IoT Now: ISSN 2397-2793

2024 • VOLUME 14 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

TRANSFORMA INSIGHTS UNPICKS PERMANENT ROAMING RESOLUTIONS

COVER INTERVIEW

Sparkle and floLIVE collaborate on sophisticated, global IoT connectivity

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

CONNECTIVITY
Why utilities select cellular for smart metering
Read the IoT Now report at www.iot-now.com

TRANSPORT
Expanded use cases and new connectivity needs explained in our Analyst Report inside

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

PLUS: 5-PAGE MARKET REVIEW EXPLAINS MASSIVE IoT IMPACTS • Why it's time for SIMPL IoT connectivity • What IFPP means for streamlined SIM integration • Qualcomm buys Sequans 4G IoT technology • China targets 3.6 billion mobile IoT connections by 2027 • Why cellular networks and IoT have a SIMbiotic relationship • Swisscom Broadcast and Nokia take off with drones-as-a-service • How MobileWare's Darby platform is supporting vertical IoT • eUICC unlocks future agriculture apps • Do all roads lead to roaming? • Trasna CEO details cloud-based eSIM deployments • See the latest News, Features and Interviews at www.iot-now.com

TRANSFORMA INSIGHTS

Global Advisors on IoT, AI and Digital Transformation

Transforma Insights can increase your revenue, reduce your costs, and limit your exposure to risk

How?

We're glad you asked...

Our white papers, webinars and other marketing support will expand your lead pipeline

Every company's top priority is selling. We can support by building your profile and feeding the sales funnel. In the last 12 months we have supported connectivity providers, platform vendors, hardware makers and many others in promoting their products and services to would-be customers through tailored white papers, events, webinars and more.

Our deep knowledge of the vendor community can ensure you pick the right suppliers who can deliver what you need

Our regular immersive benchmarking reports in IoT, AI and other emerging techs are used by clients to select the right vendor for them. We also undertake numerous client-specific vendor selection engagements, including recent projects supporting an industrial equipment maker select an IIoT platform and an auto vendor to choose a connectivity provider.

Our understanding of market dynamics means we are the best placed to advise on potential M&A, helping you make the right decisions

Bad M&A decisions can have the most serious repercussions. Our understanding of the companies, technologies and markets puts us in pole position in vendor selection and technical/commercial due diligence. We regularly work supporting Private Equity due diligence, and technology vendor acquisition target identification and rating.

Our ultra-granular IoT and AI market forecasts ensure that you're pursuing the right opportunities

Transforma Insights provides the most granular market forecasts across our technology markets, particularly in IoT and AI. Our country-by-country forecasts include detailed technology splits and use-case level granularity. If you want to identify the right markets to pursue, set company priorities, or just set sales targets, they are an invaluable resource.

Our tracking of the complexities of the rapidly evolving regulatory environment mean your risks are mitigated

Regulation is fast-moving today and mis-steps could have catastrophic implications. Our new Regulatory Database helps enterprises and technology vendors navigate through the increasingly complex regulatory environments associated with enterprise digital transformation, including related to Artificial Intelligence, Internet of Things, Data Sharing and Privacy.

Sign up to your free 'Essential' subscription to explore our research at: transformainsights.com/signup/essential

transformainsights.com enquiries@transformainsights.com @transformatweet

08 COVER INTERVIEW

17 ANALYST REPORT

38 CASE STUDY

67 IFPP INTERVIEW

IN THIS ISSUE

04 EDITOR'S COMMENT
George Malim on SIMbiotic relationships

05 COMPANY NEWS
Qualcomm snaps up Sequans 4G tech, Memfault joins STMicroelectronics partner programme

06 MARKET NEWS
China targets 3.6 billion mobile IoT connections, Oracle integrates AT&T IoT connectivity into enterprise communications platform

08 COVER INTERVIEW
Sparkle's Daniele Mancuso and floLIVE's Luigi Capoblanco detail their collaboration to support sophisticated, global IoT connectivity

12 CASE STUDY
MobileWare turns to floLIVE for Darby platform connectivity

14 CONNECTIVITY MANAGEMENT
Why IoT organisations are selecting connectivity management platforms (CMPs) to simplify and streamline management of device connections

17 ANALYST REPORT
ABI Research's Elizabeth Stokes and Dan Shey uncover the future of fleet management, detailing expanded use cases and connectivity requirements

28 ANALYST RESEARCH
Global satellite coverage supports IoT anywhere, writes Beecham Research's Sarah Woon

31 The IoT Now CEO Guide to Mitigating Roaming Risks

32 INTERVIEW
Ryan Keefe, the chief operating officer of SIMPL, tells Transforma Insights' Matt Hatton that it's now time to keep IoT connectivity SIMPL

36 MULTI-CARRIER MANAGEMENT
How SIMPL is revolutionising IoT and fixed wireless access deployments

38 CASE STUDY
Agribusiness is accessing new use cases with eUICC and SIMPL

40 PERMANENT ROAMING
Transforma Insights demystifies the resolution of permanent roaming regulatory issues

44 SECURE ROAMING
Antony Savvas assesses how modern SIM platforms are supporting cloud-connected IoT devices

46 IoT ROAMING CONNECTIONS
How IoT roaming is driving new revenue for mobile network operators

49 INTERVIEW
Nick Gyles, the chief product officer at Daizy, tells George Malim how hyperscale IoT can benefit from an open, horizontal management toolset

51 CONNECTIVITY WEB SUMMIT 2024
Our preview of this year's event

53 The IoT Now Guide to Cloud-Based eSIM 2024

54 INTERVIEW
Stéphane Fund, the CEO of Trasna, details how the company is addressing the demands of the IoT market, following its acquisition of Workz

58 CASE STUDIES
The latest deployments from iONLINE, 1oT, Monogoto and Virgin Mobile MEA

63 eSIM
Antony Savvas asks if the jury is still out on how eSIM uptake will increase?

67 The IoT Now CEO Guide to IFPP 2024

68 INTERVIEW
Dr. Philipp Schulte, the CEO of Giesecke+Devrient Mobile Security, tells George Malim how in-factory profile provisioning (IFPP) is transforming device manufacture

72 IFPP EXPLAINED
With IFPP, simplicity starts from the factory floor

74 CASE STUDY
How IFPP enabled by G+D's AirOn360 In-Factory SIM is revolutionising device connectivity

76 IFPP ANALYST VIEW
Transforma Insights' Matt Hatton explains why IFPP is useful for connected device makers

78 IFPP BENEFITS
Antony Savvas looks at how IFPP will be applied to use cases such as smart energy meters and remote logistics

81 MARKET REVIEW
Why massive IoT necessitates new models, new technologies and new relationships

87 INTRALOGISTICS
Suruchi Dhingra, a research director at Transforma Insights, explores the digital technologies that are being deployed to optimise intralogistics

90 EVENT DIARY
Where to go and what to see

The relationship between IoT and cellular connectivity is SIMbiotic

IoT has always relied on cellular connectivity to provide wire-free, secure, ubiquitous coverage to support IoT use cases. The technology is ideal for the needs of IoT devices but connecting to cellular networks has always been complex, fragmented and inflexible. This puts IoT in a chicken-and-egg situation in which complicated connectivity requirements slow time to market and impede growth

George Malim,
managing editor

The arrival of the massive IoT era has put immense pressure on the current situation as it has become increasingly recognised that current SIM regimes are a barrier to introduction of new use cases and hyperscale growth in others. This isn't news, though. The marketplace has been struggling to simplify the SIM situation for almost a decade, riding on innovations such as embedded SIM (eSIM) and, more recently, integrated SIM (iSIM).

The promise these technologies have, in terms of enabling SIM functions to be installed into devices at the point of manufacture before connecting to a mobile operator at the point of deployment, provides a glimpse of a simplified future. Ideally, a device should be turned on and automatically connect to the optimum available connectivity. Today, that's a step too far and vested interests, existing contractual obligations and even the regulatory environment exert a range of sophisticated pressures on IoT organisations.

Managing global connectivity is still complex, although connectivity management platforms have been developed to abstract much of the burden away from organisations that deploy IoT offerings. Flexibility is also not uniformly possible with much depending on commercial agreements, operator and regulator policies, and full awareness of the options continuing to elude much of the market place.

The virtuous circle of simple to access, global connectivity fuelling increased volumes of connected devices has substantial bottlenecks that new SIM technologies can ease. This faster, easier, more efficient and ultimately simpler to change SIM landscape matches the developmental priorities of IoT devices. The two are symbiotic and the more the alignment is recognised the more that easy connectivity will fuel uptake of IoT offerings and foster innovation that brings huge hyperscale use cases to life.

It's time for IoT organisations to embrace the SIM revolution and stimulate deployments with simple cellular connectivity.

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
Ark Design
Tel: +44 (0) 1787 881623

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

Qualcomm to acquire Sequans' 4G IoT technologies in new deal

Qualcomm and **Sequans Communications** have entered into a definitive agreement for Qualcomm to buy Sequans' 4G IoT technologies. The acquisition includes certain employees, assets and licences. The transaction is subject to customary closing conditions, including French regulatory approval.

Sequans is a designer, developer and supplier of cellular semiconductor solutions for massive and critical IoT markets. The addition of Sequans' 4G IoT technologies to Qualcomm's IoT solutions will strengthen Qualcomm's Industrial IoT portfolio.

"Digital transformation is being driven by high-performance processing and intelligence at the edge, positioning Qualcomm for growth in one of the largest addressable opportunities," said Nakul Duggal, the group general manager, automotive, industrial and embedded IoT, and cloud computing at Qualcomm Technologies. "This acquisition of Sequans' 4G IoT technology adds to Qualcomm's broad portfolio, further strengthening our offerings across enterprise customers of low-power solutions for reliable, optimised cellular connectivity for Industrial IoT applications."

Sequans will retain full rights to continue to use the technology commercially, via a

Georges Karam, Sequans

perpetual licence agreement, supporting the company's ability to expand its 4G business and develop its 5G portfolio.

"We are excited to announce this important transaction with Qualcomm," said Georges Karam, the CEO of Sequans. "This agreement underscores the value of our 4G IoT technology and provides us with significant capital to continue to further invest in our IoT business ambitions. We are dedicated to pushing the boundaries of innovation and providing cutting-edge 4G/5G semiconductor solutions that meet the advancing needs of AI-powered Internet of Things applications. This transaction is expected to provide us the resources and flexibility to enhance our product offerings and expand our market presence."

Memfault joins STMicroelectronics partner programme to accelerate customer time-to-market

Memfault, a provider of an embedded device observability and over-the-air (OTA) platform, has announced that it has joined the ST Partner Programme, allowing **STMicroelectronics** customers that develop embedded IoT devices to gain visibility into device performance and reliability, proactively identify issues and quickly push targeted fixes out to devices.

Memfault equips engineering and product teams with critical insights into real-world product performance, such as firmware stability, battery life and connectivity. Its automatic diagnostic data extraction, aggregation, analysis and notification capabilities improve issue detection and shorten resolution time from days to minutes, the company claims.

"Memfault's extensive experience and specialised tools uniquely position us to support STMicroelectronics' customers right from the start," said François Baldassari, the CEO of Memfault. "Our solution supports embedded engineers and developers in remotely debugging issues, deploying OTA firmware updates and continuously monitoring fleets of connected devices at scale, enabling them to make better products faster. This capability extends throughout the entire product lifecycle, from initial development to deployment."

Memfault works closely with multiple ST customers and can support any IoT device configuration. Memfault has a well-established integration with STM32 chips that is currently being used by many customers around the world.

François Baldassari, Memfault

News in Brief

Deutsche Telekom IoT joins Bridge Alliance

Deutsche Telekom IoT has joined **Bridge Alliance**, a business alliance of 35 mobile communications companies in Asia Pacific (APAC), the Middle East, Africa and now Europe. Bridge Alliance provides connectivity and integrated value-added services, including IoT/M2M, to its members. The cooperation claims to open the 'greatest possible flexibility' for both sides to meet individual customer requirements in an international environment.

