CEO Akira Shimada, **Orange Group** CEO Christel Heydemann, **Qualcomm** CEO Cristiano Amon, and **Vodafone** CEO Margherita Della Valle, among the hundreds of speakers taking part across the event.

56% of attendees represented industries adjacent to the core mobile ecosystem, 21% were C-suite attendees and 50% were director level and above

Allison Kirkby
BT Group



Margherita Della Valle
Vodafone

Dimitra Simeonidou
JOINER

Show numbers

To illustrate the scale of the show, regarded as Europe's largest annual technology event, last year's conference and expo attracted 109,000 attendees from 205 countries and territories, and there were over 2,900 exhibitors, sponsors and partners. There were more than 1,200 speakers and thought leaders, and the **GSMA** Ministerial Programme convened 188 delegations from 148 countries, 40 intergovernmental organisations, 66 ministers and 111 heads of regulatory authorities.

The 4YFN startup event welcomed over 1,000 exhibitors, nearly 380 speakers and over 900 investors with collective funds totalling €60 billion.

56% of attendees represented industries adjacent to the core mobile ecosystem, 21% were C-suite attendees and 50% were director level and above. Over 2,900 journalists and industry analysts were in attendance.

John Hoffman, CEO of GSMA, the show organiser, says: "As March approaches, I'm excited to see the industry come together again in Barcelona for what promises to be another exciting edition of MWC – our 20th in Barcelona. From Airport of the Future to our New Frontiers zone, there are so many exciting new elements to explore this year. These exhibits, experiences and technologies on-site truly capture the core purpose of MWC Barcelona – real-world innovations showcasing how we will live in the future being deployed, tested and scaled to improve our lives in meaningful ways."

Airport of the Future

The debut Airport of the Future experience will bring large-scale aviation innovation directly into the halls of MWC. Built around real world use cases and operational environments, the immersive exhibit will feature a live, full-scale motional digital twin delivered by **Outsight**, the first time the technology has been deployed at a technology event in a live, real-scale setting. Using the exhibition area as a test bed, attendees will see how airports can anonymously track passenger movement, manage queues, optimise asset use and improve operational performance in real-time.

New Frontiers

Another show debut this year is New Frontiers, an immersive, future-focused showcase exploring the outer limits of innovation. Featuring around 20 exhibitors from across the world, many appearing at MWC for the first time, the exhibition brings together "mind-expanding ideas poised to profoundly impact connectivity, industry and society", says GSMA. This will include quantum leaders **Global Data Quantum** and the **Quantum Flagship**, technology, satellite and non-terrestrial network (NTN) pioneers the **European Space Agency**, **Eutelsat** and **Viasat**, and AI humanoid leader **MagicLab Robotics**.

High-speed driving

The GSMA Pavilion will showcase the power of networks and cross-industry collaboration, with experiences including a simulator featuring the speed and precision of **Formula E**. And **NUHS**, in collaboration with **Ericsson** and **Singtel**, will showcase the future of AI and 5G-powered patient care, from an intelligent robot nurse to holographical surgical planning. In addition, **Elmo**'s tele-driving service returns, so attendees can drive a car around the Circuit de Catalunya, by steering it from the MWC showfloor. Also, **Capgemini** will showcase a smart factory in action, with a vision-guided robotic arm, whilst **Infobip** will challenge attendees to build and direct a team of AI agents to stop banking fraud.

AI

Like many attendees, Tiago Rodrigues, president and CEO of the **Wireless Broadband Alliance** (WBA), is looking forward to the AI debates in Barcelona. "One of the key discussions I foresee for MWC is how do we make connectivity feel effortless and trustworthy in an AI era where everything depends on the network," he says. "That means intelligent infrastructure, automation in network operations, and a big push towards exposing network capabilities through standardised APIs."

"For WBA, the most practical expression of that is seamless convergence between cellular and Wi-Fi," Rodrigues adds. "OpenRoaming is moving fast because it solves a problem users and enterprises ▶

Businesses want to know exactly where their data is stored, who can access it, and which laws apply, particularly as AI becomes part of day-to-day operations

face to authenticate once, connect securely everywhere and move between networks without friction. At MWC we'll be focused on scaling that ecosystem, and how AI/ML can reduce operational burdens, while raising the security level, and what's next as Wi-Fi 8 innovation comes into view."

Hriday Ravindranath, the chief digital and information officer at **Orange Business**, says: "The topic of conversation is changing from connectivity to control. AI systems and autonomous agents are starting to generate more network traffic than people, which means networks need to be designed, secured and operated very differently."

"Data sovereignty will be a big part of that discussion," he adds. "Businesses want to know exactly where their data is stored, who can access it, and which laws apply, particularly as AI becomes part of day-to-day operations. This is driving interest in private 5G, especially in manufacturing, healthcare and smart cities, where reliability, security and trust really matter."

As enterprises roll out AI across connected devices, attention often focuses on value, use cases, governance, deployment and compliance. Yet many organisations overlook a more fundamental dependency. If the network cannot deliver the required coverage, performance, intelligent routing, local behaviour and sovereign data handling, AI workloads will struggle to scale.

Nir Shalom, CEO of **floLIVE**, argues the most overlooked question in AI-led IoT is also the simplest: what is your network plan? "Enterprise leaders I speak with are primarily asking how to generate real business value from AI across connected devices. Once they identify the opportunity, their focus shifts to architectural questions: should intelligence sit at the edge or in the cloud, how does data gravity influence deployment, and how do they manage complexity while balancing security, data sovereignty and cost."

"The question I rarely hear early enough, but believe is essential, is 'what should the network look like to support this AI strategy'?" Shalom explains. "Global AI deployments, network topology, latency, sovereignty and control become foundational constraints that must be designed intentionally from the start. A deliberate network plan is required to ensure that the network topology supports data gravity needs, otherwise the benefits of local storage are lost to high latency and poor routing."

floLIVE is based on a purpose-built global cellular network for devices, but is "hyperlocal" in operation, connecting devices locally across regions worldwide. "This approach eliminates common challenges such as data sovereignty risks and high latency, while still providing enterprises with a unified, global view of all their connected assets," says Shalom.

Amanda Brock, CEO of **OpenUK**, says AI will be affecting the debates across multiple conversations in Barcelona. "Open source is finally being discussed at an informed and broader level, thanks to AI. GSMA and others are holding sessions on it, although they are broader than open source, and looking at the full gambit, including open standards, open models and hardware."

She adds: "I've always been told that the even numbers are the important iterations. For 6G, we are seeing software main stage, as opposed to the bit part it's played in the past. Networks are being defined by it, which ultimately means they are open source today. This shifts the conversation significantly, although there is still the challenge of the interface between closed standards with SEPs – even FRAND standards – and open source licensing."

Brock says: "I've been hearing representatives of **ETSI** and other standards organisations recognising they are way too slow to develop and iterate, that the software influence is demonstrating the need for them to shift to a much greater pace, and that for their survival, standards bodies need to evolve, including a shift in their business models and revenue streams. This needs to be more workable with open source, allowing a free flow of innovation, if they want to make the standards of the future."

"Barcelona will buzz with the potential productivity enhancements AI offers," ▶

Amanda Brock
OpenUK

Tiago Rodrigues
World Broadband Forum

Nir Shalom
floLIVE

she predicts. "But the real conversation is going to be the meat of how AI infrastructure can be used for 6G, and inevitably this will be framed in diversification of mobile infrastructure and sovereignty concerns."

On AI, Parm Sandhu, vice president of enterprise for 5G products and services at **NTT DATA**, says: "The biggest theme will be the shift in IoT from basic data collection and dashboarding to data inferencing, with edge AI with physical AI driving real operational outcomes. The conversation is moving beyond 'collect and visualise' toward using physical AI to interpret what's happening in real-time and to recommend or automate decisions that improve productivity, quality and throughput. A second major theme is automation and remote operation enabled by low-latency connectivity, private 5G, edge computing and physical AI, with strong focus areas like smart aviation and smart mobility."

AI will also feed into the interconnectivity debate. Sam Jackman, chief development officer of **Shared Access**, a provider of mobile connectivity solutions, says: "It is likely that data centres will be a high priority at MWC, with a focus around locations and the connections between data centres, as edge usage of AI increases through smartphones, thus potentially changing the data centre model."

Techcos?

Over the last few years, telcos have been urged to extend their offer from mainly connectivity to offering more services through digital transformation, and basically converting from a telco to a 'techco'. It's a subject that has been prevalent at MWC in the past. So is this happening?

"Telcos are increasingly acting as the front door for digital life. While they used to simply sell connectivity, these businesses are now becoming hubs that manage and monetise entire ecosystems of digital services and subscriptions," said Giles Tongue, the vice president of marketing at **Bango**. "Consumer demand is accelerating this shift. Our research shows people increasingly expect their mobile plans to come bundled with services such as AI, subscription video on demand, gaming and music streaming by default."

"To deliver on this, telcos are committing significant investment into a diversified consumer experience," he adds. "This drives retention. The more services a customer takes, the higher the net promoter score and the higher the loyalty. It also helps to provide clear differentiation against competition, from each other, and increasingly from MVNOs and even Fintech companies." ▶

Technical advances in play include deploying multi-agent systems (MAS) to redefine customer interaction and targeting next-level network autonomy

Dimitra Simeonidou of **JOINER** (Joint Open Infrastructure for Networks Research), the international next generation telecoms innovation platform across 14 universities, says the techco label isn't the most important thing: "Telcos won't stop being telcos, and that's the point. Next-gen networks must be AI-native and secure by design to optimise operations, unlock network data responsibly and expose new APIs and services. But telecoms also plays a strategic role in powering AI itself: connectivity is the fabric that interconnects data centres, edge compute and emerging supercomputer facilities, including major investments now being committed in the UK and around the world."

"In that sense, AI is a once-in-a-generation opportunity: it's not just another application layer, it's reshaping what networks are and how they create value," says Simeonidou.

Jaime Gonzalez, chief marketing officer at **MedUX**, adds: "Becoming a techco isn't about branding. It's about speed and product thinking. Telcos earn the label when they can rapidly design, launch and support services beyond connectivity, with developer-ready APIs, partner ecosystems and clear commercial models, exactly what initiatives like the GSMA Open Gateway and CAMARA are trying to industrialise."

"But the second half is delivery: those products need predictable quality and enforceable SLAs, and internally operators must unify data, processes and automation to make decisions faster, moving up the autonomous operations curve," adds Gonzalez. "This is where real experience evidence helps keep the techco promise honest."

Hanen Garcia, chief architect for telecoms in the CTO Office at **Red Hat**, says: "The core business goal remains to reverse commoditisation by prioritising intelligence over pure infrastructure. Service providers around the world are highly focused on consolidating legacy and modern applications onto a single, common cloud-native platform. This forms a large part of our collaboration with telcos to help reduce costs, increase hardware utilisation and improve scalability across IT, the core network and the edge."

"Technical advances in play include deploying multi-agent systems (MAS) to redefine customer interaction and targeting next-level network autonomy," adds Garcia. "On the organisational side, the transformation to techco requires upskilling workforces in AI, especially to manage human-in-the-loop governance for agentic systems, and transitioning from legacy operational models to cloud-optimised innovation. As ever in the telco world, some are further ahead than others, and this is what will give them a competitive edge."

