IoT Now: ISSN 2397-2793

2025 • VOLUME 15 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

Telit Cinterion's Roy MacLean says IoT developers should start at the end to achieve end-to-end, security-first, scalable deployments

UTILITIES
How IoT is enabling electricity industry transformation
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**

CONNECTIVITY
Understand how connectivity leaders should approach the market in our latest Analyst Report inside

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

PLUS: **Giesecke+Devrient's Andreas Morawietz demystifies SGP.32** • Analysts burst the IoT projections bubble • Wireless Logic zips up US acquisition • Infineon's Sivaram Trikutam explains how connectivity and edge computing are transforming smart homes • floLIVE facilitates cross-border logistics in Africa • Viasat expands global IoT with IoT Nano • Aeris and Bridge Alliance partner for IoT security • VitalThings adopts Telit Cinterion for contactless care project • Soracom expands AI capabilities with new GenAI tools • Exclusive event previews of MWC25 Las Vegas and Enlit Europe 2025 - Read the latest News, Features and Interviews at **www.iot-now.com**

CONTENTS

IN THIS ISSUE

Telit Cinterion

Cover sponsor: Telit Cinterion empowers IoT solutions worldwide. We simplify onboarding connected devices for our customers with a portfolio that offers:

- Enterprise-grade wireless communication and positioning modules
- Cellular MVNO connectivity plans and management services
- Edge and cloud software
- Data orchestration
- IoT and industrial IoT platforms

With more than 30 years of IoT innovation experience, we deliver award-winning secure and integrated IoT solutions. Our IoT experts have pioneered a successful end-to-end system approach to ensure all the pieces work together.

We enable thousands of successful IoT solutions worldwide and continue to invest in our technology roadmap to push the industry forward for years to come. **www.telit.com**

Cellular IoT analysts forever blowing bubbles with latest volume stats

The overblown predictions of growth in IoT connection volumes of a decade ago have now come to pass but the researchers may be once bitten, twice shy. The current crop of analyst projections may even undershoot reality in the face of massive IoT momentum, adding substantially to the installed base. Kicking off the latest set of figures, Juniper Research has found that cellular operators are set to generate US$30 billion from cellular IoT connectivity in 2030. That's up from US$18bn this year and represents an increase of 74%

George Malim, managing editor

Sustained growth in the cellular IoT sector has also been reinforced by Berg Insight's figures, which have reported that global cellular IoT connectivity revenues increased 12% to hit €14.2bn (US$16.6bn) in 2024. The firm predicts that there will be 6.4 billion IoT devices connected to cellular networks worldwide by 2029 and these will generate annual connectivity revenues of €22.4bn (US$26.19bn). While connection numbers are growing, average monthly revenue per user decreased by 5% to €0.33, demonstrating continued fierce competition between cellular operators. Even so, the installed bases of the largest mobile operators grew at a rate of between 5% and 26% annually in 2024.

The operators don't have it all their own way, either. IoT managed service providers, such as 1 Global, 1NCE, Aeris, BICS, CSL Group, Cubic, emnify, Eseye, floLIVE, Giesecke+Devrient, KORE, Monogoto, Onomondo, Semtech, Soracom, Tata Communications, Teal, Telit Cinterion, Velos IoT and Wireless Logic, had more than 200 million cellular IoT connections under management at the end of 2024. That equates to around €1.8bn (US$2.1bn) in annual revenues.

The growth curve is showing no sign of faltering. A substantial indicator of market growth is shipments of cellular IoT modules and IoT Analytics reports these grew 23% year-on-year in the first quarter of 2025, recording a fifth consecutive quarter of growth. It's not all plain sailing with substantial headwinds in the form of US tariffs and continuing inventory correction among vendors. Some, notably u-blox, have left the market but those that remain are capitalising on huge growth in China. The top five vendors accounted for almost three-quarters (73%) of module shipments in the first quarter of 2025.

With AI-assisted applications, variants of 5G such as RedCap and enhanced RedCap and the simplification enabled by embedded and integrated SIM technologies (eSIM and iSIM) all entering the mainstream it's possible to suggest that these reports and predictions look conservative rather than sensationalist. Let's hope that's the case. No one likes a bubble when the alternative is a market that serially outperforms expectations.

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

Wireless Logic acquires Zipit Wireless

Wireless Logic, an IoT solutions provider, has acquired **Zipit Wireless**, a multi-carrier IoT connectivity and subscription billing solutions provider. The step marks Wireless Logic's first acquisition of a US-headquartered company and aligns with its broader strategy to scale internationally while reinforcing regional expertise in key markets.

Headquartered in South Carolina, Zipit delivers connectivity across sectors including agriculture, security and surveillance and digital signage. With operations in both the US and Canada, Zipit is recognised for its flexible, white-labelled billing platform, strong customer support and regional insight. To date, Zipit's billing capabilities have supported more than US$45 million in subscription revenue for its OEM clients. Its Canadian subsidiary, **Mtrex Networks**, is a provider of global connectivity primarily serving the point-of-sale (PoS) market.

Zipit's long-standing relationships with top-tier carriers such as **Verizon**, **AT&T** and **Rogers** support global connectivity through a wide range of technologies, including NB-IoT, LTE-M and 5G. Its platform reduces commercial complexity through automated billing and flexible subscription models, giving businesses greater control over how services are packaged and billed.

Oliver Tucker, Wireless Logic

"Zipit's deep understanding of the North American market and its expertise in complex commercial models make it a welcome addition to the group," said Oliver Tucker, the co-founder and CEO at Wireless Logic. "We're delighted to have the team onboard and look forward to the opportunities this creates for our customers and partners." ■

floLIVE launches cross-border cellular IoT service spanning Africa's logistics corridors

floLIVE, a global enabler of IoT connectivity solutions, has announced the launch of its connectivity offering designed to revolutionise monitoring of transportation and logistics in Sub-Saharan Africa. The solution enables trucking, supply chain and related companies to cost effectively use video surveillance applications to conduct safe, reliable and timely operations. The service is available through select partners serving the transportation industry.

floLIVE's offering includes a high-bandwidth cellular connectivity package that is priced about 70% lower than conventional roaming services and is purpose-built for the operational realities of Africa's logistics. The service delivers seamless connectivity throughout major business corridors, overcoming common challenges such as network dead zones, inconsistent coverage and fragmented SIM infrastructure. The solution enables logistics operators to scale video surveillance, track cargo in real-time and ensure uninterrupted fleet communications.

"In a region where cellular coverage is inconsistent, we have developed a secure and resilient network that addresses service gaps and helps transportation, supply chain and logistics companies in this fast-growing region maintain secure and reliable operations," said Chen Porat, the senior vice president for floLIVE. "The service enables these companies to vastly improve their operations through a combination of frictionless cellular coverage and robust onboard always-on video surveillance equipment. Just as importantly, we have created a solution that transforms the economics of IoT and normalises the incredibly disparate data subscription rates among carriers. This not only improves the cost effectiveness and physical security of freight transportation within Sub-Saharan Africa, but it can lead to greater performance and profitability for these businesses."

The backbone of this cross-border service is floLIVE's resilient, high-performance cellular coverage across Sub-Saharan Africa. The company's multi-country infrastructure supports consistent monitoring powered by its intelligent multi-IMSI technology which allows a single SIM to automatically switch between identities tied to different mobile network operators throughout the region. Resilient, always-on connections are assured throughout the service area through direct connections with a minimum of two mobile networks in every country. ■

News in Brief

KORE and TD SYNNEX announce alliance to simplify connectivity

KORE has joined forces with **TD SYNNEX**, a global distributor and IT solutions aggregator, to simplify how businesses access and deploy IoT connectivity. Through this alliance, KORE's OmniSIM US connectivity plans are now available via TD SYNNEX's broad distribution network, making it easier for channel partners and end customers to adopt scalable, reliable IoT solutions.

"By aligning with TD SYNNEX, we are making it easier than ever for customers to access best-in-class IoT connectivity with straightforward pricing models," said Ryan Yahrmatter, the senior vice president of strategic partnerships and carrier relations at KORE. "This collaboration is a significant step in ensuring businesses have the seamless, scalable connectivity solutions they need."

Napino and Teksun launch Rapidise with US$4m seed funding

Napino Tech Ventures (NTV) and **Teksun Microsys** have launched **Rapidise Technology** (RTPL) with US$4 million in seed funding, aimed at transforming how artificial intelligence (AI)-enabled connected devices are designed, engineered and manufactured at scale.

Rapidise serves as a one-stop original design manufacturer (ODM) for start-ups, SMBs and enterprises developing next-generation, AI-powered products. As an ODM, Rapidise not only manufactures but also designs, prototypes, certifies and manages the full product lifecycle, enabling customers to focus on branding and market strategy while Rapidise delivers turnkey innovation. ■

News in Brief

Siemens and Microsoft collaborate on IoT interoperability for buildings

Siemens Smart Infrastructure has announced a collaboration agreement with **Microsoft** to transform access to Internet of Things data for buildings. The collaboration will enable interoperability between Siemens' digital building platform, Building X, and Microsoft Azure IoT Operations enabled by Azure Arc. Azure IoT Operations, a component of this adaptive cloud approach, provides tools and infrastructure to connect edge devices while integrating data, enabling organisations to optimise their operations and utilise the potential of their IoT environments.

The interoperability of Building X and Azure IoT Operations is making IoT-based data more accessible for large enterprise customers across commercial buildings, data centres and higher education facilities and provides them with the necessary information to enhance sustainability and operations. It enables automatic onboarding and monitoring by bringing datapoints such as temperature, pressure or indoor air quality to the cloud, for assets like heating, ventilation and air conditioning (HVAC) systems, valves and actuators. The solution will allow customers to develop their own in-house use cases such as energy monitoring and space optimisation.

Sateliot advances constellation with five new satellites

Sateliot has taken another step forward in the deployment of its satellite constellation by entrusting the manufacture of its next five satellites to the Spanish firm **Alén Space**. These satellites, which will become part of its low-earth orbit (LEO) network, are scheduled for launch in 2026 and reinforce Sateliot's position as a dual-use - civilian and defence - 5G satellite connectivity operator, in line with Europe's push for space autonomy.