Deutsche Telekom, through its Deutsche Telekom IoT subsidiary, is the first European telecoms company in the alliance. Its IoT subsidiary is part of the business customer activities within T Business. By joining the alliance, Deutsche Telekom can now offer global companies easy access to the APAC region.

Sateliot launches four satellites for IoT connectivity

Sateliot has successfully launched four additional satellites as part of its 5G narrowband-IoT (NB-IoT) non-terrestrial network (NTN) constellation. These satellites, designed to extend the coverage of mobile telecoms operators to 100% of the planet, were deployed on the **SpaceX** Transporter-11 mission. The launch took place on 16 August aboard a Falcon 9 rocket from Vandenberg Air Force Base in California, USA.

"This launch propels us into a new phase of development," said Jaume Sanpera, the CEO and co-founder of Sateliot. "Not only will we begin generating revenue, but we will also position Spain as a global leader in IoT connectivity."

Remote patient monitoring to grow at 12.8% CAGR, reports Berg Insight

Berg Insight has reported that the number of remotely monitored patients reached 76.7 million worldwide in 2023 as the market acceptance continues to grow in several key verticals. This number includes all patients enrolled in mHealth care programmes in which connected medical devices are used as a part of the care regimen. Connected medical devices used for various forms of personal health tracking are not included in this figure. Berg Insight estimates that the number of remotely monitored patients will grow at a compound annual growth rate (CAGR) of 12.8% to reach 140.1 million by 2028.

The three main applications are monitoring of patients with sleep therapy devices, glucose level monitoring of patients with diabetes and monitoring of patients with implantable cardiac rhythm management (CRM) devices. Sleep therapy is by far the most connected segment, dominated by **ResMed**. In 2023, approximately 32.2 million sleep therapy patients were remotely monitored, which has more than doubled since 2018. The growth is driven by the compliance monitoring requirements introduced in the US and across European countries.

Glucose level monitoring has grown in the last few years and is now the second largest segment with 12.6 million connections at the end of the year. The growth is driven by the increased adoption of continuous glucose monitoring (CGM) systems from providers such as **Abbott** and **Dexcom**. Other device categories include ECG, telehealth, medication compliance, blood pressure monitors and others. The fastest growing market segments in the next five years are anticipated to be remote ECG monitoring and medication compliance monitoring.

"With advancements in AI and machine learning, mHealth platforms are evolving from monitoring tools to comprehensive systems that assist in diagnosing and treating patients, paving the way for more effective healthcare," said Vatsala Raina, an IoT analyst at Berg Insight.

China targets 3.6 billion mobile IoT connections by 2027

China's Ministry of Industry and Information Technology has unveiled a plan to push the development of the mobile Internet of things (IoT), aiming to boost the sector's supply, innovation capabilities and industrial value. By 2027, China will strive to further improve its mobile IoT ecosystem, with the number of mobile IoT terminal connections expected to exceed 3.6 billion, according to the plan. The country expects to support the establishment of more than five mobile IoT industrial clusters and set up over ten mobile IoT industry demonstration bases by 2027, it said.

The plan outlined four key tasks, namely strengthening the foundational IoT network, enhancing industrial innovation capacity, boosting the integrated application of smart technologies and fostering a favourable development environment. China will promote the application of mobile IoT in fields such as intelligent connected vehicles, healthcare and smart homes, according to the plan.

For intelligent connected vehicles, it said efforts will be made to drive the application of mobile IoT in scenarios like driving monitoring and autonomous driving, and realise functions like information exchange and sharing, complex environment perception and intelligent decision-making.

The ministry said it will also work to accelerate the integration of mobile IoT with key industries to support their digital transformation and new industrialisation. By the end of July this year, the number of mobile IoT connections in China neared 2.55 billion, accounting for 59% of China's total mobile terminal connections, official data showed.

News in Brief

Smart meters evolve from analogue to digital

In a report titled, 'Electricity Smart Meters: Government policies and sustainability initiatives will drive 2.1 billion connections in 2033' **Transforma Insights** estimates that the total number of electricity smart meter devices will grow to reach 2.1 billion in 2033. The firm says smart metering systems either use wireless communication options or fixed wired connections such as powerline carrier (PLC). A wide range of different wireless communication options have been used, such as Wi-Fi, RF mesh networks, LoRa, Wize, Zigbee, NB-IoT, traditional cellular communication technologies (2G/3G/4G) and Wi-SUN.

Technologies such as PLC and RF mesh are currently the most common primary communication technologies with a share of 60% of devices shipped in 2023. The vast majority of the remaining new devices use 5G massive machine-type communication (mMTC) (including NB-IoT and LTE-M) and non-mMTC LPWA (including, for example, LoRaWAN) as their primary means of communication. In 2023, 5G mMTC had a share of 17%, non-mMTC LPWA had a share of 10%, 4G had a share of 9% and short range had 2%. In 2033, 5G mMTC (share of 32%), LPWA non-mMTC (30%) and PLC and RF-Mesh (30%) will be the pre-eminent means of connectivity for new devices.

Swisscom Broadcast and Nokia launch Drones-as-a-Service network in Switzerland

Swisscom Broadcast has selected **Nokia** to deploy a nationwide Drones-as-a-Service network across Switzerland. 300 Nokia Drone-in-a-Box units are planned for deployment to enable emergency response, perimeter protection and infrastructure inspection, which will help keep public safety workers safe. The companies will continue cooperating with competent regulatory bodies to ensure that operations comply with regulatory frameworks, especially from spectrum and aviation safety standpoints.

This will be the second nationwide Nokia Drone Networks project after Belgium's **Citymesh** deployment. It will support Switzerland's public safety and Industry 4.0 efforts and highlight Nokia's strength in modernising digital infrastructure projects and utilising mission-critical industrial edge computing (MXIE) with the support of 3GPP technologies for beyond visual line of sight (BVLOS) autonomous operation.

Public safety agencies in Switzerland will tap into the nationwide drone network by requesting a drone flight, similar to a ride-sharing service, from Swisscom Broadcast. They will also be backed up by a service portfolio with expertise, compliance, data collection and analysis of the collected data from Nokia and Swisscom Broadcast. The deployment is expected to be available in all areas of Switzerland.

"We are pleased to select Nokia as a partner for this important infrastructure project in

Raghav Sahgal, Nokia

Switzerland. Together, we can speed up the go-to-market of our Drones-as-a-Service offering to our customers in the industrial and public safety landscape in Switzerland," Dominik Müller, CEO at Swisscom Broadcast, said in a media statement. The integration of our existing People Density Tool and our Drone Operations expertise with Nokia's industrial grade hardware in combination with an open and future proof Software architecture is an important key to support such large-scale projects."

"We are proud to partner with Swisscom Broadcast, a true innovator in Drones-as-a-Service operation, for this important project to establish a nationwide Drones-as-a-Service network in Switzerland," said Raghav Sahgal, president of cloud and network services at Nokia. "Nokia's Drone Networks solution enables large-scale projects as it incorporates our mission-critical industrial edge (MXIE) technology to power its advanced computing functions and software. It will undoubtedly help Swiss enterprises gain access to a superior Drones-as-a-Service offering to enhance worker and public safety."

Oracle integrates AT&T IoT connectivity into enterprise communications platform

Oracle is incorporating **AT&T** IoT connectivity and network application programme interfaces (APIs) into its Enterprise Communications Platform (ECP). The initiative will enable Oracle's industry cloud application customers to connect and manage their IoT devices on the AT&T network all in one platform, enabling reliable and secure communications.

Supported by AT&T, ECP delivers IoT connectivity and near real-time communications to Oracle's suite of industry cloud applications. With integrated capabilities such as IoT edge application management, this all-in-one offering removes the customer burden of managing complex integrations and network contracts.

Built on the high performance and security of Oracle Cloud Infrastructure (OCI), the unified communication and edge architecture gives businesses the connectivity and real-time data intelligence they need to power critical new services and experiences. The integration with AT&T IoT connectivity and network APIs is available across OCI regions in the U.S.

"Our mission has always been to help improve the way the world communicates, and with ECP supported by AT&T and FirstNet, we're taking a massive step toward that vision," said Andrew Morawski, executive vice president and general manager at Oracle Communications. "Together, we can help organisations across industries benefit from the full potential of 5G, by building a new generation of vertical applications offering endless opportunities to innovate."

Sarita Rao, the senior vice president of AT&T Partner Solutions, added: "By teaming with Oracle to incorporate IoT connectivity and programmable APIs into Oracle industry applications, we are providing businesses and organisations a tighter level of integration between the network and application, driving performance and reliability gains while also eliminating integration requirements and separate contracting events. It's co-creation at its best."

News in Brief

Kargo unveils lift for forklifts and AGVs

Kargo has announced the Kargo Lift, a new addition to the Kargo product portfolio, that has been purpose-built for forklifts and automated guided vehicles (AGV). The Kargo Lift extends the AI capabilities of the Kargo Towers, automating critical processes and enhancing visibility for warehouses, manufacturing facilities and distribution centres.

"Our goal has always been to push the boundaries of what's possible in industrial automation," said Sam Lurye, the founder and CEO of Kargo. "Like with all Kargo products, we have meticulously designed the Kargo Lift to be easy to install, drive immediate value and handle all the complexity of an industrial environment."

Intelligent Living and Specifix join forces for smart locks

Intelligent Living Application Group has announced that it has entered into a cooperation agreement with **Specifix**. Specifix deploys its artificial intelligence (AI) assisted robotics research and development for construction and industrial engineering services and technology. This cooperation underscores its commitment to enhance its technological capabilities for new product development which will expand its market presence.

Specifix's approach and technology align with Intelligent Living's goal for development of smart locks and smart home security devices. The cooperation will enable it to use Specifix's technologies to enhance research and development abilities, and even new automated industrial production processes to help improve efficiency and precision.

Sparkle and floLIVE collaborate to support sophisticated, global IoT connectivity

IoT organisations are becoming more advanced as they launch richer, global IoT products onto the market. When it comes to connectivity the market has moved on from simply thinking about cost per megabyte to more carefully assessing how to handle regulatory compliance, how to balance differences in mobile network performance from market to market and how to manage the more complex latency, security and failover requirements of IoT devices. Daniele Mancuso, chief marketing and product management at Sparkle, and Luigi Capobianco, the senior vice president and head of Europe and the Middle East at floLIVE, explain to George Malim, the managing editor of IoT Now, how the companies have collaborated to create compelling, compliant sophisticated, global IoT connectivity services that level the playing field across the entire planet

Daniele Mancuso
Sparkle

GM: How does your partnership with floLIVE align with Sparkle's strategy?

Daniele Mancuso: floLIVE was for us the missing piece, a reliable partner. One of the unique strengths of floLIVE has always been that it is a customer of Sparkle's outbound worldwide connectivity solution. floLIVE being interconnected with us already as a customer was one of the enabling factors and floLIVE is an excellent developer with an excellent platform. We are finding a lot of synergies, both from a technical point of view and from a commercial perspective. The success of Sparkle using the floLIVE platform is creating benefits to floLIVE itself and also enabling further benefits to Sparkle because, if we are able to increase the traffic that floLIVE can push towards our international mobile subscriber identity (IMSI), we are creating mutual benefit for both companies.

I would say that floLIVE is enabling us to realize our product pitch from when we launched our global IoT suite and we presented the idea of venturing into the IoT market to our CEO. We created a kind of double strategy. On one side, we want to target multinational enterprises directly and address some specific verticals that are striving to enter the mobility ecosystem. We target multinational enterprises and we tend to go up the value chain to those that are producing the objects that will onboard the SIM cards, either plastic SIMs or embedded SIMs (eSIMs), it doesn't matter.