Private 5G progress?

After 5G was introduced, a big market that was expected for the technology was private 5G networks that could be used to operate factories, drive transport and logistics, and to power communications in data sensitive environments like healthcare, among other use cases. This market was initially a slow-burning one, so have things changed?

"Absolutely. In relevant industries, private 5G is already supporting automation, real-time monitoring and safer operations, from tracking assets to supporting autonomous systems and technicians in the field," says Orange Business's Ravindranath. "Because private 5G offers low latency, strong reliability and greater control, it works well where traditional networks fall short. Early adoption could be complex, but that is changing as the market matures. For organisations that need performance and control over their data, private 5G is now the practical choice."

Red Hat's Garcia says: "Private 5G is part of the enterprise opportunity. However, the bigger focus for service providers at the moment is building and expanding AI factories, making the most of their infrastructure experience to serve governments and enterprises with sovereign AI and cloud solutions. These include GPU and model-as-a-service offerings, providing large-scale AI model training and inference while ensuring data remains within specific jurisdictions to meet growing demands for security and compliance. Red Hat is currently in collaboration with multiple service providers to help them execute their AI factory strategies with a flexible, scalable underlying platform to support any model on any hardware across any cloud."

JOINER's Simeonidou adds: "Private 5G is moving from promising pilots to repeatable value, especially where organisations need guaranteed performance, tighter control and stronger security. The benefits are well understood: better traffic management, predictable latency, improved resilience and data sovereignty. Sectors like manufacturing, transport, health and social care stand to gain significantly. The key now is reducing friction, with simpler procurement, clearer ROI models and better integration with IT/OT systems. As adoption grows, we'll see private 5G mature into a dependable platform and a stepping stone towards the next wave of advanced connectivity technologies."

Mobile World Congress Barcelona takes place at the Fira de Barcelona Gran Via on 2-5 March, 2026.

www.mwcbarcelona.com

How single-pane-of-glass techniques can de-risk SGP.32 eSIM adoption

The GSM Association's SGP.32 standard is a major advance for cellular IoT, enabling remote provisioning and management of eSIMs, writes Jim Morrish, a founding partner of Transfoma Insights. The specification supports secure over-the-air profile downloads and updates without human intervention and is designed to support large-scale cellular IoT deployments. SGP.32 simplifies logistics, improves scalability and enables flexible communications service provider (CSP) switching, allowing organisations to move connections between carriers for cost or performance reasons, or to connect to private networks, and even temporarily to support tasks like firmware updates

Most end-users and connectivity service providers that adopt SGP.32 will already operate legacy fleets of cellular devices that will remain in service for years. Introducing SGP.32-managed embedded SIM (eSIM) devices into such environments can increase fragmentation in the short term, creating disconnected systems, duplicated efforts, inconsistent data, higher costs and security weaknesses.

To avoid these potential downsides, organisations should seek to adopt SGP.32 eSIM technologies in a way that does not increase fragmentation. In this article we explore how single pane of glass (SPoG) platforms can potentially be a key tool for de-risking such a development.

A lesson from the past

Historically, cellular operators typically selected a single preferred connectivity management platform (CMP) to support new IoT connections efficiently, helping to reduce costs and simplify operations. This single-sourcing approach encouraged IoT-focused operator alliances that shared the same CMP, creating a degree of device and solution homogeneity across regions and strengthening customer lock-in through platform dependency.

More recently, operators have shifted towards integrating multiple CMPs to meet increasingly diverse requirements. However, CMPs from different vendors are not seamlessly interoperable, as each has unique interfaces and roadmaps shaped by specific client and strategic priorities. This fragmentation increases costs, limits flexibility and complicates technology adoption.

To address this, CMP-focused SPoG platforms have emerged, providing a unified interface across multiple CMPs and reducing vendor lock-in while restoring operational homogeneity. Examples include **Vodafone** and **AT&T** adopting **Simetric**'s SPoG to enable management of customers' IoT estates from a variety of network partners and **SingTel** and **T-Mobile** establishing similar arrangements with **floLIVE** and **IoTM**, respectively.

A similar dynamic is now unfolding with eSIM adoption under the SGP.32 standard. eSIM management stacks from different eSIM remote manager (eIM) vendors vary significantly, currently including in the development of device-initiated actions, processes for connectivity outage management and connection optimisation, access point name (APN) handling, and approaches to adopting evolving standards. As in the case of CMPs, this diversity is likely to persist as eIM vendors seek to differentiate through value-added services.

Given these realities, SPoGs that currently abstract across multiple CMPs should evolve to also include abstraction of eSIM management, enabling users to access multiple eIM providers through a single interface.

Deploying a SPoG

Most organisations adopting SGP.32-enabled eSIM solutions will already operate large estates of traditional SIM-connected devices and possibly pre-SGP.32 eSIMs. Accordingly, adopting a SPoG for SGP.32 eSIMs can itself create a new form of fragmentation if legacy devices remain managed separately. Best practice is therefore to ensure that the SPoG interface provides a unified view across both SGP.32 eSIM and legacy SIM and eSIM connections.

An intuitive but relatively high-risk approach would be to deploy SGP.32 eSIM whilst at the same time deploying a SPoG to also encompass legacy connections, essentially as isolated projects with the intention that the estates will eventually align. However, this approach can carry over existing operational and technical debt from legacy estates into new deployments.

A better strategy is sequential deployment, implementing SPoG first to gain full visibility into the brownfield estate. With this approach the first step is to improve estate hygiene, including the identification and remediation of dead devices, security gaps, incorrect SIM associations, metadata misalignments, for example, international mobile equipment identity (IMEI) vs embedded identity document (EID), firmware drift and other issues. Once workflows and control parameters are validated, SGP.32 eSIMs can be introduced more seamlessly into the existing estate, extending established processes to new devices. ▶

This sequence prevents increased fragmentation with the introduction of SGP.32 eSIM and, in fact, often reduces it, improving fault resolution, analytics and governance. It also minimises testing for SGP.32 eSIM roll-out by using already validated workflows to as great an extent as possible, ensuring smoother, scalable adoption.

Catering for a brownfield future

As discussed, the introduction of SGP.32 devices is generally not a pure greenfield deployment but more often is the integration of a new estate into an existing brownfield environment. But beyond this, today's greenfield will become tomorrow's brownfield as technology and connectivity options evolve for future device deployments, meaning device estate fragmentation is inevitable and a long-term feature. As such, any organisation deploying SGP.32 eSIM solutions should expect to manage a fragmented device estate most likely from day one and continuously thereafter.

Managing all devices in a unified way should however remain a priority. The emergence of AI, and particularly agentic AI, underlines the need for unified management, as whole-estate device and performance data enables more effective device and network optimisation and agentic functionality. Again, this is an area in which SPoG interfaces can help to de-risk SGP.32 eSIM adoption and ongoing estate management.

Introducing the role of eSIM orchestration

When deploying SGP.32 for eSIM, it is important to differentiate between eSIM management and eSIM orchestration. While eSIM management covers the basics of eSIM updating, including provisioning, activation and updating SIM profiles, eSIM orchestration goes further by integrating device and process management across large estates.

eSIM management focuses on subscription-level actions and maintaining secure, compliant profiles, while eSIM orchestration centralises control through platforms that coordinate workflows across subscription managers, profile managers and device endpoints. For example, eSIM management processes might update credentials when a device enters a new country, whereas eSIM orchestration ensures the device has the connectivity needed to support the update and ensures that the update aligns with the correct carrier and rate plan.

Investing to achieve eSIM orchestration is particularly valuable for massive IoT deployments and should aim to encompass uniform management of both legacy SIM and newer eSIM devices. Ultimately, eSIM orchestration should enable automated and agentic scalable workflows that enhance operational efficiency across legacy and new devices.

Beyond this, some key aspects of eSIM orchestration require new capabilities. For example, traditional SIM management approaches treated connections as unique identifiers (UIDs) for devices, but eSIMs break this association, requiring a new auditable device UID that persists across eSIM configurations and networks and supports continuity of device records. This is becoming an increasingly important aspect of IoT device estate management as cybersecurity, and other, regulations ratchet up around the world.

There is also a need for robust connection migration processes and post-migration testing. Battery-aware management is another new requirement, as eSIM updates and migrations must consider power constraints and device lifetime. Multi-eSIM and hybrid SIM/eSIM devices will add further complexity.

The key here is a concept of operational readiness. Clearly, eSIM management techniques allow for control of devices equipped with eSIMs, but it is only when processes associated with eSIM extend to also include orchestration that end-users can be confident that their eSIM solutions are operationally ready.

Again, eSIM orchestration is best configured and deployed in a way that is homogenous across a mixed device estate and supported with a SPoG interface, rather than fragmented to match a patchwork of SIM types, connectivity service providers, eIMs and CMPs.

Organisational changes required in organisations that adopt SGP.32

Historically, cellular connectivity for IoT devices was treated as a fixed, unavoidable cost and simply an enabler, while value was seen as residing solely in the device and its associated applications. However, IoT solutions are increasingly central to an organisations' core propositions, placing greater emphasis on resilience, integrity and security.

As IoT becomes integral to key business processes, connectivity is shifting from a niche procurement task to become a strategic IT-managed capability. Connectivity decisions influence device behaviour (including battery life, responsiveness and reliability) so these aspects should also be considered in addition to simple direct costs.

SGP.32 eSIM technology introduces significant flexibility here, allowing connectivity providers to be changed seamlessly after deployment. This enables organisations to optimise costs, quality of service or device performance flexibly during a device lifecycle and at different lifecycle stages, such as during large firmware updates.

Consequently, SGP.32 enabled eSIM shifts the responsibility for connectivity planning upstream into product management functions. With persistent UIDs, it also enables devices to be managed as assets within workflows rather than simply as connections. This supports better lifecycle security updates and security audit, an increasingly critical aspect of IoT which has become a focus of regulators around the world. Persistent device UIDs also help to streamline user and access management and facilitate integration into financial and governance systems and also workflow automation platforms such as **ServiceNow**.

However, fragmented eIM markets and varied vendor SGP.32 stacks create risks when developing solutions with specific partners, which may later prove incompatible with new markets or requirements. Again, SPoG platforms can potentially help here, abstracting across eIMs and CMPs so that product managers can design and test solutions once while ensuring broad provider support.

Accordingly, the advent of SGP.32 enabled eSIM drives both the adoption of SPoG approaches and a re-orientation of the connectivity industry towards the needs of the end-user, becoming enterprise first and device centric. Increasingly, connected device estate requirements will be driven by end-user adopter CIO and CISO needs, rather than least-cost procurement.