With this move, Sateliot continues to implement its roadmap to deploy a constellation of more than 100 satellites, fully developed in Barcelona and validated by 3GPP - the international telecommunications standards body - with the goal of delivering secure and interoperable global coverage.

Aeris and Bridge Alliance partner to launch integrated IoT security for APAC

Aeris Communications and **Bridge Alliance** have announced they are teaming up to offer Aeris IoT Watchtower, an agentless and frictionless solution that delivers full visibility into the cyber risk of enterprise customers' IoT devices plus the tools to prevent or limit damage from an attack. The agreement is an extension of an existing partnership through which Aeris provides cellular IoT connectivity management services to participating Bridge Alliance Member Operators (BMOs) via the Aeris IoT Accelerator (IoTA) platform.

Mark Cratsenburg,
Aeris

Aeris and Bridge Alliance intend to close the cellular IoT security gap by offering the Aeris IoT Watchtower solution to enterprises in Asia-Pacific. Ong Geok Chwee, the CEO of Bridge Alliance, said: "The commercial launch of Aeris IoT Watchtower in Asia-Pacific for our BMOs and their customers is a milestone in enhancing security for the IoTA platform, and will boost security and regulatory compliance for enterprise IoT deployments and offer advanced network visibility to meet cybersecurity needs. We look forward to extending Watchtower into more APAC markets in the coming months."

Mark Cratsenburg, the chief commercial officer for the IoT Business Unit at Aeris, added: "Aeris IoT Watchtower offers real-time protection with zero friction. Forget agents, special SIM cards or complex rerouting. We provide enterprises complete visibility into their cellular IoT security risks and the ability to neutralise threats.

Viasat expands global IoT capabilities with IoT Nano

Viasat has announced that its enterprise business, part of the company's communication services segment, has launched its next generation IoT Nano connectivity service to deliver two-way messaging connectivity across the globe. IoT Nano is designed to meet growing global demand for cost-effective, low-data, low-power, Internet of Things (IoT) services across remote and challenging environments where mobile connectivity is often required. With IoT Nano, businesses can effectively monitor and control fixed and mobile assets across industries like agriculture, transport, utilities, mining and environmental monitoring — all with satellite coverage through Viasat's global L-band network.

IoT Nano is powered by **ORBCOMM**'s next-generation satellite IoT service OGx, an evolution of the IsatData Pro (IDP) service that offers faster message delivery speeds, larger message sizes and new hardware options relative to its predecessor. This new service expands Viasat's diverse portfolio of IoT connectivity services, which range from ultra-low data rate narrowband IoT services to static VSAT IoT offerings.

Andy Kessler, the vice president of enterprise and land mobile at Viasat, said: "The IoT Nano service represents a significant advancement in providing flexible, scalable and energy-efficient IoT connectivity to businesses operating in the most remote corners of the world. By using the enhanced capabilities of the ORBCOMM OGx service and equipping our partner ecosystem with new low-cost modules and service capabilities, we are empowering customers with access to smarter data, more frequently, in more places, at a lower cost."

Telit Cinterion enhances deviceWISE AI Visual Inspection with NVIDIA TAO 6.0 integration

Telit Cinterion, an end-to-end IoT solutions enabler, has announced the latest enhancement to its deviceWISE artificial intelligence (AI) Visual Inspection platform through integration with **NVIDIA TAO 6.0**. This integration brings low-code AI capabilities to industrial visual inspection, allowing manufacturers to use prompt-based segmentation, in-context annotations and powerful foundation models for tasks such as object pose estimation. Now, quality control teams, engineers and production managers can develop and deploy custom AI models more rapidly, identifying defects and optimising processes with greater precision across factories.

The integration with NVIDIA TAO 6.0 builds on this foundation by incorporating advanced annotation tools, such as prompt segmentation and in-context segmentations, which enable auto-labelling of object detection and segmentation masks using simple text prompts — like "missing bolt on assembly line" or "coating variation on component" — without the need for extensive training or fine-tuning. This reduces annotation costs and effort while improving accuracy for specific industrial objects. Because TAO ships containerised micro services with pre trained foundation models, it integrates into the existing deviceWISE Visual Inspection pipeline with minimal changes.

Linir Zamir,
Telit Cinterion

"Integrating NVIDIA TAO 6.0 into deviceWISE AI Visual Inspection empowers manufacturers to build and deploy custom AI models with unparalleled ease and speed," said Linir Zamir, the team lead for deviceWISE AI Development at Telit Cinterion. "deviceWISE Visual Inspection enables manufacturers to collect, transform and integrate data from any machine to any IT system, creating full applications for Industry 4.0 and digital transformation. With TAO's low code auto labelling, pose estimation and multi modal models built in, customers get faster deployment, higher accuracy and zero custom code or specialty cameras."

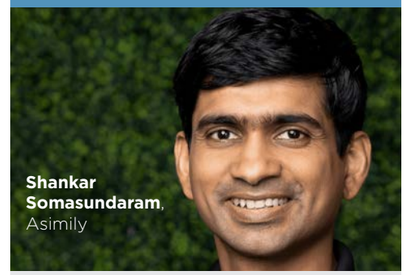
Soracom expands AI capabilities with new GenAI tools

Soracom, a global provider of advanced Internet of Things (IoT) connectivity solutions with full MVNO capability, has announced two new platform services that use GenAI capabilities to accelerate IoT development and support leading-edge video analysis use cases.

Soracom has also announced that Soracom Query, an AI integration service designed to let customers analyse and visualise their IoT network data, has transitioned from early access status to full release.

Soracom Query lets customers freely explore their IoT network and connection data to handle everything from isolating rogue SIMs to understanding underlying usage patterns. Instead of developing SQL queries manually, Soracom Query lets IoT network managers ask questions in natural language and generate data visualisations. Soracom Query is now available in general release, with options ranging from lightweight trial to full enterprise service including extensive BI tool integration.

News in Brief



Shankar Somasundaram,
Asimily

Asimily automates key defences against IoT device threats

Asimily has announced the release of several new features designed to help organisations across all industries efficiently secure and manage IoT devices while continuing down its path of cybersecurity innovation.

These features include IoT Password Management, IoT Patching and an intuitive new user interface designed for speed and efficiency. IoT Password Management simplifies the execution of password best practices across devices from multiple manufacturers. IoT Patching offers a 200% increase in supported manufacturers whose devices can now be automatically updated by Asimily.

"Organisations with device fleets have always struggled to keep them updated," said Shankar Somasundaram, the CEO of Asimily. "Unlike servers and operating systems, there is no streamlined process owned by the software manufacturer for IoT. This has always forced organisations to devote significant time and money to this essential line of defence."

Telefónica Tech expands its AI services by offering Perplexity

Telefónica Tech, Telefónica's digital business unit, is partnering with **Perplexity**, the AI-powered search engine that answers user queries in natural language and conversational format, to provide the Perplexity Enterprise Pro service to the business segment (B2B) in Spain.

Telefónica Tech is to offer the Perplexity Enterprise Pro service to business customers and complement it with its professional services to help customers implement it and get the most out of the tool. In addition, Telefónica Tech will offer a three-month pilot during the launch of the service for companies interested in trying it out.

An end-to-end, security-first approach to secure, scalable IoT deployments begins at the end

IoT organisations have matured, and the ecosystem has developed to support large, long-term, zero-touch device deployments. This has led to recognising the value of an end-to-end, full-stack approach with security by design.

Modern IoT organisations want to avoid the fragmentation and inflexibility of bespoke, highly customised first- and second-generation IoT platforms. They aim to bring products to market quickly with robust, adaptable solutions supported by a streamlined number of reliable suppliers.

Roy MacLean, the president of operations and transformation at Telit Cinterion, explains to George Malim, the managing editor of IoT Now, why the most efficient approach to deploying full-stack, end-to-end IoT systems is to begin at the end. This approach allows for greater flexibility for future changes. It encourages quick market entry with embedded security, pre-certified compliance and support for over-the-air upgrades ▶

SPONSORED INTERVIEW

COVER INTERVIEW

Roy MacLean
Telit Cinterion

George Malim: Why do so many IoT projects fail? Is this because of excessive complexity, continuing fragmentation, lack of security readiness or all three?

Roy MacLean: IoT projects often fail due to all three. These failures result from factors across cloud operations, data management and the need to harmonise across multiple systems and technologies. As complexity increases, failure is likely.

Telit Cinterion's solutions are designed to work together from the start. To reduce complexity, we use standard models. Our latest modules like the CMB100 series are optimised for rapid device prototyping. This also gives you a security-first design and means you can start with an end in mind.

The CMB100 series is Telit Cinterion's first generation of pre-certified LTE modules for end devices. The series is designed to simplify and accelerate product development.

These modules facilitate LTE Cat 4, Cat 1 bis and Cat M1. In addition, their unified form factor enables support for current LTE and future 5G technologies. They reduce development and certification costs and mitigate LTE product development risks. They also minimise redesigns and recertifications for radio changes and accelerate time to market.

Approvals include FC/IC in North America, RED/GCF in Europe, PTCRB in APAC and operator certifications for Verizon and AT&T.

GM: How can IoT organisations avoid common points of failure by selecting an end-to-end enabler that provides solutions that are secure by design?

RMcL: Partnering with a provider that understands the full IoT lifecycle enables companies to avoid ▶

Telit Cinterion's edge offering comprises a secure software stack integrated with our modules and cloud services

common pitfalls. An end-to-end enabler embeds and simplifies security. In Telit Cinterion's case, our device-to-cloud stack is a great example. It includes modules, edge integration, cloud and security, with no need for disparate vendors.

deviceWISE, powered by Telit Cinterion, is a scalable, integrated industrial business digitalisation platform. It gives customers visibility and control over all their connected devices and data. The platform collects and transforms data, integrating machines with business data.

deviceWISE EDGE features real-time data collection, transformation and business process integration. It enables predictive and preventative maintenance, as well as machine-to-machine process integration. The platform also handles event stream processing with anomaly detection and AI and machine learning (ML) integration.