The other side of the strategy was to enable Tier-2 and Tier-3 MNOs and MVNOs to develop an international IoT market based on the fact that they were already our global connectivity customers. This is enabled by floLIVE's connectivity management platform (CMP) because the platform can independently serve either enterprises, where we go directly with the Sparkle brand, or allow us to go to market with floLIVE's white-labelled solution. We can go to a Tier-3 MNO, for example, and give them our IMSIs and a customised floLIVE platform and they can resell this to their own customers using their own brand, with their own look and feel and their own commercial rules.

I think this new collaboration is a first in terms of commercial launch of an IoT solution with data localisation. There were several workgroups in international standards trying to address the topic of critical IoT. We are basically avoiding the need for SIM cards that are travelling in the US to connect back and forth with Europe

SPONSORED INTERVIEW

There will be three big gateways that we are going to localise: one in the US, one in Europe and one in Asia

or vice versa. This is going to be unique and the strengths of the partnership between floLIVE and Sparkle enable it.

There will be three big gateways that we are going to localise: one in the US, one in Europe and one in Asia. The unique factor is that it's not just a simple gateway localisation, it's a localisation in places where we have Sparkle local connectivity through peering with local carriers. Basically, we are going to provide a zero-latency IoT service for SIM cards that connect to those points of presence. This, I believe, is really a market first.

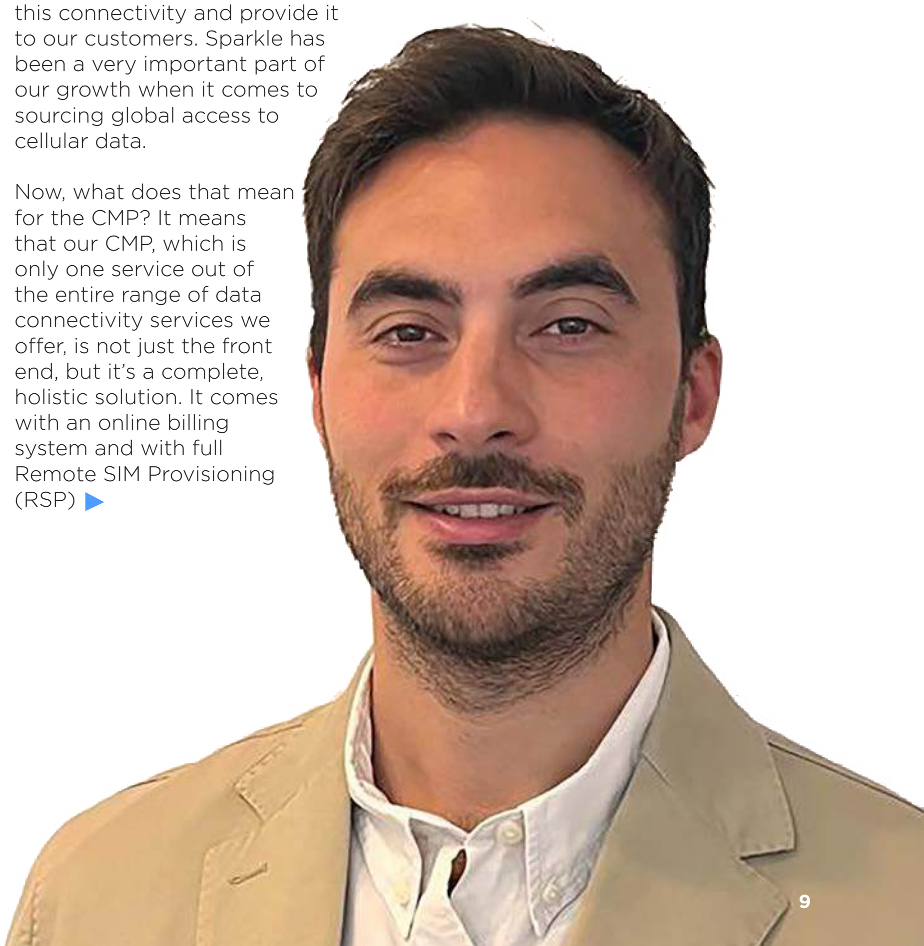
Of course, it's a combination of several factors. As we said before, let's not forget that our mobile platform runs over our 600,000 kilometres of fibre optic cables around the world, on top of our Seabone IP transit platform. We believe that we are going to see a lot of positive returns both in market appreciation in terms of revenues and margins, but what concerns us most is the customer experience. This is our main objective.

GM: floLIVE has built an impressive global IoT network; can you explain how this extensive data network benefits mobile operators compared to traditional connectivity management platforms (CMP)?

Luigi Capobianco: Our global IoT network has been designed and built in a way that allows us to constantly introduce new services and offerings both quickly and in a cost-effective way; this is because we developed the entire platform in-house using modern software architecture approaches and design guidelines. We have used Sparkle's global presence, not only for connectivity needs, but also for global presence in terms of data centres and physical interconnections globally, to access this connectivity and provide it to our customers. Sparkle has been a very important part of our growth when it comes to sourcing global access to cellular data.

Now, what does that mean for the CMP? It means that our CMP, which is only one service out of the entire range of data connectivity services we offer, is not just the front end, but it's a complete, holistic solution. It comes with an online billing system and with full Remote SIM Provisioning (RSP) ▶

Luigi Capobianco
floLIVE



Our IoT offering is based on global connectivity because of our history and because we strongly believe that being able to be connected anywhere in the world is an important foundation for the IoT business for multinational customers

capabilities for both M2M and consumer use cases, multi-IMSI capabilities and more. Our distributed network around the world enables all floLIVE customers, which could be MNOs, MVNOs and IoT service providers, to access our global data network and consume the advanced services we offer.

I think the advantage of our approach is that we do not only provide mobile operators a means for operating a profitable IoT business, but we've added two very important capabilities - one is the ability to extend their global reach even to highly regulated countries such as China, Brazil, Turkey and others. In addition, we're also enabling them to generate new revenues from advanced services that are made available via our global platform. These services include MVNE, mission-critical IoT, advanced IP data management, satellite connectivity and more. One of the new and very interesting things that we're doing with Sparkle is distributing our network capabilities and global presence.

A car maker, for example, doesn't just connect its cars in the old-fashioned roaming model. That works well when you're connected in Germany with a European MNO, but when you move to Canada or China with the same MNO, the user experience falls short. What we're going to do with Sparkle is build something that allows cars and other connected devices to have the same experience, performance, service level and security all around the world regardless of location. This is only possible when you put together a CMP for sure, but also the capabilities and the global presence of Sparkle.

GM: What makes Sparkle stand out from the competition and what impacts have you had on the success of IoT solutions?

DM: Our IoT offering is based on global connectivity because of our history and because we strongly believe that being able to be connected anywhere in the world is an important foundation for the IoT business for multinational customers. IoT by itself for us is a means to address the connectivity needs of things that are on the move. We strive to provide connectivity to things that are moving, and Sparkle is a multinational carrier with the strongest offering.

GM: Please can you tell us more about Sparkle's IoT strategy and offering?

DM: We started to develop the strategy roughly a year ago and we have already achieved good results. First of all, we had a list of requirements that are driven by our worldwide connectivity and machine-to-machine priorities. We don't need to negotiate an entire roaming agreement from scratch that is based on the full paradigm of human communication, but we can really focus on selective agreements that are related to the machine-to-machine market. Either we extend already existing partnerships and introduce a specific price list for machine-to-machine connectivity or we enter a new partnership dedicated to the machine-to-machine sector. This is already a good differentiator from other carriers that operate in the same space but I will say that the basic foundation of our global connectivity proposition, the technical foundation, is really a differentiator compared to the competition.

Our global connectivity has always been based on the concept of multi-operator service. Our platform is based on a multi-IMSI paradigm that allows us to offer to any customer wherever they are the best connectivity in terms of price, coverage or diversification. For IoT this is really a unique advantage. When you have an automotive manufacturer that needs to ship cars everywhere in the world, they need to guarantee that the vehicles they are producing can connect in all the countries and always find the best coverage at the best rates. There is also always the possibility to switch to another operator, either by failover, or by applying steering policies.

This multi-IMSI solution is corroborated by the over the air (OTA) capabilities to reconfigure a single SIM card or a set of SIM cards. If there are changes to the customer requirements or the commercial scenario in that specific country, we can still guarantee the customer that the coverage, the rates and the failover level agreements are respected over time. We can do everything with an OTA campaign. The technical capabilities that we just described with our commercial strength, part of it inherited from the TIM Group and part of it because we established this new roaming team, make us stand out. In addition, the coverage that we have with our 170 points of presence is spread around the world where we can do IPX peering with basically all the interconnect carriers. I would say that creates a unique solution in the market.

GM: How does floLIVE's solution enable mobile operators to manage and monetise IoT connectivity more effectively?

LC: The IoT connectivity market is quite competitive, so there are two things you can do: One is to try to bid the lowest possible price, which is not always easy and probably doesn't always bear the right fruits in the long term. The other is to move up the value chain to serve higher-value use cases with the connectivity they need in terms of latency, security and location. ▶

We're not telling MNO customers to do one or the other, but we are empowering them to do both. What does that mean?

First of all, as one of the world's leading IoT CMP providers, floLIVE was the first to differentiate between high ARPU and low ARPU use cases, meaning we launched an offering that distinguishes between the volume of megabytes per month and charges a platform fee accordingly. For example, with smart meters, the platform fee is a fraction of a high ARPU service's platform fee. We did this to allow mobile operators to run a profitable IoT business and compete in this challenging market.

Second, our platform, built using the latest software design, architecture and deployment practices, ensures a lower marginal unit cost as more and more devices are onboard our global, cloud-native network. In both the short and long term, this allows mobile operators to increase their profitability and obtain a strong presence in the growing IoT space.

The importance of owning our entire software stack, from the core network through SIM management, real-time multi-tier billing engine and CMP, comes into play when we deploy since we don't have fixed third-party licence costs.

Another key benefit that floLIVE brings to mobile operators is a new, constant revenue stream generated by floLIVE's global customers who seek connectivity in the mobile operator's footprint. As I stated earlier, this is how floLIVE and Sparkle began the relationship – by offering Sparkle's coverage to our global customers. This is another pillar that empowers MNOs to not only operate a profitable IoT business but also increase their revenues inorganically.

GM: How does floLIVE ensure compliance with diverse regulatory requirements across different countries, and why is this crucial for mobile operators?

LC: The world is going in a direction in which permanent global roaming is going to become more and more complex. Accessing all countries around the world, without any temporary restriction through a single IMSI is already a challenge today, but it is going to be more of a challenge in the future. Let's say you have a track and trace application for containers – you don't really care about permanent roaming. However, there are numerous use cases that where this does matter, such as smart metering, automotive, POS, credit card readers, alarm systems, video cameras and dashcams, which are all interesting use cases. These applications are more prone to requiring permanent roaming. If you deploy one of these use cases in Turkey, for example, the devices are likely to stay in Turkey for more than 90 days, and that is not allowed. Additionally, privacy regulations like GDPR and CCPA require that data remains within the country of operation, which conflicts with roaming. For example, a device operating in California but using a European SIM/profile violates CCPA regulations because data, which is protected as private, is routed through Europe instead of the device's actual location. To address this, we started cooperating with the 15 different IMSI providers we support today. We have a global bootstrap, via Sparkle, which has by far the largest coverage in the world and also reliability. Then, whenever a customer says they need to localise in Brazil we have two Brazilian IMSIs so that you can access Brazil on local networks owned by floLIVE, compliantly accessing different local operators.