Significant potential, but execution is critical

SGP.32 represents a significant step forward for cellular IoT, delivering flexibility, scalability and lifecycle control through remote eSIM management. However, without careful implementation, its introduction risks increasing operational fragmentation within existing device estates. A unified approach centred on SPoG platforms and eSIM orchestration enables organisations to integrate new and legacy devices under consistent workflows, reducing complexity while improving governance, security and operational efficiency. By prioritising visibility, estate hygiene and organisational alignment before large-scale eSIM deployment, organisations can realise the full benefits of SGP.32 while future-proofing their IoT strategies against inevitable technological and vendor diversity. With these changes, increasingly markets for cellular connectivity will pivot towards enterprise needs such as seamless enablement for security and workflow automation. ■

www.transformainsights.com

Three questions for your connectivity provider – and three answers for you

You're deploying an IoT project. You're heading into your first conversation with a connectivity provider. If you attended Onomondo's Asset Tracking Virtual Summit 2025, it's unlikely that you will pick up the old playbook – jumping straight into the pricing discussion, writes Jacob Jagger, the head of Information Security at Onomondo. But if you missed it and your first question to a prospective connectivity provider is 'what's the price', it's time to close this playbook – and throw it away because your bottom line depends on it

A PLMN list, often hardcoded into the SIM, dictates the networks your device connects to

The world of IoT and real world data collection has changed, and so must the network that supports it. The demand for always-on coverage is rising fast, with global IoT connections projected to hit 30 billion by 2030 by **Transforma Insights**. All this real-time data is feeding operational AI initiatives with massive efficiency gains. Within this flow, expectations from employers, customers and users have shifted – we all want more with less: faster, cheaper and safer. Hardware and software have caught up and IoT devices can do more than ever; they're smarter, tougher and more versatile.

Even the SIM space is evolving, with long-awaited developments like eSIM IoT (SGP.32) redefining what flexibility looks like. So far, so good – but can you wholeheartedly and confidently say that connectivity providers have evolved to respond to these changes?

That's why we encourage you to scrutinise your prospective connectivity provider because neither providers nor you can afford to treat connectivity like a commodity. You're not buying SIM cards and data plans; you're buying infrastructure. Your entire data strategy depends on connectivity working, and when it doesn't, it's binary: no connection means no data, no visibility and a direct hit to your bottom line. IoT deployments are full of shared responsibilities, but connectivity sits at the centre of them all.

In that first 30 minutes with your prospective provider, here's what to ask, what is an acceptable answer – and what is unacceptable.

1. Am I guaranteed the best possible signal?
Before we even touch upon uptime, let's unpack how devices connect to the network today – and how it affects both the lifetime of the device and your bottom line.

In the eyes of 3GPP, the threshold for 'high quality signal' is -85 dBm. But whether your device actually connects to a network above this threshold or uses another criterion lies with your connectivity provider. Welcome to the spooky world of steering, otherwise known as the public land mobile network (PLMN) priority list.

A PLMN list, often hardcoded into the SIM, dictates the networks your device connects to. This is not based on signal strength, but on commercial agreements providers have with operators. In practice, this means your device may be forced to connect to a weaker signal simply because it's higher on the PLMN list. This process, called steering, helps the provider – not you.

As a result of steering, your device can lose anywhere between 10% and 50% of its battery efficiency while struggling to maintain a weak connection enforced by the PLMN. It may also suffer dropped packets and retransmission attempts, inflating both your data bill and your frustration. ▶

SPONSORED ARTICLE

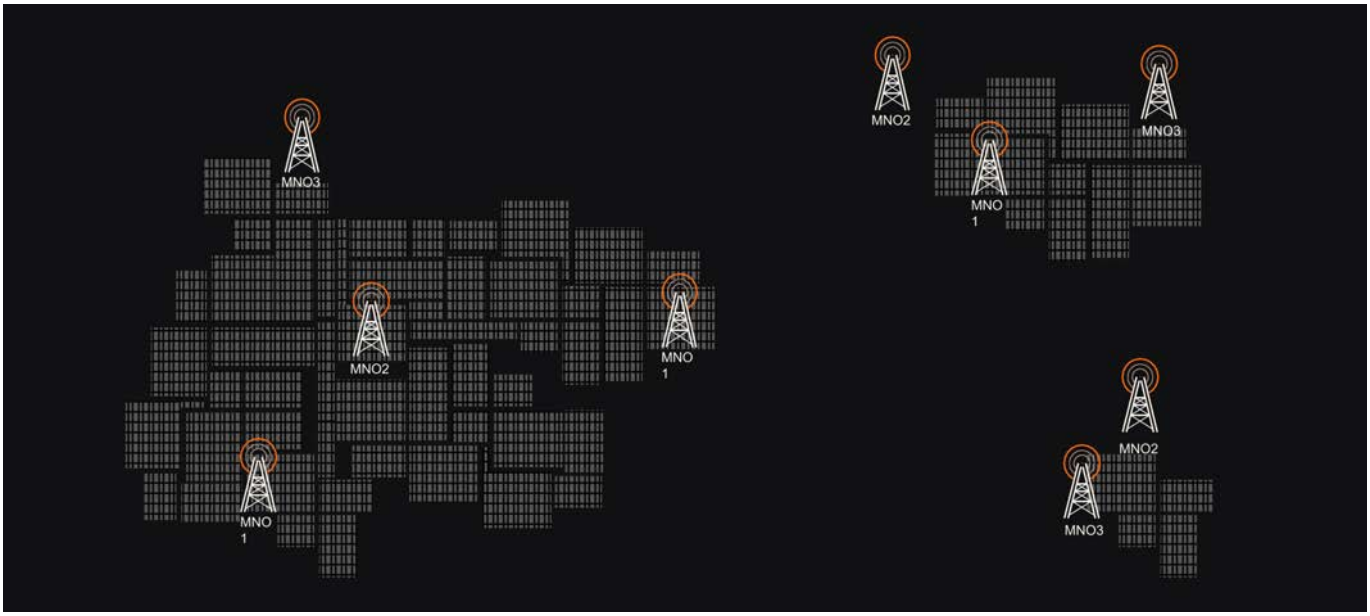


Figure 1.1

Let's visualise it for a second. In Figure 1.1, you can see an imaginary location along with all the available radio towers.

Figure 1.2

In the annotated map of Figure 1.2, you can see a steered connection scenario:

Following the SIM's PLMN, your device connects to ACME MNO despite several nearby towers offering stronger signals.

And here's the alternative.

Figure 1.3

Figure 1.3 is a non-steered map. The device automatically connects to the closest and strongest signal and tower, your coverage is better throughout and the risk of dropped packages is minimised.

Steering is, quite literally, your provider adding a rule on your device for their commercial gain. It's the SIM over-riding the logic of the radio module. Think of any instance of roaming in your private life. We have all been in a situation of roaming, where our signal is tanked and our friend's signal is stellar, even though we are in precisely the same location. This is the result of the respective providers steering the devices in different networks because of the PLMN – not because of signal strength. We've come to accept it because it's the industry norm – but that doesn't make it acceptable.

Therefore, dare to challenge the prospective provider and ask directly: Are my SIMs steered?

Here's how to interpret the answer. Some IoT providers will say "no", only to reveal later that their SIMs have dynamic or flexible priority lists. This is still steered connectivity — just with a longer leash. The only acceptable answer is simple: No steering, no priority list. The device connects purely based on signal strength, driven by the radio module, with 'good signal' defined by actual radio metrics, not commercial ones.

2. What happens when my device goes offline?

Let's go back to the change drivers for a second: Performance demands are higher, and we expect information faster. No one wants a report of what happened yesterday – what we want is a visual of what's happening right now. When something goes wrong, waiting to fix it is a luxury – fixing it as it occurs is the norm.

Anyone who has operated even one IoT device knows this scenario. Suddenly, there's an unplanned loss of connectivity, a service interruption. Someone notices it – hopefully you and not your customer – and you start investigating (as shown in Figure 2.1 over). But alas, you can't have access to data you need; it's sitting with your connectivity provider. If only the reason you deployed IoT devices in the first place was data visibility, right?

Next, you file a support ticket to your provider. Now if your device happens to be roaming, your provider has to reach out to their local partner to retrieve the data. You are already three touchpoints removed from the information you need. But since your device isn't on the provider's home network, your ticket is not prioritised.

You now depend on the provider's provider to send data back to your provider, who will then send it to you – some days later. Only then can you begin investigating and you may or may ▶

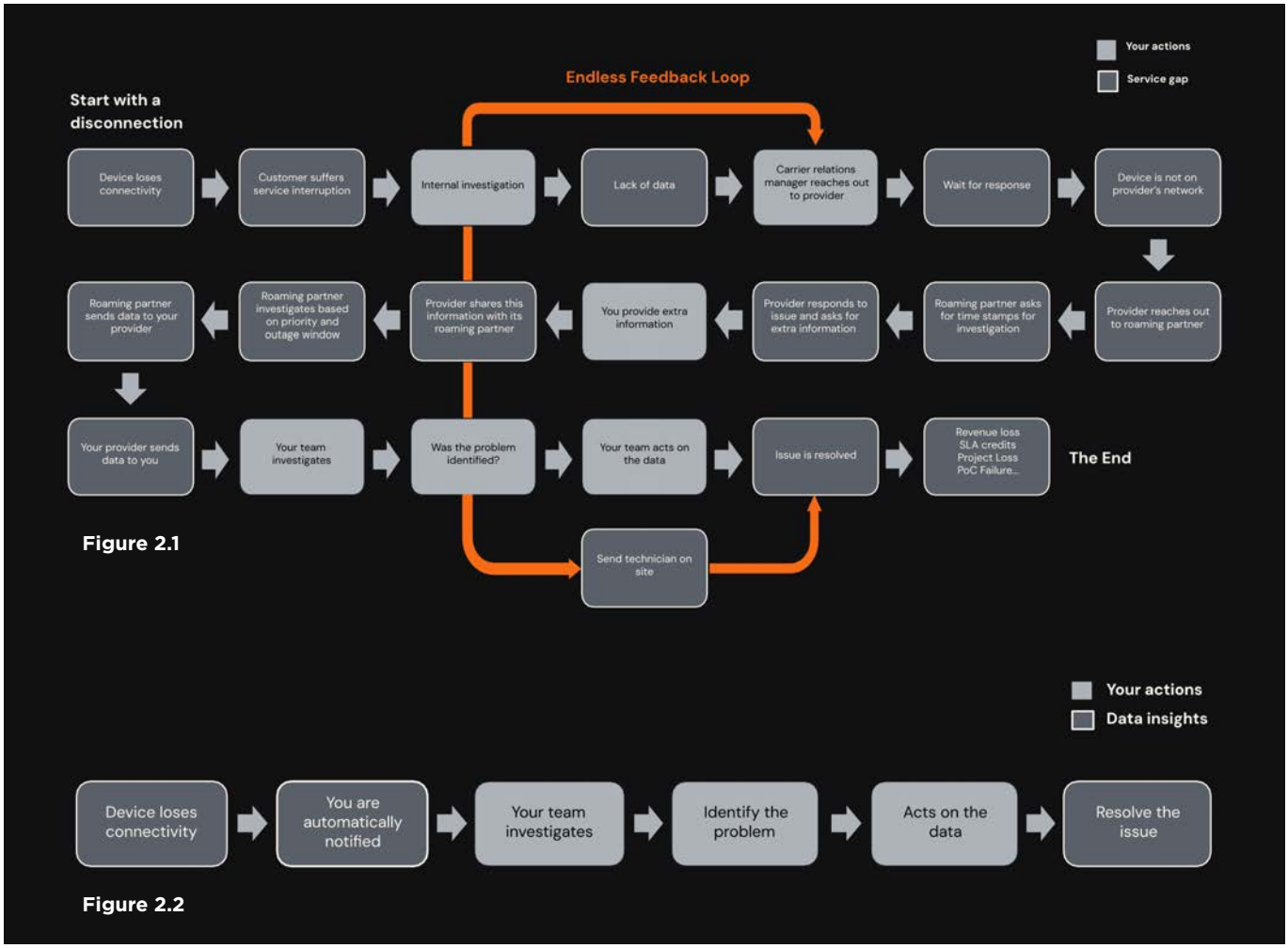


Figure 2.1

Figure 2.2

What you really want to know is whether your provider's SIM security is robust enough and, more specifically, how they handle SIM keys

not find the cause of the issue. And if you don't, you start over – no 200 Monopoly dollars for you. Meanwhile, you've lost SLA credits, possibly revenue, and instead of collecting the proverbial 200 Monopoly dollars, you're the one paying them, likely to send someone on-site and regain some control of the process.