When combined with deviceWISE EDGE, deviceWISE CLOUD delivers a complete IoT system and data management platform. It enables machine-as-a-service with data monetisation. To complete the portfolio, deviceWISE VIEW offers end-to-end, data-driven process visualisation with human-machine interface (HMI) and supervisory control and data acquisition (SCADA) in one package. This empowers identification of patterns and trends to derive operational insights.

GM: How important is it to address security at the solution design phase rather than as a retrofitted bolt-on? What vulnerabilities does not considering security early enough create?

RMcL: Doing bolt-on is a bad idea at any point in any project. Security retrofitting is risky and often ineffective. It's hard to cover all the holes you have created with this approach. Vulnerabilities are plain difficult to fix after deployment.

Common issues include unsecured communications channels, default credential management for unpatched firmware and an inability to authenticate or remotely update devices. These gaps open the door to data breaches, device hijacking and service disruptions.

Telit Cinterion modules like our recently released LE310 LTE Cat 1 bis industrial-grade module reduce costs because of its single antenna design. It's well suited for IoT use cases that need data transmission in the 10 Mbps downlink, 5 Mbps uplink range.

The module comes with built-in secure elements and support for a hardware-based root of trust. These are features that are only effective when planned from the get-go.

In addition, Telit Cinterion cloud services enforce policy-based access and secure provisioning. Early design decisions can prevent long-term exposure to security risks.

GM: What's needed to design IoT solutions that remain secure for long lifecycles in the field?

RMcL: I'll start by saying that almost all IoT deployments are long-term. There are very few that are short-term, so you need a strategy for how you're going to deal with that. Long-term security requires adaptability and thinking well beyond the initial deployment. You have to think five or 10 years out, and that's what you need to have in your mindset.

Among the items that should be on every checklist for IoT deployments with long-term lifecycles are things like hardware that supports secure elements or trusted execution environments. The software stack itself must be modular enough to adapt to the evolving security standards. The system also needs robust device and certificate management tools to handle credential rotation and decommissioning at scale. In some way, you'll want to do that as well.

Telit Cinterion's edge offering comprises a secure software stack integrated with our modules and cloud services. This simplifies IoT solution management as customer deployments scale. It supports firmware over-the-air updates, cryptographic identity management and lifecycle key relocation. All are essential to address foundational security requirements.

The software's device management tool allows for remote diagnostics and credential updates, ensuring that the device remains secure years after deployment. One lesson to keep in mind is to plan for change throughout the life of the product, not just at its introduction.

GM: IoT devices from smart meters to tracking sensors are often deployed for many years without any maintenance plans. How can IoT devices be built for this zero-touch environment and remain adaptable to accommodate changes in firmware, software and connectivity?

COVER INTERVIEW

RMcL: As you can imagine, you don't want to go out and touch every IoT device after you've deployed it. In many cases, you have them screwed to the sides of buildings in the middle of nowhere. That means you must have a zero-touch strategy, and zero-touch deployment demands economy and remote flexibility.

Devices should support over-the-air updates and features. These include firmware and security patches. They should also have embedded intelligence to handle local decision-making and reduce dependence on cloud interaction. IoT organisations need auto-provisioning for rapid hands-off onboarding. Future-proof connectivity modules can support feedback from networks. Various roaming modular software architectures allow for component-level updates but don't always address the full stack.

Embedded intelligence allows for local decision-making. Reducing cloud dependency starts with modular software and future-proof connectivity. Features such as multinetwork support demonstrate how devices can remain viable and secure. This is especially important in hand-off environments, where the majority of cases occur. If you look at Telit Cinterion modules, we support auto-provisioning and over-the-air updates. These enable devices to be deployed and maintained without physical access.

Modules like our recently launched AI-powered FE990D and FN990D 5G modules and data cards have been designed for next-generation connectivity. They can utilise AI to enhance traffic prioritisation, optimise energy efficiency, reduce latency and improve location accuracy.

Both product series support NB-IoT non-terrestrial networks (NTNs) for seamless satellite communication and align with 3GPP Release 18 for future-ready connectivity.

GM: What approaches are you seeing enterprises take to future-proof their IoT investments? How can they ensure long-term reliability and compliance without having to allow for costly field maintenance?

RMcL: You want to address all the elements of the stack. Most deployments go for eight or more years, and many remain active for beyond a decade. A lot of things change over 10 years, so you're in an environment in which you need a partner who can deal with those pieces and address the full stack.

That full stack includes the hardware, firmware, productivity tools, cloud integration and, of course, your data orchestration. You want a company that can be there and keep that stack working and support your entire product life cycle. This is the key to it.

It's also important to have a partner who's going to be around and understands how to do network evolution. Everybody who has had a cell phone knows that the networks change, that the environment changes. There's not a day that the networks aren't changing. When you look at all the networks around the world, there are always shifts.

There's an operating environment that sets out how everything works, encompassing the regulatory and security requirements. To ensure compliance and enable flexibility, you need a partner who's going to be there with you long term to make sure your full stack works. It's no easy task, and you want to have the right company. Telit Cinterion is a great company for that.

For the long term, the full stack needs to be considered, and security by design needs to be part of it. We use a lot of common application programme interfaces (APIs) and features that enable our modules to support multi-network options that avoid any vendor lock-out and ensure adaptability.

These are the kind of factors that you want to bring into play. It's all about choosing platforms that evolve with your business and the regulatory landscape, both of which change over time.

I think anybody in the business of managing a supply chain knows it's a lot better to pick your partner and make them work. Otherwise, you're accountable for making sure that the entire stack works yourself. It's easier to have a partner who lines everything up for you and has a track record of success.

It comes back to my earlier comment about not just planning for launch. The goal is to build a full-stack solution that will still meet your needs for five years or more. Long-term viability matters as much as short-term success.

It's also important to have a partner who's going to be around and understands how to do network evolution

www.telit.com

vitalthings®

Vitalthings provides contactless care for better outcomes

Fifty years ago, approximately 6% of the global population was 65 years old or older. Today, according to the World Bank Group, that number is between 19% and 23% in countries such as Denmark, Germany, Norway, Sweden and the United Kingdom. This longevity trend challenges healthcare providers, particularly in hospitals and skilled nursing facilities. The number of doctors and nurses isn't scaling at the same rate as the aging population, so technology needs to step up to address the gaps in care

Vitalthings created the Guardian M10 to meet the need for real-time monitoring

Hospitals need technology that provides continuous patient monitoring. This would allow staff to focus more on patients requiring emergency care.

Early deterioration detection and ICU transfer reduction

Vitalthings created the Guardian M10 to meet the need for real-time monitoring. It is the most precise contactless patient monitor to track respiratory rates and breathing patterns continuously. The Guardian M10 is available in a battery-powered, wheel-mounted version to detect deterioration early. This reduces costly complications and ICU transfers.

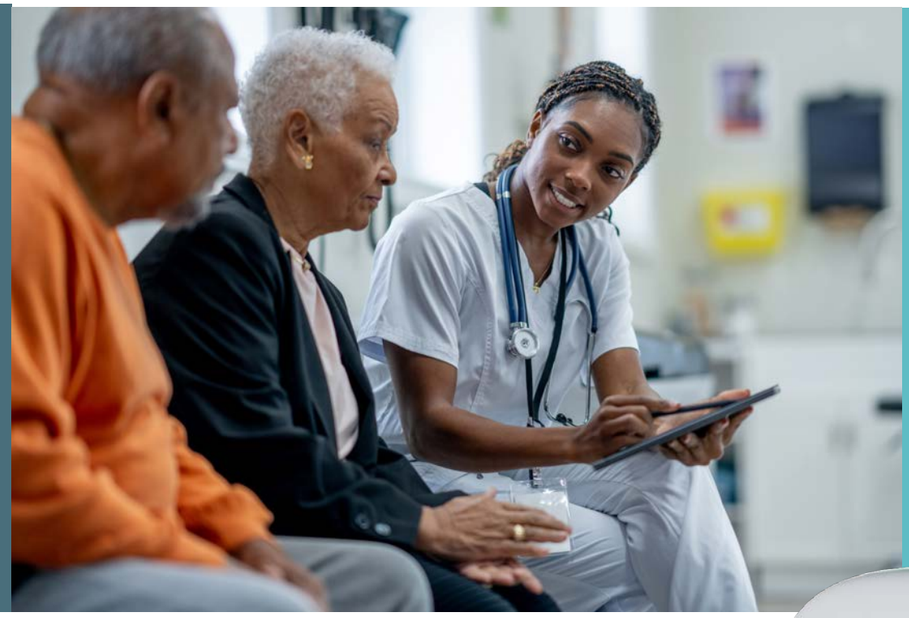
SPONSORED CASE STUDY

Research has shown that contactless health monitoring systems enable earlier transfers to lower-care units and keep patients safe. The Guardian M10 enhances the capacity to monitor more patients in standard wards in a safe way.
In February 2025, Vitalthings launched the Guardian H10. This updated monitor features the same technological platform as the M10. The Guardian H10 is currently not certified under the Medical Device Regulation (MDR). The device is technically configured for medical services; however, these functionalities will not be activated until MDR certification has been granted. The Guardian H10 is ideal for group care settings, such as nursing homes and home hospitals. It measures patient data, including:

- Breathing patterns
- Presence
- Unrest
- Sleep
- Environmental parameters

This information helps nurses and other caregivers provide proactive, early intervention and replace resource-demanding manual supervision.
The Guardian H10 also extends caregiving to patients' homes by utilising LTE. Three benefits of LTE connectivity are:

- Patients without Wi-Fi, cable or fibre can still use the patient monitor in their home through LTE ▶



"Providing health tech solutions at home can be a challenge"

- Faster and easier installation of the Guardian H10 relieves the caregiver from configuring the network

- Connected healthcare helps people remain in their homes longer, rather than having to move to an assisted living facility

Supporting patients' desires to age in place is a core objective for Vitalthings.