The world is going in a direction in which permanent global roaming is going to become more and more complex

www.flolive.net

Mobileware turns to floLIVE for Darby platform connectivity

Delivering connectivity is crucial in the Internet of Things (IoT) market. While the ecosystem is comprised of many key players, such as hardware, software and computing providers, the tie that binds these is connectivity to ensure that wherever or however devices are deployed, they can connect to the internet to communicate data

IoT solution providers (ISPs) stand at a vital juncture in providing the very critical connectivity for IoT use cases but also helping stitch together the other very important components of IoT, including data and hardware management, security, integration and maintenance and support. **MobileWare** is an IoT solution provider that enables IoT solutions in key verticals such as restaurants, retail, education, security, transportation and logistics.

Business impact of floLIVE:
- Single pane of glass for device management
- Simplified management of multi-carrier relationships
- Single stock-keeping unit (SKU) SIM
- Global connectivity designed for IoT complexity

MobileWare is successfully delivering solutions in the IoT segment but found managing the complicated connectivity ecosystem burdensome. "MobileWare developed its Darby platform to help integrate the components of the solutions we were providing to customers, which was further refined and enhanced through its partnership with **floLIVE**," says Steve Higgins, the chief executive of MobileWare. "We were trying to manage all the different carrier agreements, multiple stock-keeping units (SKUs) and who has the best SIM cards."

The nature of IoT is very different from consumer connectivity. Typically, with consumer connectivity, a user only needs a single SIM from a single mobile network operator (MNOs) but even still, an ISP generally will contract and resell connectivity from multiple carriers. However, with IoT, the complexity of that can easily multiply for several key reasons:

Coverage and availability: Network operators may have different coverage areas and service availability. In some regions, certain operators might offer better coverage or have stronger signals, ensuring that IoT devices can communicate effectively across diverse geographical locations. Multiple operators increase the chances of finding suitable connectivity options for different deployment scenarios.

Redundancy and reliability: Relying on a single network operator introduces a single point of failure. If that operator experiences outages or issues, all devices connected to that network may be affected. Having multiple network operators allows for redundancy, improving the reliability of IoT solutions. If one network faces problems, devices can switch to alternative networks, ensuring continuous operation.

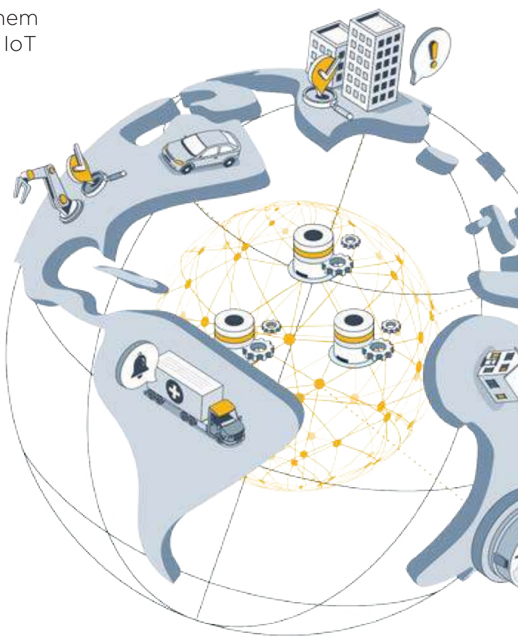
Cost optimisation: Different network operators may offer varying pricing structures and plans. Having multiple options allows businesses to choose the most cost-effective solution based on their usage patterns, scalability requirements and budget constraints. Competition among network operators can also drive down prices and improve service quality.

Global deployment: For IoT solutions with global deployments, relying on a single network operator may not be practical due to regional variations in network infrastructure and regulations. Multiple operators allow for more flexible and scalable global deployments, ensuring connectivity across different countries and continents.

Technology evolution: The field of IoT is rapidly evolving, and new connectivity technologies continue to emerge. Having multiple network operators allows businesses to adapt and integrate the latest and most suitable connectivity technologies as they become available, ensuring future-proofed IoT solutions.

Customisation for specific use cases: Different IoT applications have unique requirements, such as low latency, high bandwidth or long-range connectivity. Multiple network operators enable businesses to choose the network technology that best aligns with the specific needs of their IoT use cases.

MobileWare was successful in delivering its diverse connectivity offerings to customers and helping them save money and tap into IoT success, but behind the scenes, it was a logistical challenge. "We were asking ourselves how do we continue to grow this and have a platform – we were doing it on spreadsheets," adds Higgins. ▶



SPONSORED CASE STUDY

A platform for growth

MobileWare integrated Darby with floLIVE's connectivity management platform (CMP), which has allowed MobileWare to provide its customers with a single pane of glass to view all data usage and device activity, as well as activate and deactivate SIMs anywhere in the world. Darby's functionality ties in with hardware management so customers can utilise one platform for granular management in their IoT use cases.

floLIVE's holistic cloud-based CMP is designed to deliver a suite of services for making IoT businesses global, coherent and profitable. floLIVE fully owns its technological infrastructure and software stack, enabling it to provide full customisation and additional functionality to meet the advanced requirements of large-scale IoT deployments. This means providing more customisation, visibility and control over the network, which is essential for enterprises with sophisticated and demanding IoT use cases.

MobileWare also uses floLIVE's core network, which is a unified approach to global connectivity through key mobile network operator (MNO) partnerships. The floLIVE robust international mobile subscriber identity (IMSI) library allows for broad carrier access across the globe from a single source.

As an ISP, value-added services are paramount in differentiating services and driving service level agreements (SLAs) and quality of service (QoS). In partnering with floLIVE, MobileWare achieves:

Seamless coverage: Sourcing connectivity operator-by-operator leaves organisations in a logistical bind, but accessing a library of more than 15 IMSIs allows for coverage from a single source.

Single SKU: Multiple SIMs from multiple carriers introduce complexity, but using a single SIM that can host numerous carrier profiles creates a unified approach.

Global reach: Worldwide connectivity access from a single source that operates at the local level ensures global connectivity without the headaches or local agreements or roaming SIMs.

Full visibility: Not being incumbent on carrier's connectivity management platforms that are not designed uniquely for IoT is paramount to MobileWare in not just internally having visibility into devices, but also handing that visibility down to its customers.

Superb customer support: Offering complete customer support throughout the customer journey is imperative to MobileWare.

The results

"We like to provide service levels that spoil our customers rotten. Customers can call me day, night or during the week - I will answer," Higgins says. "Companies today really struggle with finding a way to have simple, secure connectivity, always. We provide them just that."

The complexities of IoT connectivity don't often arise until deployment or afterwards during management. Higgins said a question he sees from customers or prospects is: what is the point of partnering with an ISP when the organisation can just use two SIMs from two different providers. If one network were to fail, the second SIM provides failover connectivity.

He said that is an expensive alternative (paying for two different data plans just for a failover plan) to adopting a multi-profile solution, like the Single SIM that MobileWare offers. Powered by floLIVE multi-IMSI technology, MobileWare offers customers the ability to seamlessly switch networks over the air (OTA) in case of a network failure, network event, coverage gaps or as a device moves along networks and needs to connect to the most available network. This simplified, more cost-effective solution hosts numerous profiles, not simply two networks via two SIM cards.

MobileWare also differentiates itself through comprehensive customer support, which – in the complex sector of IoT – is important as devices must be connected and communicating consistently. Troubleshooting is supported through granular visibility provided via floLIVE's CMP and MobileWare's Darby, allowing for faster problem resolution than using multiple MNOs and the associated numerous support systems. MobileWare can confidently turn to floLIVE for top-tier support for escalated issue resolution.

"We're only as good as the team behind us," Higgins says of floLIVE. "The responsiveness on the network level – we springboard from that and provide this great experience for our customers."

Altogether, MobileWare's partnership with floLIVE enables the organisation to provide:

24/7 management and support: MobileWare's ability to provide exceptional customer support is enhanced through floLIVE's support and responsiveness.

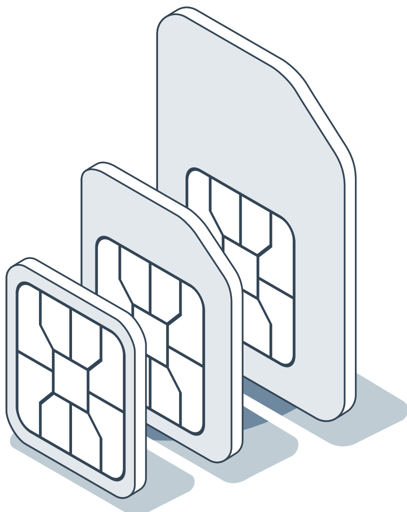
Single pane of glass: MobileWare customers can access broad connectivity and network options through floLIVE's robust IMSI library from a single source instead of carrier-by-carrier and SIM-by-SIM.

Comprehensive management: Integration with floLIVE's CMP allows MobileWare to provide the unique value proposition of granular insight into and management of connectivity and hardware components.

Connectivity across the globe: Accessing worldwide connectivity is simplified for MobileWare customers.

Reliability and redundancy: OTA switching allows customers to access the right network at the right time for optimised connectivity.

Simplified logistics: MobileWare's Single SIM opens up numerous carrier networks without the need for additional SIMs.



Connectivity services deliver the platform for hyperscale IoT innovation

With hyperscale IoT now a reality, the burden of managing connectivity has increased and magnified the complexities. To address the issues, IoT organisations are selecting connectivity management platforms (CMPs) to simplify and streamline management of device connections through a single system. With billions of devices to be managed, the CMP sector is set to generate billion dollar revenues

It's clear that enterprises are willing to pay for premium support, value-added services, consulting, network attach fees and devices

It's well understood that after years of false starts and over-hyped projections IoT is now a mass-scale phenomenon. Research firm **IoT Analytics** has reported in its 'State of IoT Summer 2024' report that there were 16.6 billion connected IoT devices by the end of 2023 (a growth of 15% over 2022). The firm expects this to grow 13% to 18.8 billion by the end of 2024 and upwards to hit 4.0 billion devices by 2030.

Cellular IoT (2G, 3G, 4G, 5G, LTE-M, and NB-IoT) now makes up nearly 21% of global IoT connections. According to IoT Analytics' 'Global Cellular IoT Connectivity Tracker & Forecast' (updated June 2024), global cellular IoT connections grew 24% YoY in 2023, strongly surpassing the growth rate for global IoT connections. This growth is due to the adoption of newer technologies such as LTE-M, NB-IoT, LTE-Cat 1 and LTE-Cat 1 bis, as older technologies such as 2G and 3G are phased out. Greater cellular choice is aiding growth with the introduction of 5G reduced capacity (RedCap) offering a reduced complexity, more affordable variant of 5G.

RedCap offers download speeds up to 150 Mbps, upload speeds of 50 Mbps and latency of less than 100ms. The technology's performance makes it well-suited for video transmission and adoption in video surveillance use cases is underway. Generally, the technology offers a cost-effective alternative to standard 5G.

Platforms for mass-scale

With momentum behind increased numbers of cellular IoT devices and new variants becoming widely available, the management of connectivity continues to be complex. A vibrant service provider sector has grown up to support organisations, many of which have little or no interest in managing connectivity, preferring to focus on their core business and IoT product and service innovation instead of becoming connectivity experts.

Transforma Insights has reported that several themes are driving IoT connectivity adoption with market evolution and the arrival of new technologies and commercial models disrupting the market. The firm sees devices and device-to-cloud propositions that incorporate sensors and data management as appealing options. In addition, it notes that service providers are looking to bring additional chargeable services to customers as they seek out new revenue opportunities.

It's clear that enterprises are willing to pay for premium support, value-added services, consulting, network attach fees and devices. However, the individual needs of IoT applications mean that customisation and adaptation are required so connectivity closely meets the needs of use cases. That's a money-making opportunity for connectivity and other service providers.

Services to support connectivity

The CMP market is changing to reflect these new needs and is adopting new models to support dual sourcing and overlay abstraction. The challenges remain significant with some markets still focused on data sovereignty and national resilience, hampering provision of standardised, global offerings. While permanent roaming has largely been addressed, ways to address the constraints need to be considered.