This process raises the underlying question: why deploy connected devices if you have to physically interfere this much to make them work? So, what is the acceptable answer here? Certainly not the process above, not a ticketing system, nor an SLA. In fact, if you hear the words support or tickets, hang up right then and there.

The only acceptable answer is that you have direct access to connectivity data and real-time troubleshooting (as shown in Figure 2.2). Every MNO has this data, it is essential to operate their networks — but MNOs won't share it. MVNOs, on the other hand, can't share it, because they don't have access to it themselves – their MNO partner does.

3. Tentatively: Are you meeting the compliance requirements?
This is a trick question. The answer you'll often get, often with far too much enthusiasm, is an alphabet soup of acronyms and a slide filled with blue certification logos. You've read this far so you can already sense it: that's not the answer you're looking for.

What you really want to know is whether your provider's SIM security is robust enough and, more specifically, how they handle SIM keys.
Here's the short version. Every SIM card has its own security key, which lives on the physical card. But each of those individual keys is usually generated from a single master key that belongs to the operator.

Let's turn this around and look at what it means for you as the customer: you – and every other customer of that same provider – are dependent on the same master key to authenticate your SIM cards into the network. If one SIM is breached (as outlined in Figure 3.1 below), the shared lineage of that key means every other SIM becomes more vulnerable.

We've tried to be factual and descriptive in the presentation of this process. But the truth is, this is legitimately terrifying.

The implications of a potential security breach when SIM security is managed this way are enormous. They can affect hundreds of thousands of individuals –not to mention IoT devices– and the monetary risk of a breach can easily climb into the millions of euros. And it is not just a ▶

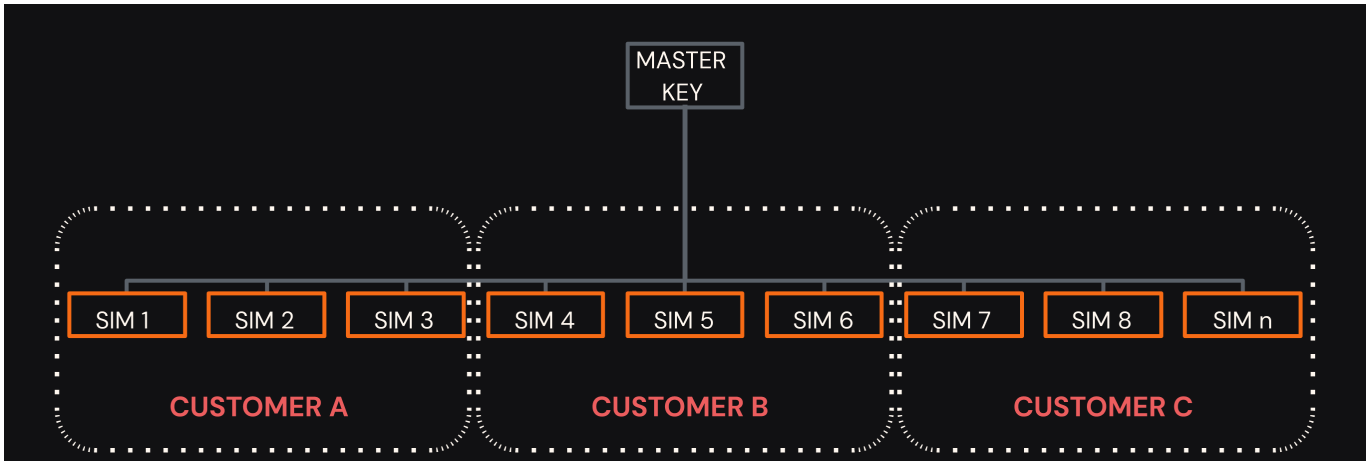


Figure 3.1

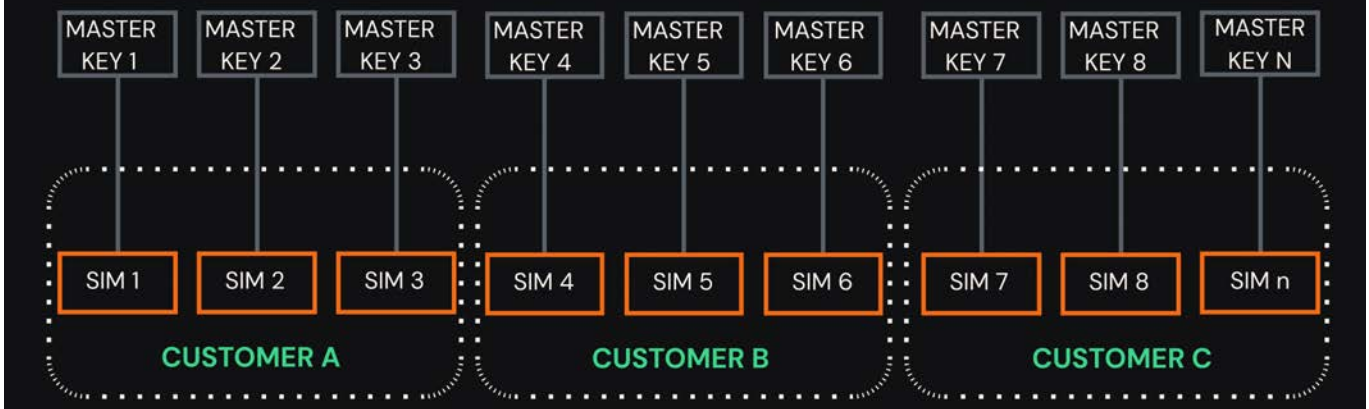


Figure 3.2

technical risk; it's the foundation of vendor lock-in. In addition, this vulnerability obfuscates the way forward for the arrival of eSIM IoT.

So, if your prospective provider launches into a tangent about certifications or fills the screen with blue logos, cut to the chase and ask: How do you manage your SIM keys today, and how do you transfer them? And do not accept any answer other than: a unique key for every SIM (as shown in Figure 3.2).

Why stop here? Ask more of your connectivity provider

Our relationship with data has changed, our expectations from technology have skyrocketed and they have both changed our entire behaviours. But our expectations from connectivity – the riverbed of our data – are arrested somewhere between 2004 and our personal references from our cellphone.

Connectivity can no longer be treated as a commodity, because your data isn't a commodity. It's the infrastructure of business decisions with real-life impact. It's not about SIM cards or data plans anymore; it's about whether your network can support the kind of performance, transparency, and reliability that modern systems demand. Commercial data infrastructure depends entirely on connectivity working as infrastructure – the unseen architecture that powers uptime, data integrity and everything your devices promise to deliver.

And while most providers still treat it like a commodity – and this is exactly the issue these three questions are meant to unveil – **Onomondo** was created because no one else was treating connectivity as infrastructure. Onomondo's connectivity infrastructure was built with those answers in mind from the start. A network designed so that devices always connect to the strongest possible signal. A system where data visibility is available in real time. A security-by-obscurity model where every SIM has a unique master key – not every customer; every SIM.

So as you step into your next IoT deployment or rethink your current one, remember: this is just the beginning of the connectivity-as-infrastructure playbook. Technology has evolved. The data has evolved. It's time your expectations and your providers do too. Ask more; demand more from connectivity, because your bottom line depends on it.

Connectivity can no longer be treated as a commodity, because your data isn't a commodity

Get in touch with Onomondo to eliminate the cost of connectivity and secure your IoT operations.
www.onomondo.com

rSIM expands MNO partnerships as resilient connectivity moves centre stage

As IoT becomes embedded deeper into business-critical processes, resilience is shifting from nice-to-have to non-negotiable. For enterprises operating in regulated or mission-critical environments, connectivity failure is no longer just an inconvenience, it's an operational risk

Over the past 12 months, **rSIM** has seen this shift accelerate.

"When we last spoke, resilience was an emerged requirement," says Daan de Wijs, the head of Business Development at rSIM. "Now it's a defined expectation. Enterprises are embedding IoT into core processes, and that makes connectivity fundamentally more critical."

rSIM has continued to expand in established verticals such as alarm services and healthcare, while moving into new sectors including EV charging. This diversification reflects a broader market reality: as IoT underpins regulated infrastructure and customer-facing services, uptime requirements are tightening.

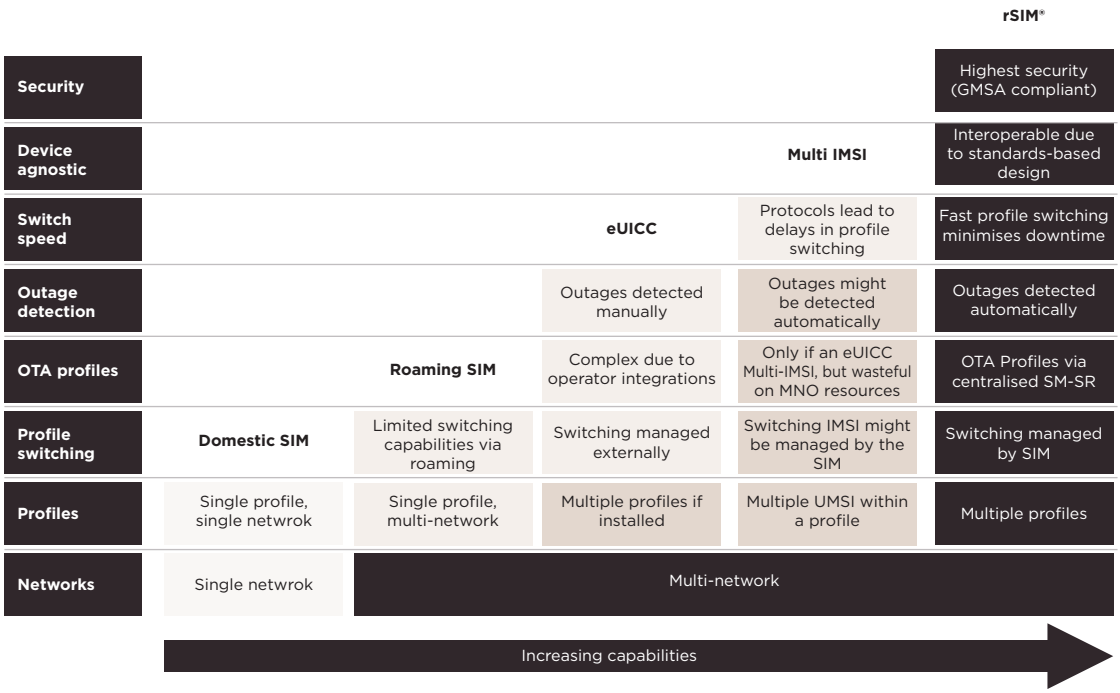
Growth in deployments and partnerships

Alongside vertical expansion, rSIM has strengthened its mobile operator ecosystem.