"Providing health-monitoring products and services in hospitals and institutions is very rewarding," says Ole-Johan Ellingsen, the co-founder and chief technology officer of Vitalthings. "With the Guardian H10, we are extending this to the home environment with the same quality of service. Setup and implementation will be easier than ever."

The Telit Cinterion advantage

The Guardian H10 uses a Telit Cinterion module from the xE910 family. The H10 also uses eSIMs and NExT, powered by Telit Cinterion. NExT is a secure mobile core network with turnkey connectivity and device management services.

"Providing health tech solutions at home can be a challenge," adds Ellingsen. "Thanks to Telit Cinterion, we have a solution to provide a wireless, unified connection for all patients. We have worked with Telit Cinterion on other projects and received recommendations from experts in the field, which made us choose Telit Cinterion as a partner. Telit Cinterion offers a complete package, including a worldwide mobile subscription."

Vitalthings partnered with Telit Cinterion due to the company's proven experience in mobile technology. For over 30 years, the company has delivered end-to-end hardware, service and connectivity plans for telehealth and other critical applications.

"When developing health technology, credibility and competence are crucial," concludes Ellingsen. "Telit Cinterion comes across as a trustworthy and safe choice. It's also practical to have the company as a partner. It's a one-stop shop with dedicated and service-minded staff." ■

www.telit.com

Andreas Morawietz
Giesecke+Devrient

SGP.32 has the power to transform IoT business cases with frictionless flexibility at scale

Andreas Morawietz is the global head of the eSIM & Solutions Portfolio at Giesecke+Devrient (G+D). With more than 24 years at G+D, he has held pivotal management positions, including leading global product management for eSIM technology and driving the company's product marketing initiatives. Since 2009, Morawietz has been a leading advocate for eSIM technology, playing a crucial role in advancing its adoption across machine-to-machine (M2M), Internet of Things (IoT) and the consumer markets. His work has been central to commercial remote eSIM management projects worldwide, strengthening G+D's position as a trusted partner to enterprises embracing digital transformation.

As SGP.32, the new made-for-IoT eSIM management specification, launches, George Malim, the managing editor of IoT Now, spoke to Morawietz to understand its likely impact and assess how transformational the specification will be for IoT devices and use cases ▶

SPONSORED INTERVIEW

George Malim: What's so important about SGP.32 - what does it enable for IoT devices and why is it better than SGP.02?

Andreas Morawietz: It's important to understand the history of innovation in embedded SIM (eSIM) management. Back in 2014, the M2M industry was working with SGP.02, a specification designed for a reasonable volume of M2M devices. This was developed to address well-controlled ecosystems such as smart metering or automotive, which involved lots of testing during design phases and therefore a longer lifecycle before a device came to market.

Devices used technologies including SMS as a communications channel to talk to the embedded universal integrated circuit card (eUICC) and data flows were limited to basic scheduled communications. Since then, the needs of IoT devices have become far more complex with widely varying data communication requirements. In addition, the velocity of IoT is far greater with devices needing to come to market rapidly and that well-controlled ecosystem fragmenting into a much faster development landscape.

In IoT, a clear need for a new specification to address different devices has emerged. We've seen that bypass the consumer specification SGP.22 from a volume perspective, with IoT expected to involve many more connected devices than consumer cellular. The GSMA therefore decided to look at what we can learn from SGP.22 for the much larger volume specification of SGP.32. Flexibility, simplicity and ease of use are priorities.

SGP.32 is so important because it provides a different approach, which is IoT device-centric. It starts with the devices, which are sometimes constrained – they can be network-constrained, power-constrained or user interface-constrained by intention – and the specification needs to accommodate this. Next, we needed a modern architecture that is more fitting for 5G than SGP.02, which was based on SMS or M2M communications protocols.

SGP.32 encompasses protocols for processing such as message queueing telemetry transport (MQTT), lightweight M2M (LwM2M), constrained application protocol (CoAP) and HTTP. These channels are established in IoT and the new specification works with them, which fits the needs of IoT.

A final aspect, which is especially important for G+D, is security. It's essential for everything we do in IoT and we see a much bigger challenge here than in consumer markets because IoT involves unmanned devices often in remote locations. There's nobody in front of the device to see an indicator, realise that something is going wrong or directly trigger a countermeasure.

SGP.32, with all these aspects in mind, modernises and adapts earlier specifications. Its development has involved listening to the needs of IoT solutions developers so a much more scalable solution can be created – with improved flexibility, ease of management and security.

GM: How does G+D see organisations adapting from force-fitting the SGP.22 consumer specification to their IoT devices to adopting SGP.32 as a made-for-IoT alternative? What new processes and management burdens need to be addressed to close the loop and enable frictionless eSIM activation?

AM: One of the industry norms is to embed a SIM into a device. In the consumer space, eSIM was delivered to the market as a standard in devices such as smartphones, notably with support from Apple and others. In IoT, a smart meter, for example, comes with a SIM embedded into the device, and it needs to be in the market for a very long period of time, withstanding extremes of heat and vibration. In theory and practice, nobody ▶

In IoT, a clear need for a new specification to address different devices has emerged

In SGP.22, G+D has provided its managing-DP+ to IoT players, which allows devices to be managed remotely but in the context of SGP.22

should need to visit that device during its lifetime, so the specification needs to reflect that type of use case.

However, the IoT market is not black or white, it's not IoT or consumer and many apps are in the grey zone in between. An example of this is an automotive use case. The connection in a car has two halves. One is for the consumer to enable it to connect and utilise services such as infotainment or navigation. The other is vehicle-centric and enables the car for safety communications (such as eCall) or to communicate with the manufacturer and dealer to optimise maintenance and perform updates.

The challenge is how to manage that optimally and deliver value both from a consumer perspective and for the IoT application. IoT, compared to consumer eSIM management, is different because a user can provide consent which can trigger an eSIM management event. IoT devices need to be managed without friction and critically, this needs to happen remotely with no physical interaction.

In SGP.22, G+D has provided its managing-DP+ to IoT players, which allows devices to be managed remotely (but in the context of SGP.22). We have brought these learnings in SM-DP+ to the GSMA working groups to define the SGP.32 specifications to enable remote management in the IoT context. One of the learnings is the need for the eSIM IoT Remote Manager (eIM) in an independent new service in addition to the SM-DP+. The ownership of the eIM is targeted at IoT OEMs or IoT service providers but can also be provided by connectivity service providers (CSPs) or MNOs.

This enables the device to interact with two key components: the SM-DP+ from the SGP.22 specification and, on the other hand, the eIM which fits the needs of the IoT industry. The eIM, in my view, closes the gap for remote management capability within IoT ecosystems.

With SGP.32, there is the capability for different players to own the eIM which is the trigger mechanism so they can acquire a new profile. We're combining a new process of management with eIM and fully utilising the security and processes of SGP.22. A well-defined API can seamlessly integrate the eIM into an existing legacy infrastructure of IoT players or service managers or use case owners, such as connectivity or device management services. Therefore, the eIM can integrate into the existing infrastructure of IoT players.

Beyond the SM-DP+ and the eIM, a third element is the software component at the device edge. This is the IoT profile assistant (IPA) and it can be deployed either on the device application layer (IPAd) or embedded into the OS of the eUICC (IPAe).

Each approach has advantages. The IPAe is suitable for low-end IoT constrained devices which have the lowest frequency of eSIM management events. The IPAd is normally designed for mid to high-end IoT devices which are non-stationary, such as trackers or vehicles. The remote connectivity management capability of IPAd driven devices allows for the active management of devices in the field to optimise cost, fulfil regulatory requirements or follow the use case demand.

GM: What trends are you seeing in relation to SGP.32? It's one thing to have a specification but another for it to be adopted and the benefits realised so how do you see the market maturing? ▶

AM: The benefit of SGP.32 is that both the GSMA specification and the services to enable it are available. By intensive testing, we have proved that the specification is ready so there's no need for IoT developers and designers to wait any longer. The work G+D has been involved in has encompassed writing the specification in parallel with building and developing the software and assessing early proof points to prove the specification we've defined fits the needs of the IoT industry.

Now, SGP.32 is really in the adoption phase among device makers, utilities and the industrial segment. When you think back to SGP.02, it was the automotive industry that understood the value of SGP.02 for its business model. Again, the automotive industry has been closely looking at SGP.32 for some time. Already, the first automotive manufacturers have adopted the technology and are integrating it into the next generation of products.

We also expect to see significant growth, especially from logistics, smart meter and automation companies. In the 6-18 month range, we will see deployments at industrial scale, not just in terms of companies adopting the specification but in terms of products shipping that utilise it. At G+D, we are already seeing many PoCs, MVPs, RFPs and RFQs and the volume of interest we are seeing in the energy and power markets suggests this kind of technology is enormously important.

Across the board, the standardised approach means it can be 10-12 weeks for an OEM to have a device designed, tested and ready to go to market. That's a substantial acceleration and simplification. SGP.32 helps to integrate connectivity management into new IoT device communications capabilities with new hardware, firmware and contractual frameworks.

It's not just a technical question that SGP.32 addresses, it's about integration and ensuring the whole ecosystem is ready. We're fully confident that this is the way to go to create a future-proof, frictionless, zero-touch solution.

GM: How does SGP.32 fit into the wider IoT ecosystem?

AM: When you look at the IoT industry, it has become a massive volume sector so cost is definitely an issue and cost optimisation is essential. To be in a position to say that with SGP.32, a device can have one variant to address the global market is a huge benefit for reducing total cost of ownership (TCO). This is really important to many IoT deployments, and we see this reduction enabling new IoT use cases on a wider scale.

I believe SGP.32 provides a strategic opportunity for OEMs and IoT service providers to position themselves in the overall value chain. The current value chain has a very sequential approach with modules, device and application development, on-demand manufacturing and software customisation driving handover of products between different providers. Connectivity management allows different players to add additional value to the product and that opens up opportunities to simplify and create new offerings. IoT will fly if it reduces complexity, so making a highly standardised way for all the players involved enables scalability to increase massively.

GM: How does G+D help to prepare for eSIM management in IoT?