CMPs are needed because bringing together an international set of IoT connectivity is complicated. The blend of connectivity from lower end technologies up to 5G and spotty coverage of emerging technologies makes it difficult to assemble truly global offerings and this makes well-established technologies such as LTE-Cat 1 and LTE-Cat 1 bis appealing for multinational deployments, although interest in 5G, non-terrresterial networks and NB-IoT is rising.

A spread of different types of IoT connectivity providers currently serves the market. "There are three main categories of leading CSPs for IoT," confirms Matt Hatton, the co-founder of Transforma Insights. "At the very apex of the diamond are the major mobile network operators, led by **Vodafone** and followed closely by **Deutsche Telekom IoT**, **NTT**, **Telefónica**, **AT&T** and **Verizon**. ▶

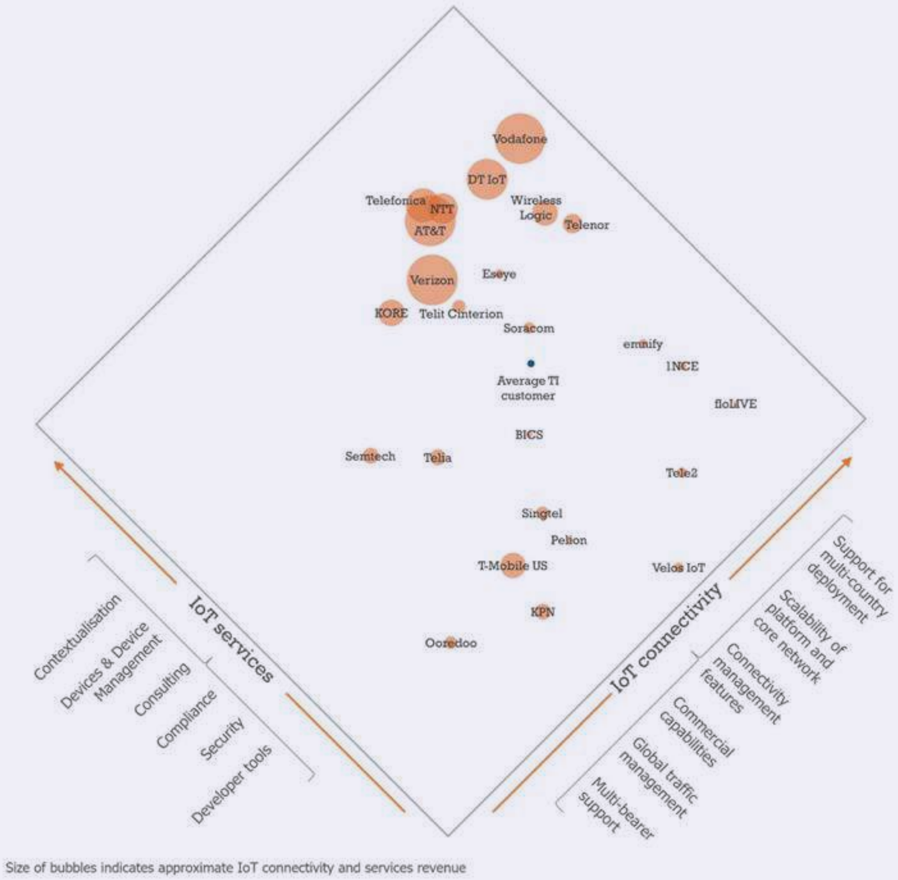


Figure 1: CSP ratings for global IoT connectivity and associated IoT services

(Source: Transforma Insights, 2004)

The second category of market leaders are those that have focused exclusively on providing excellence in a narrow element of pure cellular connectivity, largely ignoring devices or much in terms of customisation for the enterprise client. This group includes **1NCE**, **emnify** and **floLIVE**. Finally, there is a group of communications service providers (CSPs) that straddles the two camps, in some cases with equally capable connectivity offerings, but typically married with a more complete set of capabilities around IoT services. This group comprises **Eseye**, **KORE**, **Soracom**, **Telenor**, **Telit Cinterion and Wireless Logic**."

Figure 1 sets out Transforma's vision of the global CSP IoT connectivity landscape, placing different organisations on a grid composed of IoT services and IoT connectivity.

All players demonstrate awareness that simply selling connectivity as a commoditised product for customers to self-manage has limited appeal to IoT innovators and also see service provision as a means to drive revenues. For this reason, analyst firm **Berg Insight** reports that IoT managed service providers now play a key role in the ecosystem. Most players operate as full mobile virtual network operators (MVNOs) and typically offer IoT connectivity services based on a mix of roaming and local access agreements and sometimes also value-added services targeted at vertical segments. The firm's research has uncovered that IoT managed service providers had more than 200 million cellular IoT connections under management at the end of 2023 and around US$1.9 billion in annual revenues.

Platforms for visibility

This level of revenue highlights that connectivity management is a significant problem for IoT deployments and enterprises are looking or ways to abstract complexity away and gain greater insights into their IoT connectivity needs. A recent survey of IoT connectivity providers conducted by **Kaleido Intelligence** on behalf of floLIVE found that 72% of respondents stated they do not have full visibility into network activity. In addition, the survey uncovered that just 27% of respondents provide customers with full visibility into network activity.

"IoT has reached a significant turning point where increasingly complex and larger device deployments require best-in-class solutions to support connectivity," said Steffen Sorrell, Kaleido Intelligence's chief of research. "MVNOs and IoT service providers delivering connectivity to customers form a crucial part of the market and their customers need to be supported through a CMP that allows customers full access and control over their device fleets."

Understanding device behaviour and whether they are connecting to the network as expected is an essential underpinning capability for large-scale IoT deployments and sophisticated customers now expect this. CMP providers, from the Kaleido Intelligence survey responses have strong understanding of the potential they have to demystify device behaviour and support IoT security as part of their offerings.

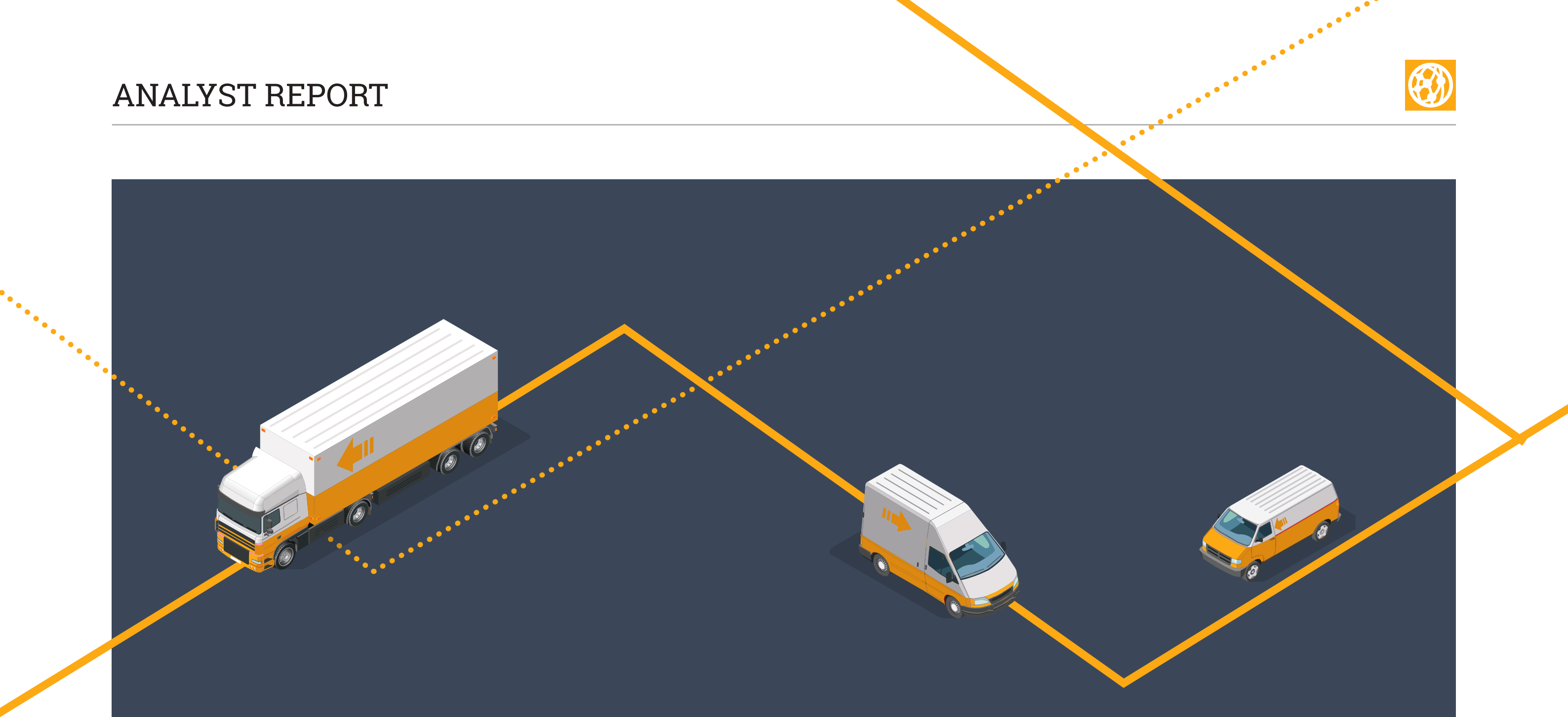
All players demonstrate awareness that simply selling connectivity as a commoditised product for customers to self-manage has limited appeal to IoT innovators and also see service provision as a means to drive revenues


GITEX GLOBAL
14 - 18 OCTOBER
DUBAI WORLD TRADE CENTRE
MON 11 AM - 5 PM
TUE - FRI 10 AM - 5 PM
THE LARGEST TECH & STARTUP EVENT IN THE WORLD
Global Collaboration to Forge a Future
AI ECONOMY
6,700+ Exhibitors
187k Visitors
1,800+ Speakers
Where the visionaries and policy makers meet.
#GITEXGLOBAL
gitex.com
Scan the QR code to
SECURE YOUR PASS
ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

ANALYST REPORT

The future of fleet management: Expanding use cases and connectivity requirements

Report sponsor:

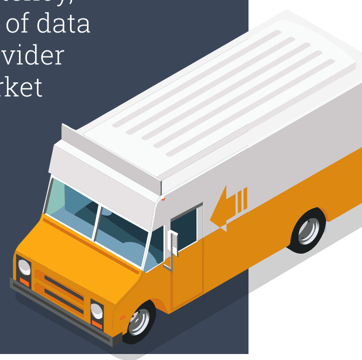


The future of fleet management: **Expanding use cases and connectivity requirements**