In addition to existing collaborations with **Deutsche Telekom** and **Tele2**, rSIM has collaborated with new partners including **Vodafone IoT** for example. These partnerships allow operators to offer resilient connectivity through a single contract and single point of contact. A key requirement for enterprise customers.

"For MNOs, the driver is clear," says de Wijs. "Customers expect resilience, but they don't want additional contracts or operational complexity. ▶

SPONSORED INTERVIEW



rSIM enables operators to deliver dual-core resilience within one commercial relationship."

The company's go-to-market model remains firmly partner-led, with the rSIM team supporting partners closely through customer engagements.

Beyond multi-IMSI

Multi-IMSI has long been positioned as a resilience strategy. However, according to de Wijs, it does not fully eliminate single points of failure. "rSIM is built on two fundamentals: continuous validation of the connection and two completely separate MNO core networks on one eSIM," he explains. "That second core is the differentiator. Many multi-IMSI solutions still rely on a single core, which means the risk of single point of failure remains."

Rather than reacting to fluctuating signal strength, rSIM monitors whether data can be sent and received. If service-affecting connectivity loss is detected, rSIM autonomously switches cores within seconds.

"It's not about chasing signal bars," says de Wijs. "It's about validating performance and acting only when necessary."

Correcting misconceptions

One of the biggest misconceptions heading into 2026, de Wijs argues, is underestimating how critical IoT connectivity has become.

"As more infrastructure becomes connected – substations, transport systems, EV networks – connectivity becomes part of the operational backbone," he says. "Regulations, customer expectations and new business models are all increasing the stakes."

He also stresses the importance of customer-led innovation.

"Too often in telecoms we build technology first and look for a problem to solve later. rSIM was developed from a real operational challenge. We experienced the pain of outages and complexity ourselves. That shaped the solution."

The shift towards SGP.32

While AI will dominate headlines at MWC, de Wijs believes the more immediate shift lies in the eSIM evolution and SGP.32.

"We're seeing a clear increase in customer and RFP requirements on eSIM capabilities and localisation," he says. "Customers are now ready to implement SGP.32-based models. That's where the imminent change is."

rSIM is finalising its eSIM strategy and plans to make further announcements in the coming months.

"The tipping point is here," concludes de Wijs. "Enterprises now understand that resilience isn't optional. The question is no longer 'can I connect?' but 'what happens when the network fails?'"

Too often in telecoms we build technology first and look for a problem to solve later. rSIM was developed from a real operational challenge

www.rsim.com

Connect with Berg Insight at MWC Barcelona March 2-5

Johan Fagerberg	Fredrik Stålbrand	Martin Cederqvist	Melvin Sörum	Filip Andersson
CEO & Founder	Principal Analyst	Senior Analyst	Analyst	Analyst

Berg Insight is an independent industry analyst and consulting firm, providing research, analysis and consulting services to clients in the areas of IoT and digital technologies. Our analysts possess deep expertise in major IoT verticals such as fleet management, automotive telematics, smart metering, smart homes, mHealth and connected industry. Founded in 2004, Berg Insight has its headquarters in Gothenburg, Sweden and serves more than 1,500 clients in 73 countries.

Berg Insight™

info@berginsight.com | Phone +46 31 711 30 91 | www.berginsight.com

SEMTECH®

Connecting smart meters

A guide to long battery life, wide coverage and secure deployments with cellular LPWA

Report sponsor:

SONY | altair

Connecting smart meters
A guide to long battery life, wide coverage and secure deployments with cellular LPWA

Smarter metering for a changing world

Utilities today are facing increasing pressure from every direction: aging infrastructure, climate-related disruptions, rising operational costs and evolving regulatory requirements. At the same time, customers expect accurate billing, seamless service and real-time data access—all with the highest standards of privacy and security

Smart metering has emerged as a critical solution to meet these demands. By digitising metering, utilities can transform their operations: reducing non-revenue losses, improving customer satisfaction and enabling more efficient use of resources.

Smart electricity meter adoption continues to accelerate across global markets. In Europe, electricity meter penetration is expected to reach 78%, with 326 million smart meters deployed by 2028. Smart gas metering is also on the rise, with installations projected to reach 77.6 million by 2028 – representing more than 61% percent of natural gas customers in the EU27+3 region[1] In North America, the installed base of smart electricity meters is projected to hit 182 million, representing approximately 95% market penetration by the same year[2]. ▶

Smart meters require extended operational lifespans, typically spanning 10–20 years, to minimise ongoing maintenance expenses and replacement costs. Installed in hard-to-reach areas, they must have durable components and reliable power to ensure consistent energy data collection over time. This also means that the technology selected for these products should be future proof to ensure reliable connectivity infrastructure for years ahead. In addition, as these are considered critical infrastructure, there are many security considerations and regulations to be met when rolling out a solution, requiring security to be built-in at the device level.

But enabling these long-life, widely distributed IoT devices requires not only the right meter devices, but also the right connectivity.

In this white paper, we explore the six critical connectivity considerations for smart metering deployments, from minimising power consumption and maximising coverage, to protecting security and ensuring future scalability.

Read this white paper to learn how to:

- Select a connectivity technology that aligns with power, performance and deployment goals.
- Understand how evolving regulations impact security and vendor selection.
- Extend coverage to rural and hard-to-reach areas using LPWA and satellite fallback.
- Balance data rates and latency for applications that need just enough bandwidth.
- Enable long-term success by choosing future-ready technologies.
- Partner with trusted suppliers to streamline integration and support lifecycle performance.

Coverage that reaches every meter

In smart metering deployments, reliable connectivity isn't a nice-to-have—it's essential. But meters aren't always installed in ideal locations. Whether buried in basements, housed in rural substations or mounted in hard-to-reach areas, they must remain online and operational.

LPWA: Built for hard-to-reach locations

Low power wide area (LPWA) cellular technologies like LTE-M and NB-IoT were designed for exactly these types of deployments. They offer extended coverage, better indoor penetration that supports better sensitivity and long-range connectivity with minimal power draw, thanks to features such as power saving mode (PSM) and extended discontinuous reception (eDRX) – making them a popular choice for utilities that need reliable links to geographically dispersed or shielded meters. These technologies also extend the signal capabilities of the devices. 3GPP established a target of achieving at least 15 dB of coverage gain for LTE-M, relative to a baseline Cat-1 Release 10 UE.

As part of the broader LTE infrastructure, these technologies benefit from mature global network support and efficient data handling tailored for smart meter use cases.

Expanding coverage with NTN

Still, even LPWA networks can leave gaps, especially in remote or sparsely populated areas. That's where non-terrestrial networks (NTNs) come in.

By using satellites to extend cellular connectivity beyond terrestrial limitations, NTN opens new possibilities for smart metering in:

- Off-grid or rural installations
- Remote energy infrastructure monitoring
- Locations impacted by natural disasters or coverage disruptions

Using the 450 MHz spectrum for deep coverage and utility applications

Another emerging option for utilities is the use of the 450 MHz spectrum, which offers excellent propagation characteristics. Operating at lower frequencies than typical LTE bands, 450 MHz can penetrate buildings and reach remote areas more effectively, making it well-suited for deep indoor coverage and rural smart meter deployments. In many markets, this band is designated specifically for critical infrastructure applications, allowing utilities to build private or semi-private LTE networks that deliver both coverage and control. Embedded in the LTE spec, using this spectrum relies on the proven and widely deployed LTE network worldwide, ▶

with the best-in-class security and quality of service features. Semtech's HL7845 fully supports the 450MHz spectrum, enabling deployment of these solutions.

Bottom line
By combining LPWA efficiency with NTN reach, utilities can achieve uninterrupted coverage across virtually any geography. This enhances not only data availability, but also the continuity of service, security and regulatory compliance - even under the most challenging conditions.

Getting the right data rates for the job

Not every smart metering application needs high bandwidth – but consistent, reliable data transmission is essential. Choosing a module with excessive throughput capabilities may increase cost and power consumption unnecessarily, while selecting one that's too limited can restrict functionality or future scalability.

What speed is 'enough' for smart metering?

Most smart meters transmit modest amounts of data–often just a few kilobytes per day. This might include interval data, diagnostics or status reports. In typical scenarios:

- Smart gas and water meters may need just 1–5KB/day.
- Smart electricity meters with more frequent reporting might average 50–200KB/day.
- More advanced meters that support real-time usage, remote disconnections, or firmware updates may require higher peaks–potentially several MB/month.

Thus, consistent uplink performance in the range of 10–200 kbps is often sufficient for smart metering deployments.

Matching module category to your needs

Technologies like NB-IoT and LTE-M were purpose-built for these low-throughput use cases with data rates of up to 156kbps for NB-IoT and 1.119Mbps for LTE-M, offering:

- Low power consumption
- Deep indoor coverage
- Broad operator support
- Future compatibility with 5G networks
- Robust security scheme, based on existing cellular rigorous security requirements

By contrast, options like Cat-1 or the upcoming RedCap offer higher data rates (up to several Mbps), but at the cost of greater power draw which is potentially unnecessary for fixed smart meters. These technologies are better suited to high-throughput or low-latency use cases like electric vehicle (EV) charging or video surveillance.

The pitfalls of overengineering

Selecting a higher-category module than needed can have unintended trade-offs:

- Higher module cost
- Increased power consumption
- Unnecessary spectrum usage (which may impact carrier costs)
- Greater design complexity

Smart metering solutions must strike the right balance between capability and efficiency.

Transmit power considerations: 20dBm vs. 23dBm for smart metering

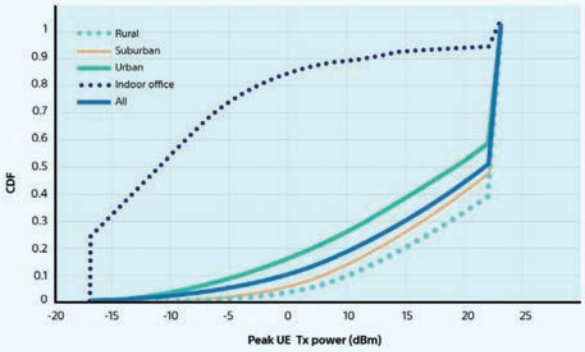
Power consumption is one of the most critical factors in smart metering deployments. Because devices are often deployed for a decade or longer – without easy access to power–selecting the right transmission power level can significantly impact performance, coverage and total cost of ownership (TCO).