AM: Our role here has multiple aspects, as we are the trusted and experienced partner for MNOs and the IoT industry. For many years we have been operating eSIM management services for MNOs around the globe. To date, we've delivered more than 500 million eSIM profiles and have strong relationships with a large number of OEMs, IoT service providers and MNOs.

Take that as a proof point that G+D is the most experienced player in the market to deliver eSIM profiles in a highly reliable and secure way to a wide variety of devices. Addressing and understanding the needs of different industries such as telecommunications and IoT has led us to create our AirOn360 product family. Within this seamless interworking family, we offer DP+ or eIM as a service, not only for customers directly but as a highly standardised, cloud-based eIM solution that is ready to cope with the highest volumes.

We focus on making eSIM management simple so the different IoT verticals can become eSIM enabled. For example, we hand over our IPAd reference code to customers so they can speed up the time to market for new devices. This makes it much easier for developers and we support them as an experienced partner on their journey.

Another important service required for IoT deployments is managing devices as well as managing connectivity along the full life cycle of devices. Our connectivity management platform, IoT Suite, offers a leading connectivity management service which seamlessly interacts with an eIM or legacy eSIM management services. This gives IoT players access to an intelligent device and connectivity management service with a single pane of glass for all devices. The AirOn360 family offering includes certified eUICCs, IPAd reference code, the eIM, Discovery service (DS), the IoT Suite and a large number of deployed AirOn360 RSP (DP+) services for MNOs, which allows IoT companies to be confident that they can download a profile from whichever MNO they choose.

IoT has strongly focused on SGP.32 but when we look a bit further ahead, the next step is to load the connectivity profile at the point of manufacture. This is covered in another GSMA specification (SGP.42), which is currently being defined. A key part of that is in-factory profile provisioning (IFPP) and this is where we see a really big need to seamlessly load connectivity in manufacturing environments into devices that are then shipped to the outside world. These devices will use SGP.32 technology to manage connectivity on the fly for the full device lifecycle. The telecommunications and IoT industry is at a very important point in time, as services based on SGP.32 play an essential role in enabling large scale IoT cellular connectivity from the cradle to the grave. And the best part - it just works. ■

Now, SGP.32 is really in the adoption phase among device makers, utilities and the industrial segment

https://www.gi-de.com/en/digital-security/connectivity-iot/iot

Giesecke+Devrient

Kaleido Intelligence

Mobilesquared
Decision ready data

MAJOR 2025 TRAVEL eSIM RESEARCH UPDATE

New Update for August 2025

New Strategic Insights

New “Travel eSIM Retail Market Outlook 2025" update featuring analysis of key market trends, developments, adoption & usage.

New Survey Insights

Based on responses from 5,000 travellers across 20 key markets, with new reports covering:

✓ The State of International Roaming in 2025
✓ Travel eSIM Usage & Preferences in 2025
✓ International Travel Intentions & Outlook 2025

Access All Research in the Complete Travel eSIM Package

✓ Market data for 115+ markets (2016–2030)
✓ Competitive analysis of 50+ vendors
✓ Insights from 5,000 travellers across 20 markets
✓ Insights from 100+ MNOs, MVNOs & Service Providers

ANALYST REPORT

The connectivity revolution is upon us, but how should connectivity leaders approach the market?

Kaleido Intelligence

Mobilesquared
Decision-ready data

Report sponsor:

flo. LIVE

Sponsored by:

flo. LIVE

The connectivity revolution is upon us, but how should connectivity leaders approach the market?

In Kaleido's recent H2 2025 survey, sponsored by floLIVE, of over 200 mobile network operators (MNOs) and connectivity service providers, it is evident that survey respondents are facing significant challenges in how to approach the market to deliver solutions to customers that need multi-regional if not global coverage while also remaining compliant, while at the same time ensuring a seamless, secure and reliable service

What do end customers require?

- **Solutions that mitigate risks associated with traditional roaming connectivity.** In this context, data sovereignty is important, as some markets require specific handling of IoT device data. Meanwhile, some markets prohibit permanent roaming at a regulatory level (such as Turkey) or on a wholesale agreement level (such as Australia). In an H2 2024 survey of enterprises and OEMs conducted by Kaleido, these issues were cited among the top five key concerns among respondents.

- **Performance needs are diverse and customers need solutions to be able to adapt to these.** High latency or low throughput capabilities, commonly associated with traditional roaming architectures, are not suited to a significant portion of IoT applications. Only 14% of survey respondents see roaming as applicable to more than 70% of use cases from a performance standpoint.

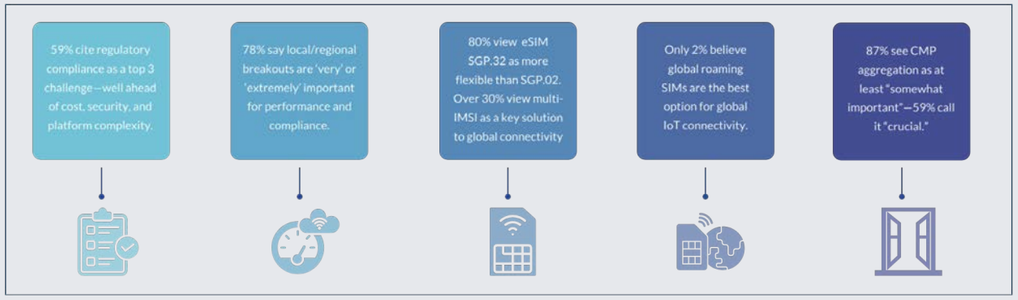
- **Global coverage is desirable, in a manner that is both seamless and reliable.** Survey respondents view this as the second most pressing challenge related to connectivity today.

Achieving this requires a very high level of flexibility on the part of the service provider. The ability to meet today's regulatory and customer requirements is not possible through a pure reliance on roaming agreements, which means that strategies must be adapted to remain competitive. ▶

Sponsored by:

flo. LIVE

Key survey results: summary



Source; Kaleido H2 2025 survey of 211 MNOs and Connectivity Service Providers

Kaleido Intelligence | Mobilesquared

What did we learn from the survey?

Global coverage is viewed as a key challenge by nearly half of all connectivity service providers. IoT has long been an internationally-focused market, with over half of all enterprise and OEM cellular IoT connections reported (in the aforementioned H2 2024 survey conducted by Kaleido) to require international connectivity support. For end customers, the need to scale IoT programmes globally has often required engaging with multiple service providers, which in turn realises complexity in terms of platform capabilities, service agreements and billing as well as diverse touchpoints and processes.

Infrastructure expansion and programmable SIM technology are core strategies

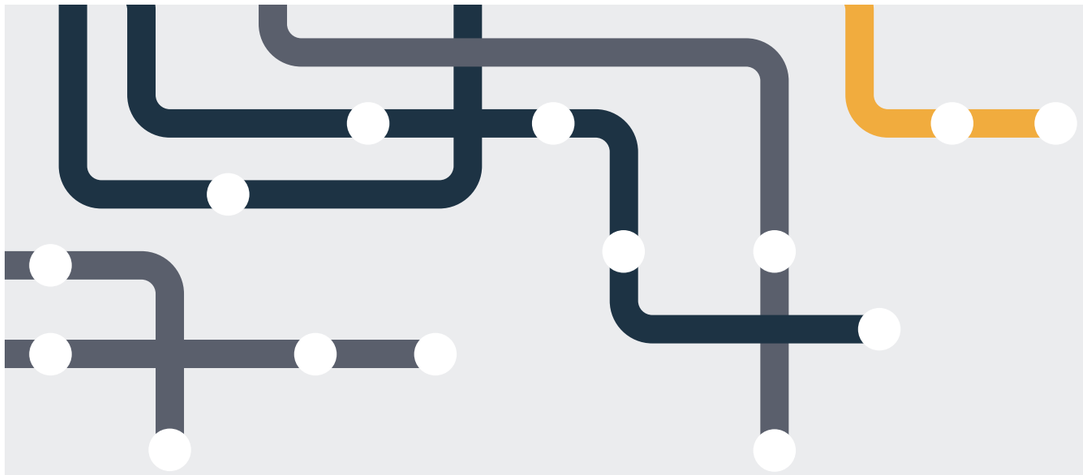
Today, SIM technology to remotely administer network access capabilities is available in the form of multiple international mobile subscriber identities (multi-IMSI) and embedded SIM (eSIM), which allow dynamic configuration of credentials over-the-air (OTA). The commercial release of eSIM's SGP.32 (IoT specification) during the latter portion of 2025 promises to add enhanced flexibility in how connectivity is provisioned and administered OTA by utilising the relative technical simplicity of the SGP.22 (the consumer specification) and combining it with the remote management paradigm that was utilised for SGP.02 (the M2M specification) eSIMs.

Here, nearly 80% of survey respondents view SGP.32 as more flexible than SGP.02 and, importantly, 61% believe the new specification will see coverage options for customers improve. Historically, support for SGP.02 among MNOs was roughly one-third that of SGP.22, which reduced the number of eSIM-based connectivity options for customers and made the technology difficult to scale. Connectivity service provider onboarding for SGP.32 is now much simpler than previously, while existing investments into SGP.22 can be used for SGP.32 use cases, reducing any perceived risk in ecosystem participation. We can thus infer that coverage options, from the standpoint of which network accesses will be available via eSIM, will indeed be greatly improved as the new eSIM specification matures on the market.

eSIM is not necessarily a panacea for the market, however. The technology will continue to generate friction in terms of elevated pricing versus legacy universal integrated circuit cards (UICCs), which is unavoidable due to the hardware. Meanwhile, an OEM selecting connectivity from a larger pool of providers than was previously possible means managing connectivity across multiple platforms. As ever, the market is shifting to reduce customer complexity in this regard, which will be explored shortly.

Ultimately, the loss of the business relationship with the customer is naturally a key concern for MNOs and connectivity service providers. Indeed, this is why the ability to extend coverage and meet compliance requirements in response to customer demand is so ▶

Sponsored by:



important. It is certainly the case that MNOs and service providers view connectivity break-outs, as well as multi-IMSI, as viable alternatives.