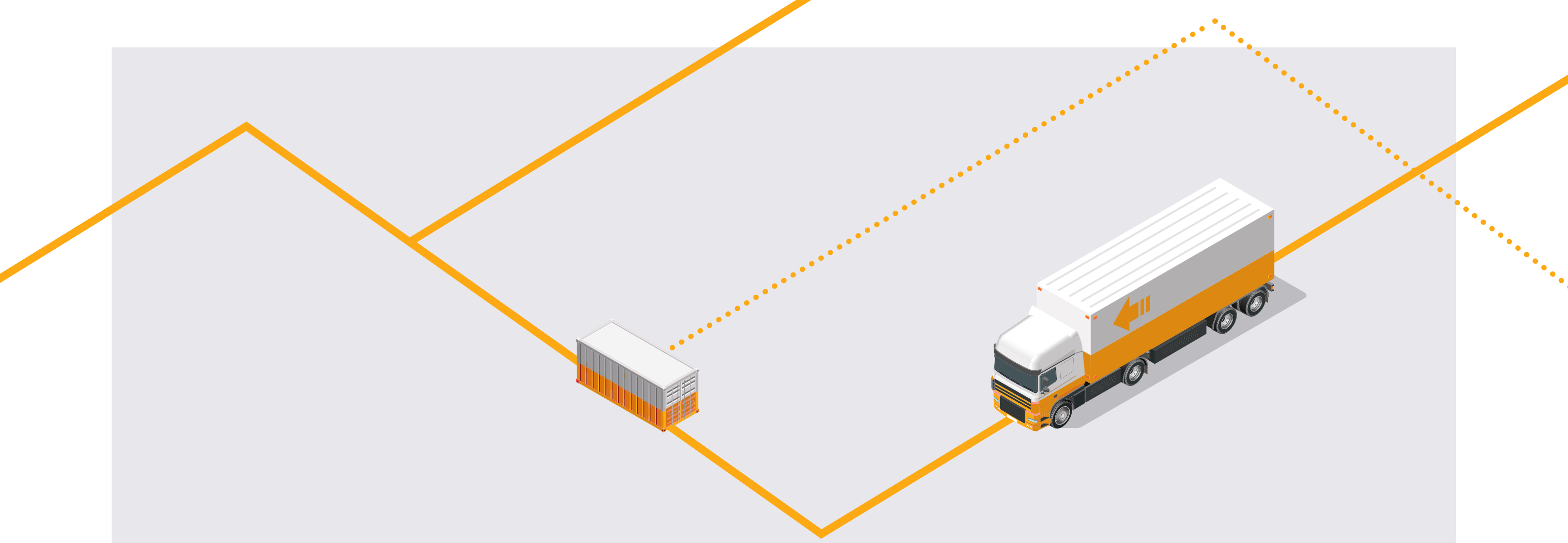
Introduction

The fleet management market has undergone a rapid digital transformation, write ABI Research's Elizabeth Stokes, a senior analyst for IoT Network and Platforms, and Dan Shey, the vice president of Enabling Platforms. The industry has evolved from simple location-based tracking to an ecosystem of advanced IoT applications that require cutting-edge cloud and communication technology. Advanced use cases, including video monitoring for driver safety, are quickly becoming standard in the industry, paving the way for the highly-anticipated future applications of commercial vehicle electrification and autonomous driving. These future use cases will drive even greater demand for advanced IoT devices, data management platforms and, perhaps most importantly, an unprecedented level of localised global connectivity.

As fleet managers prepare for this future, many find that their internal infrastructure and connectivity services are underperforming. Many fleet operations still depend on manual processes, and many fleet management use cases continue to rely on low power wide area (LPWA) networks, even as video-based applications and other future fleet management use cases demand the throughput of 4G and eventually 5G networks. Given these developments, fleet managers in the future will require a completely different type of network and connectivity service provider, one that can offer a range of highly available networks and a connectivity management platform designed for advanced IoT applications. Local connectivity on a global scale is going to be a boon for the demands of low latency, battery-optimised connectivity that meets the increasing regulatory requirements of data sovereignty, privacy and roaming restrictions. Choosing a connectivity service provider equipped for the future will be integral to enterprises as the fleet management market prepares for another wave of innovation and use case expansion. ▶



SPONSORED REPORT



Use case expansion

The telematics space is at a unique convergence of tried-and-true use cases that will remain pivotal within the industry. In contrast, newer use cases arise, creating the opportunity to develop technologies and more accessible hardware and connectivity costs.

Traditional use cases

These familiar use cases will continue to have a stronghold in the industry, supporting a range of benefits from efficiency, cost-saving and regulatory compliance adherence:

Track and trace: Track and trace is a baseline use case for fleet management and a building block for the most advanced fleet application technologies today. At its most basic, track and trace refers to using global positioning system (GPS) technology to track vehicles and assets in transit. Track and trace is a legacy use case, first made possible by the commercial introduction of GPS in 1993. By the early 2000s and with the removal of selective availability (SA), major companies began to rely on GPS and fleet management systems (FMSs) to receive remote updates from their fleets on the road, ushering in a new age of enterprise telematics.

Improvements in cloud services, machine-to-machine (M2M) communications and edge compute have greatly improved track and trace technology since its early adoption at the turn of the century. Fleet managers now have unprecedented, granular visibility into a vehicle's performance, allowing for insight into individual components of the car and a holistic understanding of the vehicle, its route and the driver at its helm.

Regulatory compliance: Enterprises must navigate various state and federal regulations that require fleet managers to log vehicle maintenance, driver hours of service and behavior, load weight and more. Failure to comply with these reporting standards can lead to heavy fines or harsh penalties.

Fleet management technology can offload these data collection and analysis activities to sensors and fleet management platforms. Many fleet managers rely on LPWA networks like LTE-M to send sensor-based compliance data to FMSs that can package it into ready-made reports. This process eliminates the manual reporting tasks these regulations previously required.

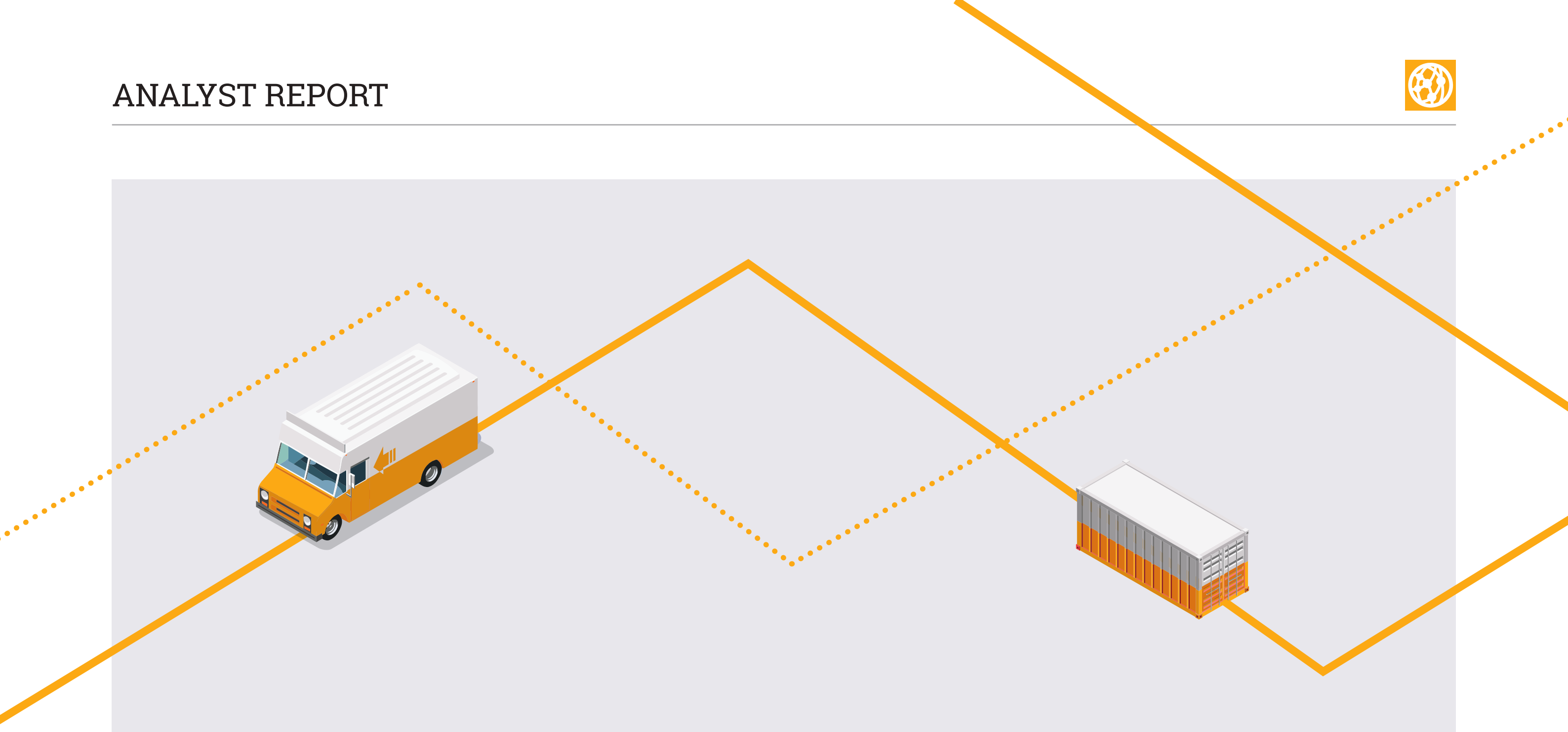
Asset tracking and protection: Like those used to prevent vehicle theft, GPS sensors on assets can track fleet cargo movements in real time, assuring asset managers that goods are moving on their designated routes. Additionally, condition-based monitoring (CBM) sensors can track a trailer's condition to protect environmentally-sensitive assets, typically using LPWA networks to relay important data points like moisture levels and trailer temperatures back to fleet managers.

Emerging use cases

These communication and technology advancements have created a range of cutting-edge fleet management use cases that build on the foundational principles of track and trace.

Vehicle theft prevention: Vehicle theft is an ever-present threat to enterprises and is increasingly likely as incidents of carjacking climb. The National Insurance Crime Bureau (NICB) in the United States recently reported that over one million cars were stolen nationwide in 2023, stating that vehicle thefts have steadily grown since 2019. GPS-based sensors and FMSs that track vehicles and cargo at all times on a virtualised map are critical tools to protect company assets. GPS tracking also enables enterprises to employ geofencing, which sets virtual boundaries for a vehicle. Geofencing technology can help fleet teams stay vigilant against suspicious movements by sending real-time alerts to the proper teams if a vehicle exits the virtualised perimeter.

Driver safety: The Federal Motor Carrier Safety Administration's (FMCSA) most recent Large Truck and Bus Crash Facts report reveals how truck driver behaviour impacts the safety of those on the road. According to the 2021 report, at least one driver-related factor, like speeding and distracted driving, "was recorded for 32% of the large truck drivers in fatal crashes." Driver safety is a critical fleet management use case, requiring various technologies to monitor both a driver's physical state and their behaviour on the road. FMS solutions often feature driver scorecards based on telematics data from sensors that monitor their average speed, lane changes and ▶



braking. The scorecard can help coach drivers and ensure they are not driving aggressively and putting themselves or others at risk.

Telematics data can also help alleviate fatigue, a common risk factor for professional drivers. Fleet management solutions often collect relevant data to determine the most efficient routes of travel, playing a crucial role in ensuring drivers are not on routes that are too long or accident-prone.

Video surveillance: In both driver safety and vehicle theft prevention, use cases offer a significant opportunity to integrate video capabilities. More robust connectivity through cellular as primary or failover creates a chance to mobilise video surveillance and lower hardware costs, making implementation much more possible. In both these use cases, video monitoring capabilities can capture surroundings to provide detailed insights. In driver safety, unsafe behaviour can be flagged. In theft monitoring, real-time and historical data can help track down culprits and help recover equipment.

Business Process Integration: Fleet business operations have historically been forced to rely on inefficient manual processes. Yard management, for example, has been plagued by manual gatekeeping and documentation, leading to costly congestion and transport delays. According to ABI Research, 80% of transportation delays occur because of yard inefficiencies, with experts predicting that the situation could worsen as global supply chains and distribution networks become more complex.

Fleet telematics are critical in streamlining yard management and other operational processes. GPS technology, sensors, and LPWA and 4G communication enable vehicles to transmit vital data from the road to the yard, such as alerting yard managers to potential delays or cargo movements within the yard. These insights can prevent stockouts and improve the efficiency of the yard and the supply chain.

IoT applications, devices and technologies

Sensor technology and wireless communication advancements have transformed commercial vehicles into epicentres of IoT innovation. A single truck can now incorporate an entire ecosystem of devices and sensors, giving fleet managers access to the workings of individual vehicle components like engines, tyres and trailers. The next section explores how IoT devices have improved remote monitoring use cases and led to new, advanced fleet management applications incorporating video.