Most utilities evaluate two primary power classes for cellular modules: 23dBm and 20dBm (dBm stands for decibel-milliwatts). Understanding the differences between them is essential to making a long-lasting, cost-effective choice. While mobile devices can move in and out of coverage areas, smart metering deployments consist of static devices. When a device is installed in an area with poor coverage, it will experience inferior performance throughout its lifetime, making the following performance comparison even more crucial. ▶

Why 23dBm is the standard

- Defined in 3GPP Release 8, the 23dBm class is foundational to LTE deployments– and many mobile network operators have optimised base stations for this power level.
- These base stations also support LPWA LTE-M and NB-IoT networks, making 23dBm an ideal match for smart metering.
- Real world data (shown in **Figure 1**) illustrates that 23dBm devices transmit at peak power over 50% of the time, maximising throughput and spectral efficiency.

Figure 1: Distribution of peak UE transmission power in different scenarios5



What's different about 20dBm?

- Introduced in a later 3GPP release, 20dBm devices have lower signal strength, which can be offset with:
- More transmission repetitions
- Reduced data rates
- However, because dBm is logarithmic, a 3dBm drop means halving signal strength, which can significantly affect connectivity in indoor, underground or rural environments.

Performance trade-offs in challenging conditions

In poor coverage scenarios, 23dBm devices offer notable advantages. While 20dBm devices may appear cheaper, the savings are marginal and often outweighed by hidden costs:

CATEGORY	20dBm	23dBm
Coverage	Weaker	Stronger – better penetration
Data Rates	Slower	Faster – shorter transmissions
Power Use	Higher (longer active time)	Lower (shorter active time)
Battery Life	Reduced	Extended
Application Support	Limited	Broader range of use cases

- **Power amplifier cost savings** (from 23dBm –> 20dBm) are minimal–typically only 5–7% of the total module cost.
- **Battery requirements** are often higher for 20dBm devices due to longer transmission times.
- **Service costs** can increase as well, since these devices consume more spectrum–a precious, expensive resource for mobile network operators.

Throughput drops with lower signal strength

When signal strength drops, performance can degrade significantly. A 3dB reduction in signal (maximum coupling Loss, or MCL) – equivalent to the difference between 23dBm and 20dBm – can lead to up to 50% lower data throughput. This has a direct impact on a smart meter's ability to transmit efficiently and reliably in fringe or obstructed environments. ▶

Figure 2: Effect of TX Power difference on device throughput and power consumption

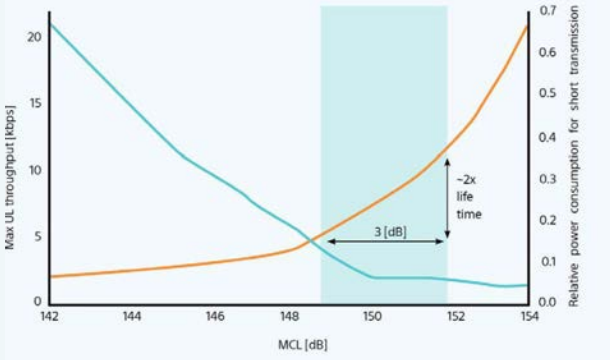


Figure 3: Effect of transmission time on overall power consumption

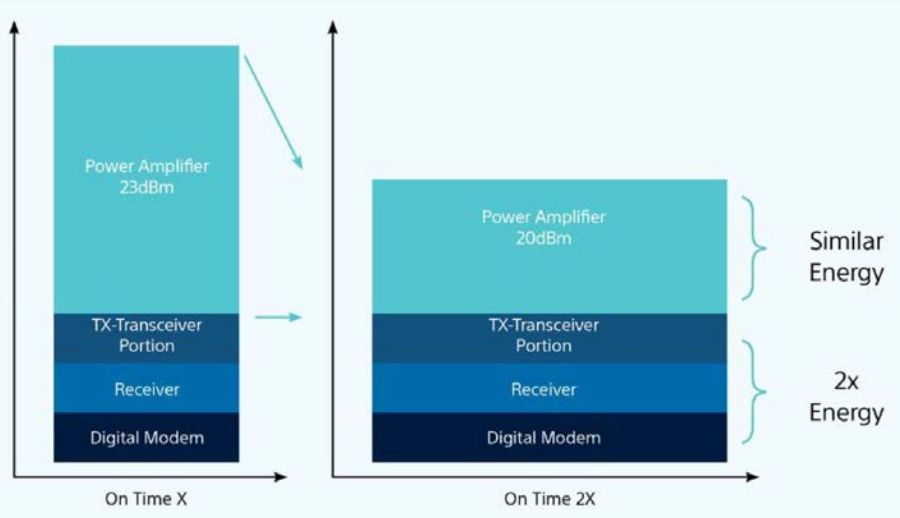
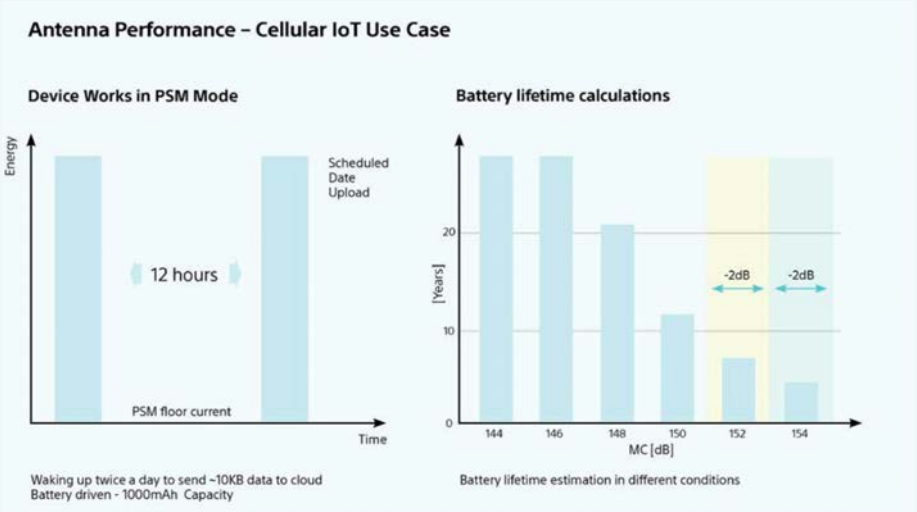


Figure 4: Battery Lifetime versus 2dB coverage difference scenarios



Transmission time and power usage increase

Slower throughput means devices must remain active for longer periods to complete their data transfers. This extended transmission time dramatically increases energy consumption—particularly for battery-powered devices. **Figure 3** illustrates how, in weaker coverage conditions, the overall power usage climbs even as the signal output decreases.

Even small signal drops can have big impacts

Even a 2dB decline in signal strength can increase power usage by 60–70%, especially in devices that send relatively small daily payloads – for example, 10KB/day. This makes the choice of transmission power not just a performance decision, but one that materially affects long-term operating costs and battery lifespan.

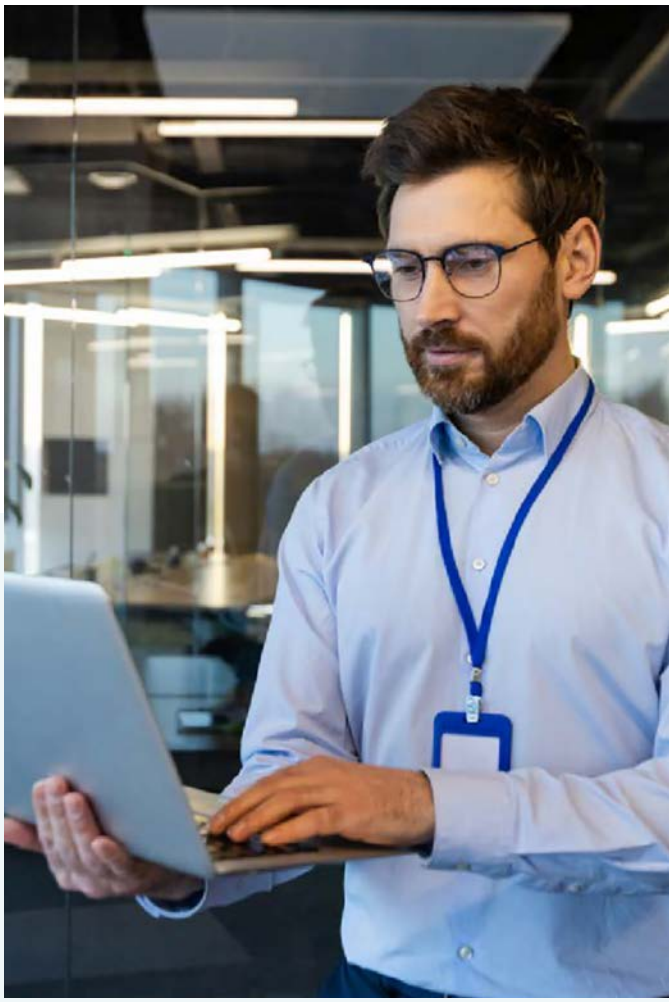
Bottom line

Although 20dBm devices offer slight cost savings on paper, their lower performance, higher energy consumption and reduced spectral efficiency can make them more expensive in the long run. For utilities seeking longevity, reliability and efficiency, 23dBm modules typically superior total value over the device lifecycle.

Securing smart metering in a changing regulatory landscape

As smart meters become integral to national infrastructure, ensuring robust, end- to-end security is no longer optional – it's a regulatory and operational necessity. Cyber threats can surface at any stage of a device's lifecycle, and new regulations continue to raise the bar for device integrity, supply chain transparency and long-term resilience.

Recent regulations such as the CE Radio Equipment Directive (RED) in Europe and the FCC Covered List in the US highlight growing concerns over untrusted suppliers and components. These frameworks are designed to prevent the deployment of infrastructure that could introduce cybersecurity risks, requiring utilities and device manufacturers to take a more proactive, holistic approach to security. ▶



EU standard EN 18031 is another good example. Under the Radio Equipment Directive, the three-part EN 18031 standard was harmonised on 30 January 2025 and became mandatory on 1 August 2025. Smart meter vendors may self-declare conformity, but must maintain a technical file proving secure boot, authenticated updates, and ongoing vulnerability management to satisfy RED requirements.

There are also many security considerations at the device level. SIM is the standard method of authenticating to networks, and the latest integrated SIM (iSIM) technology offers even greater resilience at the hardware level. iSIM embeds the SIM secure element inside the system-on-chip, eliminating the physical card slot, saving space and power, and establishing a hardware root of trust. iSIM allows utilities to swap network profiles over the air, reducing truck rolls and lowering total cost without compromising cryptographic security.

It's not just about enabling secure boot and deploying secure firmware updates– although firmware-over-the-air (FOTA) capabilities remain essential for long-term protection. True infrastructure resilience demands that every element of the smart metering ecosystem – from the silicon and firmware to the connectivity module and cloud management platform – comes from trusted, verified suppliers with proven security practices and regulatory compliance.