For example, 78% of the survey audience view local or regional break-outs as either very or extremely important to their organisation. The need for this type of infrastructure ties heavily into the increasing maturity of IoT projects. On the one hand, break-outs can aid in data sovereignty compliance by ensuring that payload traffic is routed within a specific country or region, rather than to the home network and back, as is the case in traditional roaming architectures. Meanwhile, the notion of breaking traffic out closer to the device offers obvious latency benefits compared to home-routed roaming, and means that more demanding IoT applications can be supported with the connectivity remaining as a first-party offering from the MNO. Thus, it is not surprising to see that more MNOs place a slightly higher importance on break-outs than non-MNO counterparts.

Around one-third of survey participants stated that multi-IMSI is an important technology to help achieve global coverage, with a surprising number of MNO respondents in favour of the technology. Traditionally eschewed by MNOs as a connectivity mechanism, the increasing acceptance of multi-IMSI among this cohort highlights how traditional walled-garden approaches are being eroded. Once again, customer relationship retention plays an important role here: the rise in shared infrastructure resources from telecoms service providers offering seamless access to off-footprint network resources, while allowing the primary serving operator to retain the billing relationship with the customer has been instrumental in this shift.

Rather than the static dual-IMSI approaches that might have been used in the past, access to a multitude of potentially accessible IMSI ranges means that OTA offers a rather dynamic solution to the connectivity problem. The proprietary nature of the technology in addition to the fact that some countries demand a fully-local solution, does mean that, in most cases, it is more appropriate to combine multi-IMSI with local break-out or eSIM to deliver compliance, better performance and flexibility.

No one-size-fits-all solution to optimising the deployment

The survey underlines the fact that several choices exist on the market today to deliver connectivity that is positioned to meet increasingly complex and stringent demands across various customer and regulatory environments. Perhaps what is less clear – although not surprisingly in the world of IoT – is that there is no one-size-fits-all solution for connectivity.

Local or regional break-outs are deployed as an extension of the serving operator's own network infrastructure and in most cases will use that operator's own network access agreements to support a global roaming initiative. Extending the network infrastructure footprint is no simple matter and requires a strong focus towards IoT if an in-house route is taken or a partnership with an appropriate third-party network-as-a-service provider. Meanwhile, 'roaming' is key here: while compliance may be achieved from a data sovereignty standpoint, markets that prohibit permanent roaming from a regulatory or commercial standpoint mean that static IoT devices cannot be deployed using a combined roaming-only and break-out model. Localisation in some fashion thus becomes an important consideration.

Multi-IMSI technology can serve as a mechanism for localised connectivity if appropriate ranges are available to the connectivity provider. This requires that the serving operator has made the necessary commercial agreements and technical integrations to access IMSIs, either via their own infrastructure or via a shared infrastructure concept provided by a third party. Nevertheless, multi-IMSI is not always compliant with local regulations, while it is not an industry-standard solution to connectivity.

eSIM offers a fully-compliant route to global connectivity, particularly when combined with multi-IMSI. By the end ▶

Sponsored by:

of 2025, commercial solutions will be on the market that greatly reduce the technical complexity associated with eSIM deployments for IoT use cases thus far, although in practice, eSIM retains a relatively high level of friction that will require innovative solutions to simplify. Most importantly, where eSIM from various providers is selected as the route to global connectivity, the multi-vendor sourcing challenges outlined at the beginning of this article rear their head once again.

Managed alone, a complex scenario of platform integrations and workflow processes arises which ultimately mean that scaling is extremely challenging. It is therefore not surprising to see a rising trend in the market for connectivity aggregation solutions, which allow customers to manage connectivity across a multitude of disparate management platforms via a single-pane-of-glass interface. Notably, 87% of survey respondents see this concept as at least somewhat important, while 59% view it as crucial.

As ever, maintaining a direct relationship with the end customer is of primary importance here, with billing and invoicing via a single point in addition to typical connectivity management and orchestration capabilities. It should be noted, however, given the various differences between connectivity management platform interfaces and capabilities, single-pane-of-glass aggregation solutions will support common denominators across integrated platforms, with more complicated functionality requiring direct access to the platform.

Each of the approaches discussed in this report are viewed as valuable according to Kaleido's survey results, with benefits and drawbacks dependent on the needs of both the end customer and the service provider. It is thus evident that ultimate flexibility is realised through a combination of these solutions. Indeed, a combination of local and regional break-outs alongside a combined multi-IMSI and eSIM solution delivers optimisation in terms of performance as well as compliance. While this approach may not always enable end-to-end delivery of connectivity via a serving operator, an important factor – the customer relationship – is retained. Perhaps most important of all is that new business, as well as ongoing opportunities are not missed as a result of a lack of performance or access capabilities. ■

About floLIVE

floLIVE designed and developed an elastic, robust core cellular infrastructure that is the largest connectivity infrastructure in the world. Through this powerful infrastructure, the company offers numerous services to mobile operators, IoT MVNOs and global enterprises seeking seamless, compliant, high performance and regulatory compliant connectivity, anywhere in the world.

With a global carrier library that is based on interconnected local core mobile networks, floLIVE ensures low latency, high performance and full compliance with privacy acts, data regulations and roaming restrictions. As of today, more than 20 mobile operators are on board the platform, giving companies multi-tier connectivity access.

Through direct access to our network, customers can monitor their devices, access real-time network events and usage, switch operators remotely, and troubleshoot failures ahead of time, providing a seamless experience that keeps devices connected at all times. Through one integration, one stock-keeping unit (SKU) and one platform, customers have a world of connectivity and endless possibilities. www.flolive.net

How connectivity and edge computing take smart homes to the next level

Sivaram Trikutam, the senior vice president of Wireless Products at Infineon, tells IoT Now how edge computing is making connected devices smarter. It's not just semantics. Edge computing enables devices to become more intelligent and 'thoughtful' when performing an action and this is all enabled by connectivity and edge computing. He also explains how AI fits into the smart home landscape

Sivaram Trikutam
Infineon

IoT Now: We hear the terms 'connected devices', 'smart devices' and 'smart homes' almost used interchangeably in different channels. Can you help explain the difference between these three, and how connectivity will play into this shift?

Sivaram Trikutam: Although all these terms are used interchangeably, there are some key differences between them. They all have one thing in common though – they are all connected to the internet. For the sake of simplicity, let's look at connected devices. They allow us to monitor and control our homes remotely, and to virtually manage our home. This makes our lives convenient and easier.

For example:

- With a doorbell that's connected to the internet, you could talk to someone at your door when you're not home using your smartphone.
- With a connected door lock, you could open a door for your child when she forgets to take her keys when she goes to school.
- With a connected thermostat, you can turn on the heat or air conditioning in your house before you leave from work so your house is at a comfortable temperature when you get home.
- With connected security cameras, you could check out the front yard or the backyard of your house if they detect some activity, just to make sure nobody is trying to get into the house.

Connectivity technologies play a major role in enabling these devices. Wi-Fi, Bluetooth and 15.4 are the most common technologies for such devices. Wi-Fi connects directly to access points and routers, while Bluetooth and 15.4 allow connection to the internet through an IoT gateway or a smart speaker. ▶

SPONSORED INTERVIEW

While we've been using Wi-Fi commonly with our smartphones, laptops, gaming controllers and myriad other devices for years now, these are mostly deployed in living room or bedroom use cases, which are typically closer to the Wi-Fi routers in living rooms or study areas. Connected home devices on the other hand are installed and used in all corners of our homes, on external walls, in backyards, in basements, in car garages, on roofs and other out of the way places. These need to provide robust, always-on, low-power connectivity in increasingly network-congested environments.

Smart devices are connected devices that do more than remote monitoring and control. They act on your behalf, make certain decisions for you and ultimately make life more convenient.

IoT Now: Can you expand on that? What makes these devices smart? Give us a few examples.

ST: The ability to anticipate your needs makes the smart device truly smart. Let's go back to the thermostat. In addition to being able to control the temperature remotely, it looks up the weather forecast from the internet and adjusts the temperature autonomously. It learns your preferences – how hot you like the temperature at night versus the day and takes care of that for you. It knows that your cost of electricity is based on the time of day, minimising the time it turns on heat when electricity is expensive. That's a smart thermostat. It's acting on your behalf.

A smart door lock or a video doorbell would recognise you and your family members and open the door automatically when you're at the door. Your garage door opener could recognise your car and open automatically when you get home.

A smart security camera could filter out situations that don't need your attention, like a tree branch moving on a windy day, your pet or a squirrel running past your house. It can also learn to recognise who your neighbors are, your postman's usual visiting hours, an Amazon delivery truck, and not alert you to these known events. It's adapting and using accumulated knowledge to make decisions.

Smart devices act on your behalf and do what you would do if you were paying full attention. These devices learn, adapt and use accumulated knowledge.

IoT Now: Ok, then what's a smart home? A house with many smart devices?

ST: Yes, but there's more to it than that. We need to think of broader functions in the context of a smart home. Let's consider a few examples. ▶

If we look at home security as a broad function, we'd like the system to take care of security as a whole

If we look at home security as a broad function, we'd like the system to take care of security as a whole. Make it easy and convenient for your family members to enter and leave the house but keep an eye out for intruders and act on your behalf without bothering you when there's nothing to be worried about. You might install security cameras, video doorbells, door locks, garage door openers, sensors to detect doors and windows being opened or closed or many other smart home devices. These could be connected devices that individually have some smart features. If all these devices collaborate with each other, exchange information and ultimately achieve an optimal security system for your home, that's a smart home function.

Let's consider energy management as a broad function – we'd like the system to optimise the overall energy consumption for the home. Control the temperature of the house throughout the day, across seasons, to what you and your family find most comfortable, with the knowledge of who's home at a specific time and where they are, whether it's in the living room watching TV or in the study working. It also uses the weather forecast to understand how much energy the solar panel on the roof will produce, it knows the energy price variation based on the time of day. The device uses all this knowledge to optimise the energy consumption for your home. This requires smart thermostats, connected air conditioning and heating systems, connected solar panels, battery storage systems, heat pumps, electric car chargers and so on, and a way for all of them to collaborate.