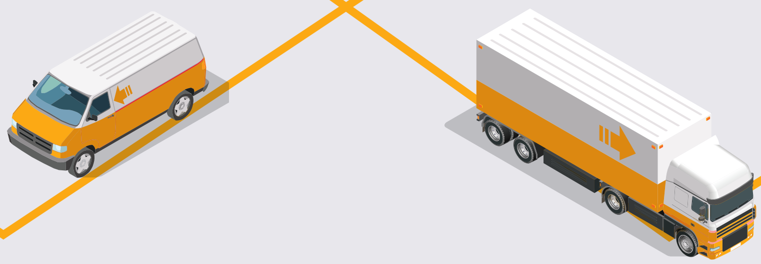
Sensor-based monitoring

Many fleet management use cases require sensors to collect and send crucial performance and condition-based data to FMSs. The sensors - often placed on fallible components like tyres - usually use Bluetooth to send these data to the vehicle's telematics control unit (TCU), the on-board diagnostics (OBD) system or a gateway. The TCU, the OBD and the gateway is likely to use an LPWA or 4G cellular network to ferry the sensor data to a cloud-based application.

Most engine diagnostic and GPS location data go through the TCU, which is built into the vehicle by the original equipment manufacturer (OEM). Other data that need to be aggregated, like data from the tyres, fuel lodge or camera system, will likely go through either a gateway, the TCU or both.

Tyres: Monitoring tyre health is a crucial task for fleet managers. Using sensor data sent through a cellular connection, an FMS can alert relevant maintenance teams if a tyre requires maintenance, allowing fleet managers to plan for potential downtime before an unexpected event like a flat tyre or blowout occurs. Such unexpected incidents usually result in expensive in-field maintenance that can keep a vehicle out of commission for a while. According to one 2016 survey[1], the average fleet experiences around 97 flat tyres per year, each costing around US$338.42 for downtime ▶

[1] https://www.automotive-fleet.com/157115/cost-of-flat-tire-to-a-fleet-detailed#:~:text=Of%20the%20survey%20respondents%2C%20the,tires%20fleets%20face%20annually%20%E2%80%94%2097.



and replacement. This would mean that fleets spend approximately US$32,800 on flat tyres annually. As a result, companies are increasingly investing in sensor-based solutions that can predict tyre incidents before they happen. **Geotab** estimates that businesses can save 10% to 20% on maintenance costs with data-driven, predictive maintenance solutions. These solutions often work best when backed by a strong connectivity partner that can facilitate real-time diagnostic data transfers from the road.

Engines: Sensor-based solutions and telematics data can digitalise engine monitoring, saving engineers' time from the manual processes of the past. For example, an hour meter is a sensor that counts the hours an engine has been running. The sensor signals to fleet managers when maintenance is required based on the hours it records. Collecting the hour information from the meters was historically a clunky process. Staff had to log the hours from the sensor manually and only had access to the meter when the vehicle was stopped. Modern fleet management solutions and improved LPWA coverage have simplified this process, with hour meters now sending automatic hour logs to maintenance software as the vehicle runs.

Fuel: Remote fuel management gives fleet managers access to information once reserved for drivers. In the past, business owners did not have much visibility into vehicle fuel levels or the fueling process. Now, fuel sensors can send relevant data to remote teams, giving fleet managers insight into fuel levels and sending alerts if low fuel or abnormal fuel usage is detected. Telematics solutions predominately used for driver safety can also monitor for driving behaviours that waste fuel, such as speeding. Some studies have shown that fleet managers can save up to 20%[2] on fuel and maintenance costs by investing in connected fleet management solutions. Cost savings in this area have become even more important as fuel prices rise. According to a recent American Transportation Research Institute (ATRI) report[3], average fuel costs per mile for fleets rose almost 54% from 2021 to 2022, the largest increase of all fleet cost centres.

Video monitoring

Video telematics represents a leap forward in fleet management technology. New gateway technology and better cellular coverage enable vehicles to send video footage from the field to remote teams, giving rise to a new category of telematics use cases that require reliable, high-throughput connectivity. According to ABI Research, commercial video telematics solution shipments will reach 17.8 million units by 2030, with shipments growing almost 24% from 2020 to 2030[4].

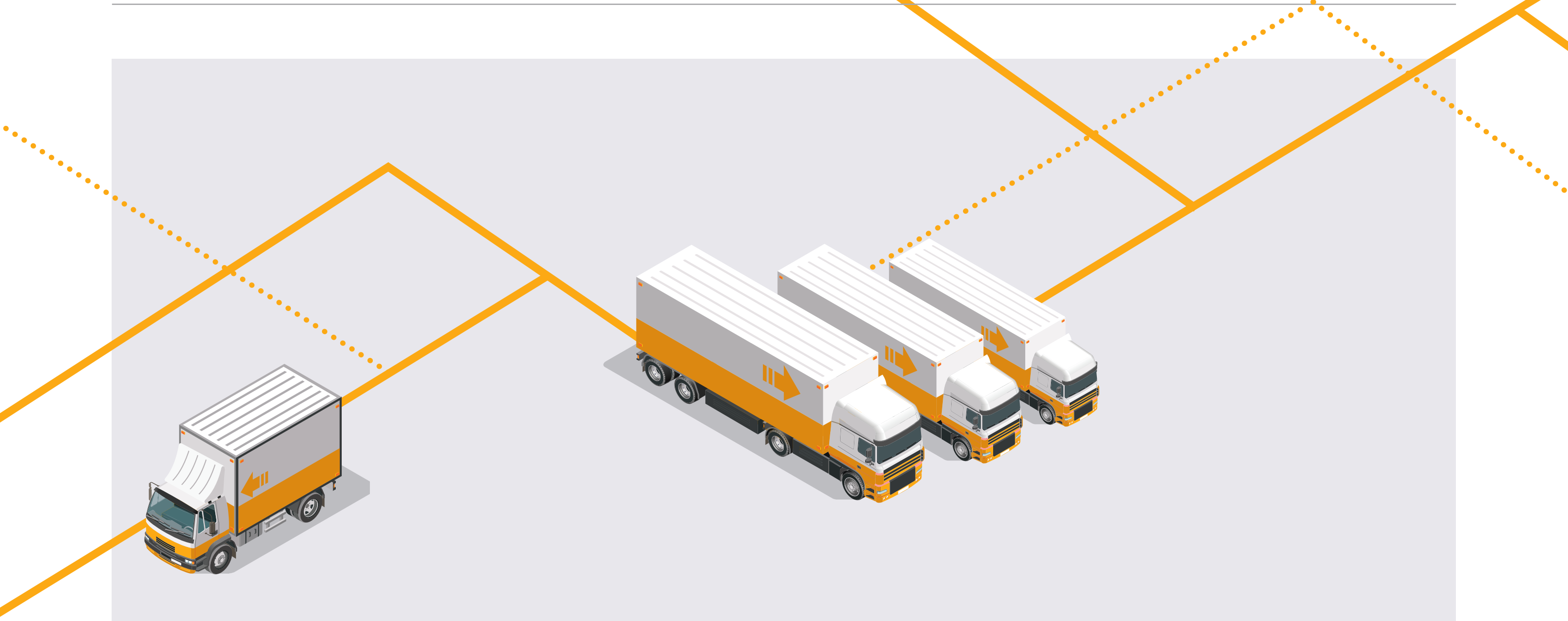
A video telematics system typically includes a deployment of road-facing, load monitoring, back-up or driver-facing cameras. Unlike other track and trace-related use cases that predominantly rely on LPWA networks, the use of video will require more fleets to utilise highly available, high-bandwidth networks. A fleet's camera system typically connects to a vehicle's diagnostics port or telematics gateway through Wi-Fi, Bluetooth or a wired connection. The chosen gateway is then likely to use a 4G network to send relevant footage to the cloud.

Two main video monitoring applications in fleet management include asset loading and unloading monitoring and driver supervision. Both use cases escalate a fleet's connectivity and coverage requirements.

Asset loading: Load monitoring cameras monitor employees as they load and unload cargo from a vehicle's trailer. These cameras are increasingly popular, as they can monitor cargo movements and ensure that cargo is not damaged or stolen in the docking process. The footage can also serve as evidence to exonerate employees and enterprises from any potential accusations of damage or stealing.

Driver safety: In the past, dashcams in commercial vehicles were passive instruments, capturing footage that could only be reviewed after an incident occurred. ▶

[2] https://www.tourmo.ai/resources/guides/the-essential-guide-for-fleet-management-cost-savings-tm#:~:text=The%20well%2Dknown%20benefits%20of,analysis%20and%20taking%20corrective%20action.
[3] https://www.fleetowner.com/operations/article/21268287/fleet-costs-rise-213-with-fuel-the-leading-expense-atri-reports
[4] https://www.abiresearch.com/news-resources/chart-data/commercial-video-telematics-solution-shipments/



Now, smart dashcams equipped with video analytics and artificial intelligence (AI) can recognise predefined events in real-time. For example, AI-enabled driver-facing dashboard cameras can monitor drivers and autonomously recognise pre-defined prohibited behaviour, including smoking or mobile phone use. If concerning behaviour is detected, the cameras will automatically begin recording and can alert the proper teams. Forward-facing cameras can have similar triggers, recognising potentially dangerous road conditions. Advanced driver assistance systems (ADAS) enabled by video can take driver coaching even further through real-time, in-cab alerts like forward collision or lane departure warnings.

Having footage of driver behaviour and the areas surrounding the vehicle can be particularly helpful in the case of accidents. According to the US Department of Transportation, 162,529 large trucks were involved in crashes in 2023. Video monitoring systems can help prevent such accidents and also protect drivers and companies from false claims should a crash occur. According to **ASIS International**[5], businesses with connected telematics solutions like in-cab dash cams can reduce insurance claims by at least 25% and crashes by around 50%. To maximise cost savings and minimise accidents, fleet managers need a reliable connectivity partner to support the throughput and coverage requirements of such advanced, video-led applications.

Shared mobility

The shared and micro-mobility market, featuring rental rideshares, e-bikes and e-scooters from companies like **Uber** and **Lyft**, is a relatively new fleet management vertical with unique connectivity considerations. Micro-mobility devices like rental e-scooters and e-bikes require high-uptime connectivity, as customers expect to pay for these devices through a mobile app and gain immediate access to them. This real-time transaction requires low-latency connectivity, often in urban areas crowded with other connected devices. These connected e-devices also must provide constant, real-time location data so micro-mobility companies can accurately track their scattered fleets. Locating every e-scooter and e-bike in dense urban areas requires resilient connectivity and wide-area coverage - poor connectivity or inaccurate location data could lead to missing units and loss of revenue.

These companies' shared vehicle services similarly depend on reliable mobile connectivity to complete customer transactions. The importance of flexible and reliable connectivity to this market is showcased by the recent news that Uber could potentially offer in-app embedded subscriber identity module (eSIM) solutions in the future to facilitate transactions, even in areas where customers have no mobile data.