Start with trusted suppliers

Every device in a smart metering deployment is only as secure as the components inside it – and the partner behind them. That's why the first step in a secure lifecycle is choosing a vendor with a proven track record in:

- **Secure supply chains:** Verified sources, transparent processes and components manufactured and handled to international security standards.
- **Regulatory compliance:** Demonstrated alignment with data privacy laws and evolving industry regulations in key markets like the EU and US.
- **Ongoing innovation and support:** A roadmap that enables devices to stay protected and compliant over their entire operational lifespan.

Maintain resilience with secure FOTA

Once deployed, devices must remain secure and up to date–even as threats evolve. FOTA capabilities are essential to enabling this long-term protection, especially for distributed, hard-to-access smart meters. For these types of devices, it is also crucial that the FOTA process will be as secure and as efficient as possible, to not impact other device requirements

Key components of a secure FOTA system:

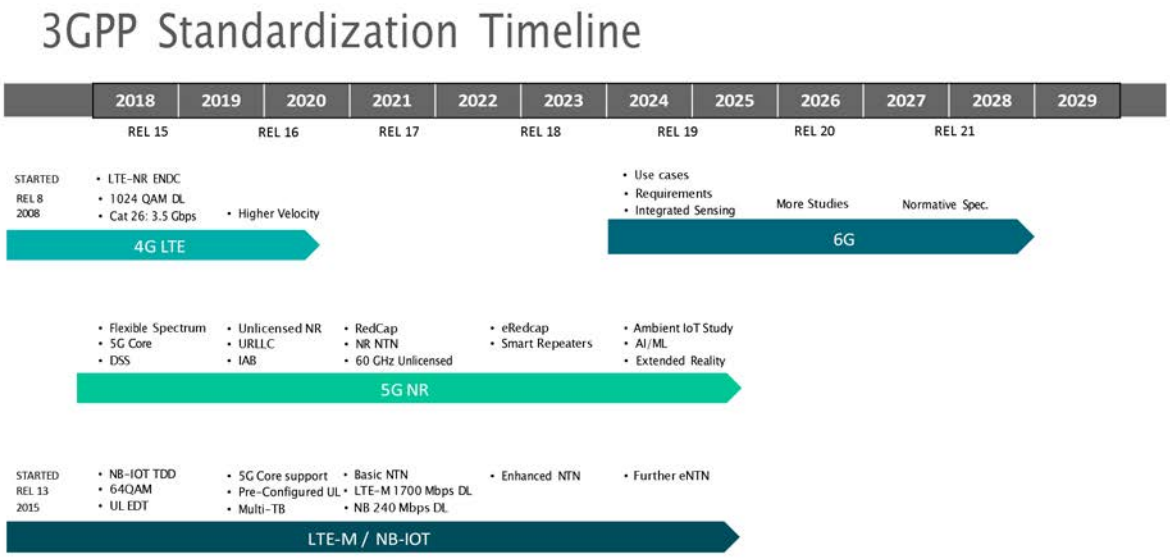
Platform security

The infrastructure where updates are stored, signed and deployed must be hardened against intrusion. That includes strong cryptographic key management and hosting within compliant jurisdictions, such as Europe and the US, for better regulatory alignment and control.

Device security

Devices must securely store cryptographic keys and validate update authenticity. Best practices include:

- Encrypted communication protocols (LwM2M, CoAP).
- DTLS 1.2 for secure data transit.
- Pre-shared keys and RSA signatures for mutual authentication.
- IP filtering and identity verification. ▶



Key rotation

Many regulations now require periodic key rotation – typically every 90 days – to reduce risk exposure. Secure device management systems must support this out of the box.

Resilience in the FOTA process

Even the best security won't help if an update fails in the field. FOTA systems must be designed to handle interruptions gracefully:

- Auto-resume or restart after power loss or signal failure.
- Rollback to the previous firmware version if issues arise.
- Allow update delays to preserve uninterrupted device operation.
- Self-monitor to proactively flag and resolve upgrade failures.
- Rollback protection to legacy, field-proven version.

Bottom line: Security starts at the source

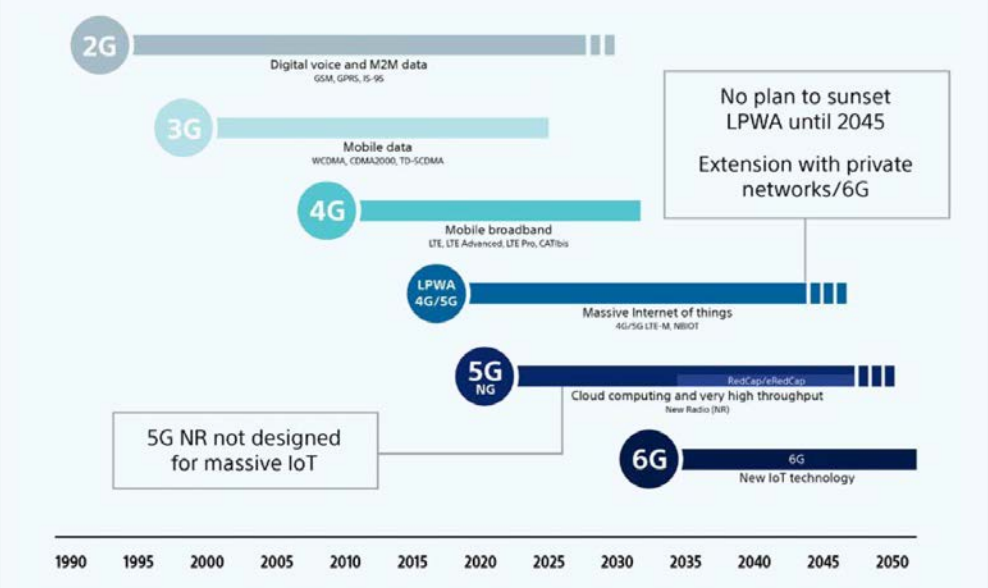
End-to-end security doesn't begin with an update. It begins with choosing the right partner. From hardware to firmware and management platforms, working with trusted, future-ready suppliers can help to ensure your smart metering deployment stands the test of time, regulation and risk.

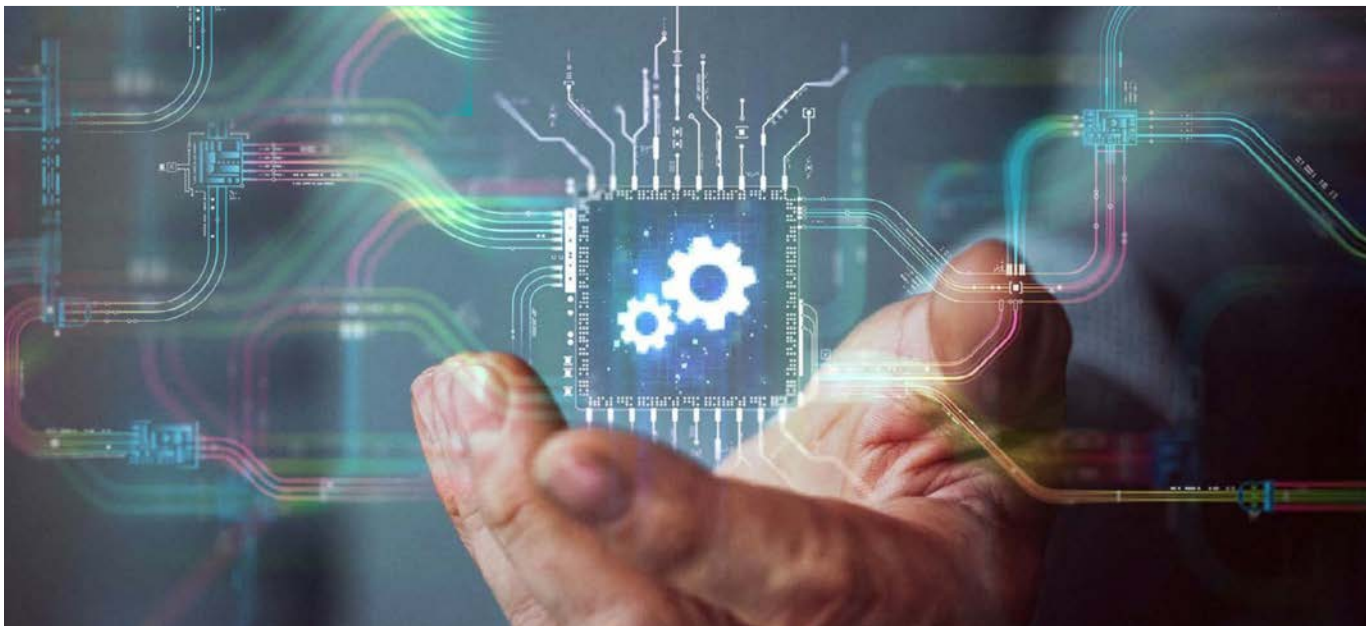
Future-proof smart metering deployments

Navigate the 2G/3G sunset

The global phase-out of 2G and 3G networks is well underway, with many carriers decommissioning these legacy systems to reallocate spectrum for more advanced technologies. This transition poses significant challenges for utilities and other sectors that rely on long-term, low-data IoT deployments, such as smart metering, which often have service lifespans exceeding a decade. ▶

Figure 5: Battery Lifetime versus 2dB coverage difference scenarios





To ensure uninterrupted service and avoid costly hardware replacements, it's imperative to adopt connectivity solutions that are resilient to these network evolutions. LTE-M and NB- IoT technologies are designed to remain viable beyond the 4G sunset, due to the inclusion of these protocols in the 5G standard.

Embracing LPWA technologies for longevity

LPWA technologies, specifically LTE-M and NB-IoT, have emerged as the preferred alternatives for future-proof IoT deployments. These technologies offer several advantages:

- **Extended network support:** LPWA technologies are designed to be integral parts of the 5G ecosystem enabling their relevance and support well into the future.
- **Enhanced coverage:** They provide superior penetration in challenging environments, such as basements or remote areas, enabling reliable connectivity where traditional networks may falter.
- **Optimized power consumption:** LPWA solutions are tailored for low-power operations, making them ideal for battery-powered devices that require long operational lifespans without frequent maintenance.

A future-ready platform: The HL7900 module

To satisfy utilities' smart metering needs, Semtech offers the HL7900 module, a global 5G LPWA module featuring the Sony's Altair ALT1350 chipset. Building on the proven success of the widely adopted HL7810 and HL7812 4G LPWA modules, the HL7900 was designed from the ground up to support long-lasting, secure and efficient smart metering deployments. ▶

Key features include:

- Ultra-low power consumption for 10+ year device lifecycles.
- Native support for LTE-M and NB-IoT.
- Support for 3GPP Releases 14/15/16/17[3], enabling longevity across evolving standards.
- NB-IoT over satellite support on the roadmap for remote and resilient deployments.
- Unlicensed band radio support—such as Wi-SUN or wM-Bus—eliminating the need for external wireless MCU.
- Security by design, including secure boot, encrypted FOTA and trusted provisioning.
- Integrated GNSS and edge processing, enabling location awareness and reduced cloud dependencies.

With a platform that prioritises long-term stability, compliance and innovation, utilities can confidently invest in infrastructure that will remain resilient and connected well into the future.