Similarly, we might think of 'health and hygiene' as a broad function to keep our homes clean, vacuuming when the floor is dirty and controlling cleaning functions accordingly. Lighting is also a broad function. And so the list of broad functions that make up a smart home goes on.

IoT Now: How are smart homes becoming a reality?

ST: It's an interesting evolution. First, we need all devices to be connected. Some of these are pretty common these days – thermostats, door locks, security cameras, lighting and vacuum cleaners. There are more that are getting connected, such as smoke detectors and appliances. This is enabled by robust, low-power, always-on, Wi-Fi, Bluetooth and 15.4 products that are optimised for such IoT use cases.

These devices are getting smarter by using intelligence powered from the cloud. This was enabled by adding additional sensors to these devices and transmitting locally generated data to the cloud and the rapid progress over the recent years of machine learning-based algorithms running on the cloud that added a layer of intelligence to these devices.

We are at the next stage of that evolution, with that intelligence moving to these smart devices – also known as intelligence at the edge of the network, rather than the cloud. This allows for faster response times, local learning and improved privacy and security by not having to transmit locally generated data to the cloud. This evolution is being enabled by microprocessors and low-power microcontrollers with ML capabilities at cost points that make it possible to bring this type of intelligence to the edge and for this to go mainstream. We are at the early stages of this evolution and poised for massive progress that'll happen in the next few years.

For these smart devices to talk to each other and collaborate, and achieve broad system level efficiency, we need additional layers of standards-based software protocols. The Matter standard is addressing this now, though it is still evolving. Many new device types are being defined by Matter each year, allowing standard interfaces and frameworks for devices to interact and collaborate.

IoT Now: You used the term intelligence at the edge. What exactly is edge computing and how is this making connected devices smarter?

ST: Most of us have used smart speakers at some point. When you ask one for today's weather forecast, the device captures the voice locally and sends it over to large datacentres in the cloud for processing, then it gets the 'answer' back and plays it out locally. As you can see, this adds quite a bit of latency, consumes additional power, and adds cost to use the cloud services.

Until recently, this was the only way to implement intelligence on these devices. With the recent developments in technology, it is now possible to do a lot of these actions locally without having to go to the cloud. This is enabled by edge computing devices that have the capability to run ML-based algorithms locally, at the edge of the network instead of in the core of the network. In addition to improving the latency and power consumption, it has the added benefit of privacy and security. Locally captured data doesn't leave the home, and it provides the ability for locally-optimised learning and adaptation.

IoT Now: What is Infineon doing in this space?

ST: Infineon is very committed to this space, and we offer a broad portfolio of industry-leading products that are relevant for this space. We offer our AIROC family of wireless products, the ▶ industry's best Wi-Fi and Bluetooth products optimised for IoT use cases – robust performance around and outside the home and ultra-low-power for always-on connectivity. We offer a gamut of high-quality sensors – mmWave radar, pressure, gas and magnetic sensors, MEMS microphones and others. More recently, we introduced our latest ML-optimised PSOC Edge family of low power microcontrollers that can be used for a variety of intelligence at the edge applications I talked about earlier. In addition to all this, we also offer our DEEPCRAFT Edge AI and software tools products that allow our customers to get their products from ideas to market much faster.

IoT Now: Any last comments for our readers?

ST: Yes. Infineon has three key messages:

a. The future of computing is at the edge and when you see a smart, connected device, it is likely to do its computing on the device - at the edge. Edge computing is making smarter devices a reality.

b. Infineon is a leader in decarbonisation and digitalisation and we are enabling designers to bring their designs faster-to-market with our semiconductor products and flexible software platforms including our ModusToolbox software and DEEPCRAFT, which enables an end-to-end workflow.

c. Connectivity is the enabler. Connecting devices to the internet allows us to make them smart. The software, microcontrollers and microprocessors that implement smarter functions are becoming more readily available. This combination of connectivity and intelligence will deliver the smart devices and smart homes of the future. ■

These devices are getting smarter by using intelligence powered from the cloud

www.infineon.com

MWC25 doubles down on Vegas for 5G, AI and IoT innovations

MWC25 Las Vegas once again returns to Nevada, USA, on 14-15 October 2025. This year, the event is taking place at the Fontainebleau Las Vegas and over two days will unite tech innovators, industry experts and policymakers to explore how companies can adapt to accelerating digital change and seize new opportunities – from unlocking growth through 5G and AI to shaping the future of cloud and IoT

Taking to the keynote stage will be the CEO of Verizon Business and CTIA chair Kyle Malady, CTIA president and CEO Ajit Pai and GSMA CMO Lara Dewar. These speakers will offer a macro view on the future of connectivity and enterprise transformation. In a dynamic panel to follow, Palantir CTO Jim Siders and Amit Zavery, the president, CPO and COO of ServiceNow, will be joined by other leading industry executives to examine how legacy systems are being reinvented for the digital age.

This year's agenda centres around three interconnected themes: Connected Industries, AI+ and Connected Enablers. Through these themes, the event will examine how enterprises are ▶

This year's MWC will take place at a new, luxury venue, the Fontainebleau Las Vegas, bringing with it a refined focus on real thought leadership, real challenges and real-world applications

modernising critical infrastructure, deploying AI responsibly and powering more resilient enterprise transformation across sectors.

Alongside confirmed sponsors and partners – including Boldyn Networks, JMA Wireless, Intel, Iridium, Qualcomm and Valid – other recently announced speakers include:

- Automation Anywhere CEO, **Mihir Shukla**
- Box CTO, **Ben Kus**
- IBM Global head of Venture Capital, **Emily Fontaine**
- Former Scale AI Field CTO, **Vijay Karunamurthy**
- Nutanix chief AI officer, **Debo Dutta**
- Ritual CEO and co-founder, **Atif Rafiq**
- SoundHound AI CIO, **Shawnna Delhierro**

Across keynotes, summits, panels and curated networking, MWC Las Vegas will spotlight and provide practical solutions to the challenges that matter most to CIOs and tech leaders – from scaling up AI to managing infrastructure complexity – anchored by an agenda meticulously designed to connect leaders and accelerate industry-defining collaborations.

As the demands on enterprise tech leaders continue to intensify – driven by rapid AI adoption, growing infrastructure complexity, and persistent cybersecurity challenges – so too does the need for more actionable insight and meaningful thought leadership grounded in real-life application.

Put simply, today's tech leaders aren't just looking for inspiration; they're seeking the kind of expertise, content and networking that helps them make smarter decisions, faster and at scale. MWC25 Las Vegas, delivered in partnership with CTIA, meets this pressing need head-on. As the GSMA's flagship North American event, it brings together the voices that matter most in enterprise connectivity, all in one place – offering focused, executive-level content designed specifically for CIOs and senior IT decision-makers navigating the current era of transformation.

A conference built for CIOs

This year's MWC will take place at a new, luxury venue, the Fontainebleau Las Vegas, bringing with it a refined focus on real thought leadership, real challenges and real-world applications. Built around two days of curated keynotes, summits, and networking, MWC25 Las Vegas is meticulously tailored to the evolving needs of the North American enterprise ecosystem. ▶

At the core of MWC25 Las Vegas is a bespoke agenda that spotlights the CIO's strategic role in enterprise transformation

At the core of MWC25 Las Vegas is a bespoke agenda that spotlights the CIO's strategic role in enterprise transformation. Attendees can expect first-hand insights from leaders behind the scenes of some of the world's most complex, innovative, and, most importantly, successful IT infrastructures, with representatives from Boldyn, IBM, Intel, JMA Wireless, Palantir Technologies, Qualcomm, ServiceNow, T-Mobile and Vodafone all due to attend.

2025 themes: From tech vision to execution

This year's packed agenda will explore enterprise connectivity through three interconnected themes:

- **Connected Industries:** Dive into how 5G, IoT and automation are reinventing sectors like manufacturing, logistics and government services. Case studies from leading adopters will demonstrate how industrial-grade connectivity is turning ambition into operational change. Highlights include keynote sessions from CTIA CEO Ajit Pai, CTIA chair Kyle Malady and the GSMA's very own CMO Lara Dewar – followed by a panel of tech leaders, including Jim Siders, Palantir CTO, Amit Zavery, ServiceNow president and former McDonald's CDO and Ritual CEO and co-founder Atif Rafiq, unpacking how legacy infrastructure is being transformed in real-time.
- **AI+:** Explore how generative and agentic AI models are reshaping IT architecture, workforce productivity and service delivery. These sessions go beyond the hype – focusing on ethical integration, measurable outcomes and sustainable AI deployment. Attendees will hear directly from AI leaders at Box, Deloitte, Scale AI and Qualcomm, discussing how enterprises can move from experimentation to scalable deployment. The event also features an expert panel offering practical playbooks for thriving in the AI era.
- **Connected Enablers:** No transformation happens in isolation. Learn how edge computing, network APIs, cloud-native infrastructure and security are driving scalable innovation across enterprises. Keynotes will explore how to build intelligent and resilient enterprise, with senior leaders from Automation Anywhere, IBM and Serve Robotics discussing how CIOs are making smart capital investments while deploying intelligent automation to build more adaptable operations. ▶

North America's connectivity landscape is advancing fast and CIOs sit firmly at the helm. MWC25 Las Vegas is the place where enterprise technology leadership meets execution

Spotlight summits

At MWC25 Las Vegas, attendees can look forward to new and returning summits, including:

- **CIO Summit:** A dedicated stage for CIOs to exchange lessons learned and navigate shared priorities.
- **Smart Aviation Summit:** Industry-specific forums on connectivity in high-stakes environments to support a new era of intelligent airport/airline operations and passenger experiences.
- **Agentic AI Summit:** Discover how telcos and enterprises are using autonomous AI agents to drive network intelligence, service personalisation and operational efficiency.
- **Satellite & NTN Summit:** Examine how mobile operator and satellite ecosystems are converging to expand connectivity – covering spectrum strategies, direct-to-device innovation, global roaming and IoT at scale.
- **Private Wireless Networks Summit:** Dive into real-world private 5G deployments across manufacturing, logistics, healthcare and government, exploring best practices in security, latency control, network slicing and enterprise integration.