Next-level resilience: Satellite-ready modules and dual-mode innovation

For utilities operating in hard-to-reach or low-connectivity regions, Semtech's HL7810 and HL7812 modules provide a seamless path to NB-IoT over NTN. These modules are certified to operate on the Skylo satellite network, offering satellite fallback via a simple firmware upgrade—no hardware changes required.

Looking ahead, Semtech is preparing to launch a comprehensive dual-mode solution that combines the HL78 series with Smart Connectivity Premium. This approach enables dynamic switching between cellular and satellite coverage, unlocking unmatched global reach and operational resilience for smart meter providers.

Utility deployment scenarios: The role of Semtech and Sony's Altair in smarter metering

While technology decisions are often made at the design level, their true impact is revealed in real-world deployments. Semtech's customers have successfully deployed millions of Sony's Altair-based LPWA modules in the field, demonstrating proven technology reliability over years of real world operation. These smart metering examples highlight how connectivity choices translate into long-term success in the field, backed by extensive deployment experience and field-tested performance.

Water metering in the United States: Navigating harsh conditions and long lifecycles

A leading water metering manufacturer in the US needs a connectivity solution that can operate in some of the most demanding environments – underground pits, deep basements and remote utility sites. Their key challenges include:

- **Harsh installation environments:** Many meters are installed in buried enclosures or under concrete slabs.
- **Power constraints:** Meters must operate on battery power for up to 20 years, with no access to mains power.
- **Data demands:** Regular interval-based readings and alarms, such as tamper alerts or leak detection, must be transmitted reliably.

By selecting an LPWA module supporting LTE-M, and by utilising 23dBm transmit power, the manufacturer can achieve consistent coverage, even in signal-challenged locations. Future support for NB-IoT over NTN will enable extended fallback coverage as their deployments expand to more remote regions. The HL7900's power-saving modes further help extend battery life—helping to support the utility's goal of 15+ years of operation without battery replacement.

Smart gas metering in Europe: Planning for longevity and regulatory shifts

In Europe, a gas metering provider is rolling out a next-generation solution across several countries. Their top priorities include:

- **Future-proof technology:** Devices must remain operational for 15+ years as 2G/3G networks sunset and LPWA matures.
- **Modular design:** A single cellular module must support a range of meter models and be upgradeable via firmware.
- **Regulatory compliance:** The connectivity solution must meet strict regional data sovereignty and security rules.

The provider chose the HL7900 for its combination of low-power performance, support for 5G LPWA and firmware-based upgradability. Its fallback to NB-IoT will enable resilience, while security features like trusted key storage OTA updates support compliance with evolving European regulations. The result is a smart metering platform that can scale across countries and adapt to future changes—without hardware redesigns. ▶

Powering the future with trusted technology partners

The evolution of smart metering is reshaping how utilities manage resources, improve service delivery and plan for a more connected future. Success depends on selecting connectivity solutions that address current challenges – and are ready for what's next.

Throughout this whitepaper, we've explored the critical factors for utilities to weigh when choosing modules for smart metering deployments:

- **Coverage:** Using LTE-M and NB-IoT, with fallback to non-terrestrial networks for uninterrupted connectivity.
- **Data rates:** Aligning network performance with real world application needs to avoid over- or under-specification.
- **Power consumption:** Selecting the right power class to extend battery life and optimise operational efficiency.
- **Security:** Improving device and platform integrity through end-to-end protection and compliance with evolving global regulations.
- **Future-proofing:** Investing in technologies that support long deployment lifecycles, flexible upgrades and standards evolution.

Ready to move forward?

Contact us today to learn how Semtech's and Sony's Altair trusted IoT solutions– powered by decades of experience and innovation–can support your next- generation smart metering deployment.

About Semtech

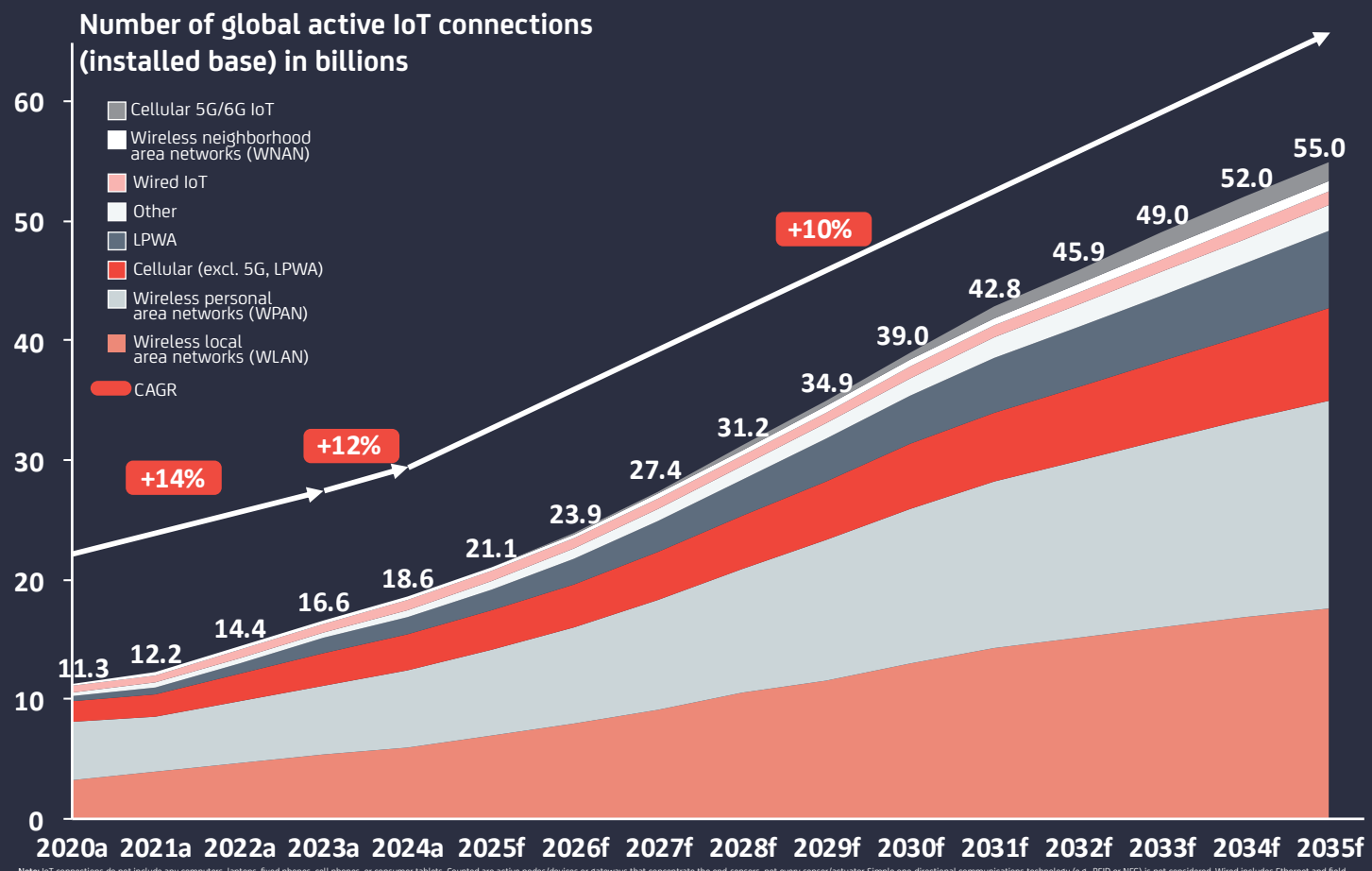
Semtech Corporation (Nasdaq: SMTC) is a high-performance semiconductor, IoT systems and cloud connectivity service provider dedicated to delivering high-quality technology solutions that enable a smarter, more connected and sustainable planet. Our global teams are committed to empowering solution architects and application developers to develop breakthrough products for the infrastructure, industrial and consumer markets.

1. https://media.berginsight.com/2024/02/16191446/bi-sm18-ps.pdf
2. https://www.marketresearch.com/Berg-Insight-v2702/Smart-Metering-North-America- Edition-37204261/
3. Release 15/16 and 17 will be supported in the future (roadmap item)

IOT ANALYTICS

State of Enterprise IoT 2026

Number of connected IoT devices to reach 39 billion in 2030; >50 billion by 2035



Note: IoT connections do not include any computers, laptops, fixed phones, cell phones, or consumer tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology (e.g., RFID or NFC) is not considered. Wired includes Ethernet and field buses (e.g., connected industrial PLCs or I/O modules); The number of wired IoT aggregation nodes represents the primary connection point and excludes all wired end nodes. Cellular includes 2G, 3G, 4G, 5G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave, or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

ANALYST OPINION

"IoT is no longer only about connectivity. It is shifting toward on-device compute and intelligence because most of the 20+ billion deployed endpoints still rely on cloud processing or simple rules, driving an edge AI upgrade cycle. At the same time, connectivity economics are branching, with Cat 1 bis carrying replacement volumes while RedCap and eRedCap define the next premium revenue pool, and satellite IoT quietly expanding coverage where terrestrial networks cannot reach."

Satyajit Sinha, Senior Principal Analyst at IoT Analytics

ABOUT IOT ANALYTICS

Headquartered in Germany, we provide holistic market insights and strategic business intelligence for IoT, AI, cloud, edge, and smart manufacturing. Our analyses are unbiased, high-quality, and in-depth.

Trusted by over 1,000 global companies, our analysts dedicate 6 to 8 months to a single market report. This investment is 2 to 3 times the industry average. We place high emphasis on primary research, including interviews and surveys of vendors, end-users, system integrators, and consulting companies across the tech stack, verticals, and regions.

More information: www.iot-analytics.com

SCAN TO DOWNLOAD A FREE REPORT SAMPLE

www.iot-analytics.short.gy/WxP3aG

SGP.32 Buyers Guide

What IoT Decision Makers Should be Asking about eSIM

> ***SGP.32 is not just another connectivity upgrade: it redefines how IoT connectivity is sourced, delivered, and governed.***
>
> Beecham Research, SGP.32 Buyers Guide

SGP.32 marks a fundamental shift in how IoT connectivity is sourced, managed and governed, yet many organisations are still struggling to separate practical impact from technical detail.

This Buyer's Guide cuts through the complexity to focus on the questions decision-makers actually need to ask when evaluating eSIM strategies, global deployments and long-term connectivity control.

Drawing on independent analysis and real-world deployment experience, the guide highlights where SGP.32 is already delivering business value, and where assumptions can create risk.

Designed for OEMs, enterprises and service providers, it provides clear decision frameworks, use-case insight and RFI-ready questions to support confident, informed choices.

Download Free Report

wireless logic

beecham research

Shaping the IoT future

flo. LIVE

Stop forcing AI through traditional networks

A network beyond, purpose-built to make you future-ready.

Built with and for AI.

Even a 3-year-old knows when something doesn't fit.

If you're scaling AI-led IoT, you need a network built for local behavior, intelligent routing, and sovereignty by design, ***Seamless***, ***Secure***, ***Adaptive***, and ***Crazy Smart***.

Go Beyond Connectivity

www.flolive.net