Turning innovation into action

North America's connectivity landscape is advancing fast and CIOs sit firmly at the helm. MWC25 Las Vegas is the place where enterprise technology leadership meets execution. Attend the event to explore what's next, make the right connections, and take ideas from concept to company-wide deployment.

Register at **www.mwclasvegas.com** to be part of the conversations shaping connectivity across North America.

From shared ambition to collaborative action – building the digital backbone of the energy transition

The energy sector is at a pivotal moment. On one side lies the urgent imperative to decarbonise in response to climate change. On the other, a wave of technological innovation in IoT, AI, digital platforms and sensors offers tools that can reshape energy systems into something cleaner, smarter and more resilient. The convergence of these forces is not an abstract concept; it is happening in real-time, across Europe and the world

This is why the conversation around energy is no longer confined to engineers or policymakers. It belongs equally to technologists, data scientists, innovators, utilities, regulators and citizens. And it's why 15,000 energy professionals will come together in Bilbao, Spain this November for Enlit Europe 2025, a meeting point where ambition turns into collaboration and collaboration into action. The event will unite more than 700 exhibitors and 500 speakers to share insights and shape the digital backbone of the energy transition.

This event happens at a strategic moment as the industry faces the urgent need for these conversations to happen. Topics include: what is happening in the energy sector today that makes such a convergence so necessary? The answer lies in how digitalisation, AI and system resiliency are redefining the way we power our world.

Digitalisation is the new grid stability tool

Energy systems were historically designed for predictability with centralised fossil-fuel plants, steady demand and linear flows. That paradigm has shattered. With renewable generation, electric vehicles and distributed resources now central to Europe's mix, stability depends on something new: intelligence.

Here, IoT acts as the digital nervous system of energy infrastructure. Sensors in substations, turbines, EV chargers and industrial processes feed vast datasets that can be analysed in real-time. These insights make it possible to forecast renewable output, balance demand and optimise grid operation in ways that would have been unthinkable just a decade ago.

For example, smart meters, once seen as billing tools, are becoming pivotal enablers of demand-side flexibility. By giving households and operators real-time visibility, they allow for a more dynamic, participatory model of grid stability. This shift demonstrates how digitalisation directly supports decarbonisation, while also lowering consumer costs and empowering prosumers.

This shift will be explored in detail at the Digitalisation Hub, with sessions such as Smart Metering & Data Management on second-generation metering and flexibility, and Software Defined Power, which looks at how software and digital twins can enhance the reliability of transmission and distribution networks. The Basque Country Focus: Advanced Digital Tools for a Robust Power Grid session will also highlight innovative regional projects. ▶

AI to turn data into decisions

Sensors alone don't create value, AI does. The energy transition generates torrents of data, far too much for humans to process. Machine learning models are now being deployed to forecast demand spikes, detect faults before they cascade and optimise integration of distributed renewables.

Importantly, AI is not replacing human judgment; it is enhancing it. Grid operators, market traders and policymakers are using AI-generated insights to make faster, better-informed decisions. The question of trust is central here: trust that an algorithm can detect anomalies without bias, trust that personal data from smart devices remains secure and trust that AI supports human oversight rather than undermining it.

One Summit session, AI for Energy, Energy for AI, will tackle the growing paradox that while AI helps manage the energy transition, it also drives soaring power demand from data centres. And at the AI Hub, the topic will be further explored with sessions like AI in Practice, which share real-world use cases in grid prediction, energy management, consumer behaviour and disaster response. The AI in Other Industries session will provide lessons from sectors such as automotive and banking that can be adapted to energy. These conversations connect technical innovation with social responsibility.

Cybersecurity is the silent battlefront

Digitalisation also brings risk. Every sensor, every connected asset, every cloud platform expands the attack surface. The past few years have shown the consequences with attempted intrusions into power systems, ransomware affecting utilities and the constant probing of critical infrastructure.

Cybersecurity in energy is now as fundamental as physical security. The convergence of IT and OT requires adaptive, layered defences where AI-driven anomaly detection complements traditional firewalls and where resilience planning assumes that attacks will happen. The ability to detect, contain and recover quickly is becoming a core competency for modern utilities.

At the Summit, the session Grids: Security, Resiliency and Adaptation will bring together experts to discuss how to strengthen Europe's grid security and build systems that can withstand both physical and cyber disruptions. Complementing this, the Digitalisation Hub will also feature discussions on building cybersecurity into distributed systems.

Sensors, sustainability and smarter use of resources

The climate challenge isn't just about generating cleaner energy. It's about using it better. Here, IoT and sensors are proving indispensable. In energy-intensive industries like steel, cement and chemicals, sensors now track emissions in real-time, enabling operators to adjust processes on the fly. In cities, connected infrastructure such as streetlights, EV charging and district heating turns urban areas into living laboratories of efficiency.

This is where ambition meets practicality. Every avoided kilowatt-hour, every reduced tonne of CO_2, is the result of systems that are not only greener but smarter.

These topics will feature strongly in the Decarbonisation Hub, including sessions on industrial energy efficiency and real-time monitoring of carbon capture performance. They show how IoT-enabled systems are moving from pilots to scaled deployments, driving measurable progress towards net zero.

Collaboration on the human side of the transition

Perhaps the most profound truth is that no single actor can achieve the energy transition alone. Utilities need technology providers. Start-ups need policymakers. Cities need industry partners and all of them need trust from citizens.
That is why gatherings where these different communities intersect are so important. They are not about showcasing products or branding; they are about accelerating the conversations and collaborations that turn shared ambition into collaborative action.

Enlit Europe reflects this collaborative spirit. Cross-sector panels such as Securing Europe's Competitiveness in the Energy Transition bring together utilities, regulators and technology firms. Meanwhile, the AI & Digital Hub will host workshops where start-ups and corporates co-develop solutions, embodying the collaborative ethos the sector desperately needs.

Another important example is the Think Tank Workshop: What do we need to do to create greater energy system resiliency?, held on the third day of the Summit. This is where top leaders convene to co-create approaches to the most urgent challenges. From these discussions, the annual Enlit Report emerges, capturing both insights and actionable strategies. This year, the Think Tank's focus on System Resiliency underscores the need for collaboration to safeguard energy systems against climate shocks, cyber risks and geopolitical disruptions.

Why you should join the conversation

The energy transition is not theoretical. It is unfolding now and its success depends on how effectively technology, policy and human collaboration come together. Platforms like Enlit Europe matter because they create the space where these conversations turn into partnerships and partnerships turn into action.

In Bilbao this November, more than 15,000 energy professionals, 700 exhibitors and 500 speakers will gather to exchange insights, showcase solutions and tackle the challenges shaping our collective future. Whether your expertise is in IoT, AI, cybersecurity, system integration or decarbonisation, this is where your work connects with the broader mission of building resilient, sustainable energy systems.

Enlit Europe is not just about ambition. It is about action. It is about shaping strategies that respond to climate change, designing systems that withstand disruption and ensuring that technology serves people as much as the planet. ■

Attend Enlit Europe 2025

- **Bilbao, Spain**
- **18–20 November 2025**
- **15,000+ Attendees | 700+ Exhibitors | 500+ Speakers**
- **Theme:** From Shared Ambition to Collaborative Action

Register now

Our pick of the IoT industry's upcoming events

The Things Conference
23-24 September 2025
Amsterdam, The Netherlands
https://www.iot-now.com/event/the-things-conference-2/

Edge Computing Expo
24-25 September 2025
Amsterdam, The Netherlands
https://www.iot-now.com/event/edge-computing-expo-europe-2025/

Connected Britain
24-25 September 2025
London, UK
https://www.iot-now.com/event/connected-britain-2025/

IoT Tech Expo Europe
24-25 September 2025
Amsterdam, The Netherlands
https://www.iot-now.com/event/iot-tech-expo-europe/

IoT Days Fall: 5G Networks
24-25 September 2025
Online Event
https://www.iot-now.com/event/iot-days-fall-5g-networks/

International Cyber Expo
30 September – 1 October 2025
London, UK
https://www.iot-now.com/event/international-cyber-expo/#

Automa 2025
13-14 October 2025
Amsterdam, The Netherlands
https://www.iot-now.com/event/automa-2025/

MWC25 Las Vegas
14-15 October 2025
Las Vegas, Nevada, USA
https://www.iot-now.com/event/mwc25-las-vegas/

Network X 2025
14-16 October 2025
Paris, France
https://www.iot-now.com/event/network-x-2025/

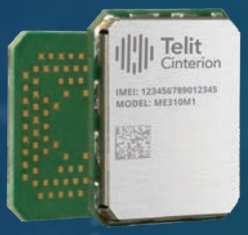
11th Global Edition of Gen AI & HyperAutomation in Finance Summit
16 October 2025
Chicago, Illinois, USA
https://www.iot-now.com/event/11th-global-edition-of-gen-ai-hyperautomation-in-finance-summit/

Telit Cinterion

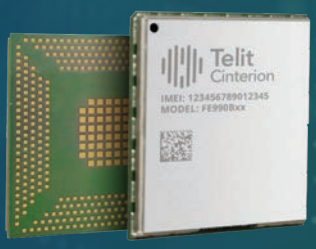
Scale Faster. Connect Globally. Remain Secure.

Regional to Global IoT—Powered by NExT™ SIMs and Cellular Modules

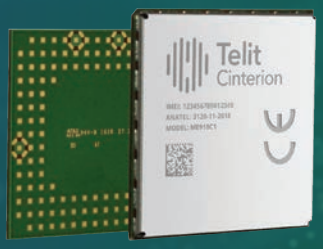
LE910C4 Linux



ME310M1



FE990B



ME910

NEXT™

From mission-critical reliability to global coverage and embedded intelligence, our award-winning modules paired with our trusted connectivity deliver performance without compromise.

Request a Kit