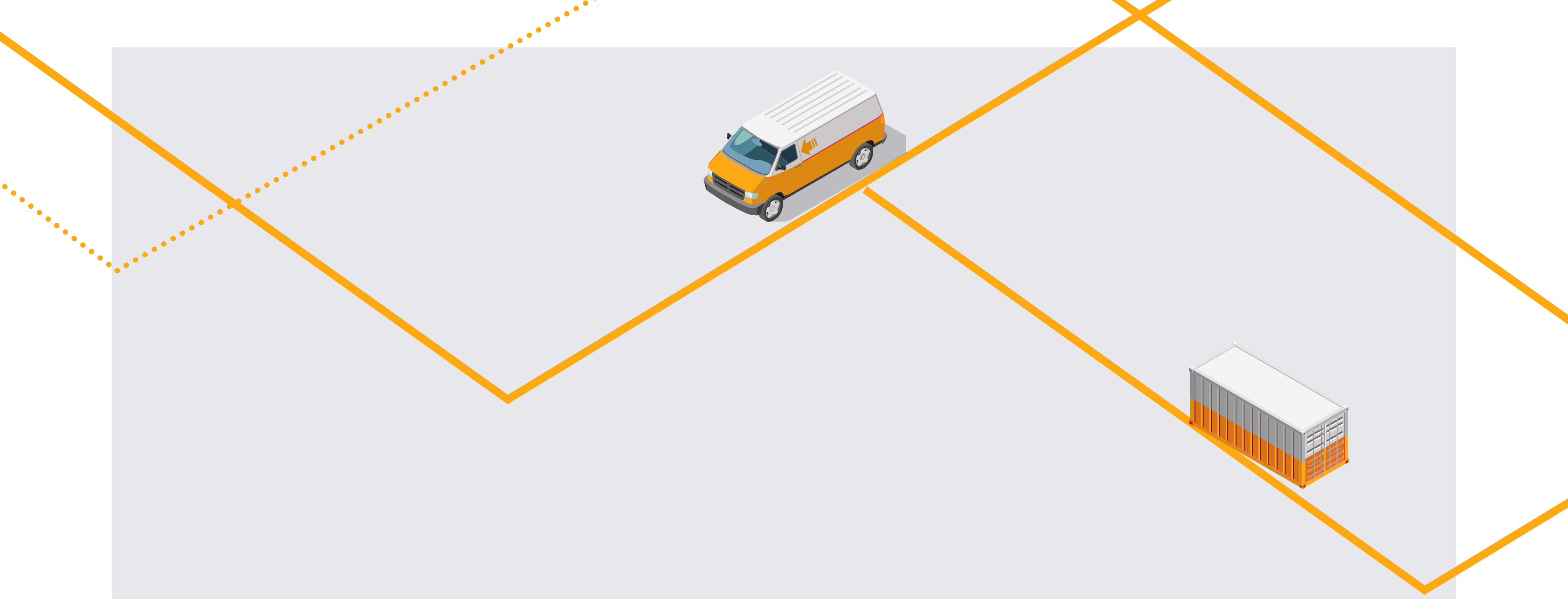
Implementation struggles for advanced fleet management use cases

Fleet management use cases like asset tracking and protection, tyre and engine monitoring, and video monitoring can greatly enhance a company's fleet operations and efficiency. However, like all digital transformation projects, several implementation roadblocks can slow a solution's time to market, impacting a fleet manager's ability to adopt the latest fleet management use cases.

A primary concern of fleet managers when implementing a new fleet management technology is cost. In one survey conducted by ABI Research, 45% of enterprises with fleets cited cost as their biggest barrier to tech implementation. Many also cited a lack of internal infrastructure as the biggest challenge in becoming a more data-driven organisation. Purchasing the necessary infrastructure for advanced fleet management use cases - like new dashcams or thousands of new battery-powered sensors - can be a costly endeavour for enterprises that is hard to justify.

In addition, fleet managers often do not know where to begin when trying to digitalise their fleet, with some ▶

[5] https://www.asisonline.org/security-management-magazine/articles/2023/10/road-safety/telematics-road-safety/#:~:text=Reduce%20insurance%20premiums.,crashes%20by%20around%2050%20percent.



relying on trusted system integrators (SIs) for guidance. Vendor ecosystem confusion can also lead to vendor lock-in, as some fleet managers would prefer to have one solution vendor for tyre, engine, fuel and video monitoring use cases. Though this reduces the complexity of an FMS, it can limit a customer's choices and capabilities.

Future fleet applications

Fleet management applications have undergone unprecedented digital transformation in the last two decades. Use cases quickly graduated from simple location tracking to real-time vehicle performance monitoring. The fleet management industry is now preparing for another wave of innovation as fleet electrification, autonomous driving, and vehicle-to-everything (V2X) communication demand even better data management and wireless connectivity capabilities.

Electrification considerations

The transportation industry is in the midst of an electric revolution. Commercial fleets are transitioning to electric vehicles (EVs), with forecasts predicting that three million commercial EVs will be on the road worldwide by 2030[6]. Fleet operators who have yet to make the switch are preparing for this approaching transition by collecting reams of data from their diesel or gasoline-run vehicles, seeking to understand their fleet's average mileage, fuel capacity and fuel consumption to anticipate how their routes will change when adopting EV vehicles. Fleet operators must also collect and analyse data about fleet engine health and vehicle lifecycles to determine the best time to retire their fuel-based vehicles. Fleet electrification has, therefore, created enormous amounts of telematics data, driving demand for advanced cloud applications that can do this type of analysis.

Low latency in EVs is crucial for enhancing the responsiveness and reliability of real-time communication. This includes reducing data transmission errors, ensuring data integrity, enabling vehicle systems to react quickly to changes in the environment, potential malfunctions and road safety situations. By improving latency, EVs can better manage critical functions like adaptive driving assistance, collision avoidance and other safety systems, thereby improving overall vehicle performance and safety.

Autonomous driving

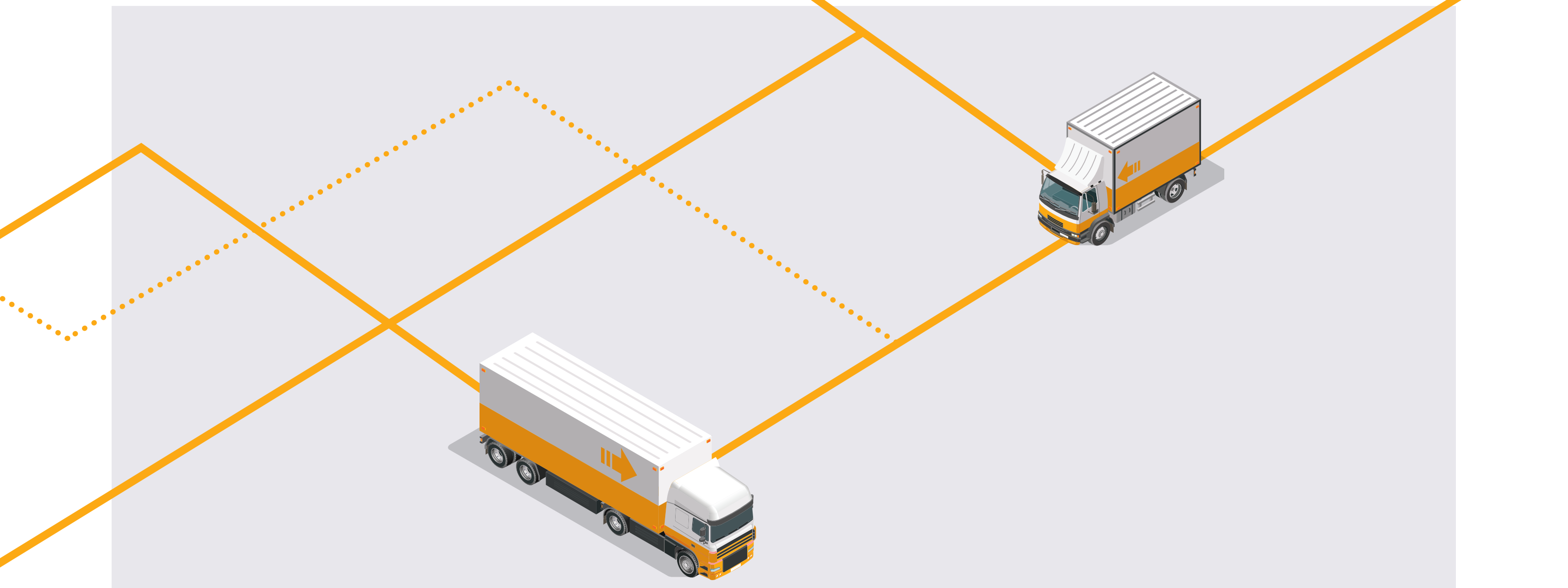
Creating autonomous trucking and commercial fleets has become a significant strategic goal for vehicle OEMs like **Volvo**. While fully autonomous vehicles are nowhere near the point of mass adoption, glimpses of a driverless future can be gleaned from current ADAS solutions with semi-autonomous features like automated steering. Categorised as Level 1 or Level 2 automation, these current ADAS solutions already require a complex array of sensor, video, and computing technology to partially aid the driver. Levels 3, 4, or 5 automation, where a vehicle can monitor and respond to the exterior environment without much or any human supervision, will require even more advanced technologies and will create an unprecedented influx of telematics data for fleet managers to use. In the future, enterprises will require ultra-reliable connectivity for the anticipated levels of data transmission.

V2X communication

V2X is a communication technology that enables a vehicle to transmit data to different devices in its environment, including infrastructure like road signs and other vehicles. The V2X communication vision is ambitious and predicated on an unprecedented level of connected things sharing the same communication protocols. If established, V2X communications would improve road safety and result in more efficient traffic coordination. Seen as a major use case for smart cities, V2X has the potential to transform the entire transportation market.

Connectivity is the cornerstone of future V2X endeavours. Vehicles will need the support of widespread, low-latency cellular networks to communicate with each other and ▶

[6] https://www.abiresearch.com/blogs/2023/06/07/commercial-fleet-electrification/



surrounding connected elements. V2X use cases will necessitate widespread 4G or 5G connections, with 5G's advanced speed and low latency likely providing better support to the large-scale use cases envisioned by V2X proponents.

Connectivity is king in the future of fleet management

All future fleet management use cases - including the near-term electrification of vehicles or the far-off V2X vision - will result in a massive increase in telematics data. Funnelling that data from vehicle gateways to cloud applications will require wireless communication companies that can provide uninterrupted connectivity.

Traditional approaches simply cannot fulfill the demands of next-generation telematics use cases. Mobile network operators (MNOs) deliver critical network services, but the scope of MNOs is severely geographically limited. IoT mobile virtual network operators (MVNOs) have been uniquely equipped for the tasks of more agile connectivity services by delivering more consistent coverage through a more globalised, agnostic approach, but can also be limited by dependency on MNOs, technology and logistical hurdles, and a lack of infrastructure ownership.

What emerges is a new kind of IoT software-as-a-service (SaaS)-based service provider that uses a unique, core network-owned infrastructure that is cloud-based that extends coverage from MNOs across the world through local points of presence (PoPs) for localised global connectivity. Advanced cloud-based connectivity management platforms give flexibility and cut the ties of legacy connectivity management platforms (CMPs) to empower organisations to have real-time insights and control over deployed devices.

ABI Research forecasts that data and analytics services revenue in the fleet management market will reach nearly US$75 billion in 2030, underscoring the need for strong connectivity partners that can support the industry's data-driven ambitions.

Network types and requirements

4G LTE networks are a dominant connectivity choice for fleet management use cases, especially as 2G and 3G networks are now being sunset around the world. The wide adoption of 4G, its consistent coverage and versatile throughput options can support a range of higher-throughput fleet management use cases like cargo tracking, fuel management and video-based use cases like driver behaviour monitoring. LPWA networks like LTE-M and narrowband-IoT (NB-IoT) are a cost-effective choice for low-data asset tracking and remote monitoring use cases.

However, LPWA and 4G networks can seem limiting for fleet applications when compared with 5G networks. 5G networks have exponentially faster data speeds than 4G networks and ultra-low-latencies, but its slow adoption and inconsistent geographical coverage has limited its impact on the fleet management market. However, it can be easier to adopt this developing connectivity technology through a network provider that owns the core network infrastructure as a more direct approach. The piecemeal rollout of 5G can create hurdles when trying to tie together an approach that utilises multiple network providers or MVNOs. A robust network provider can provide service using multiple MNOs within a region - in a sense, aggregating the 5G rollout of each one to maximise 5G coverage nationwide and globally.

5G adoption will slowly grow in the near term when more network rollouts occur and advanced fleet use cases like video monitoring and autonomous driving make headway in the market. Satellite connections will also steadily increase in the fleet management market, as being connected continues to be critical for fleets in remote areas with limited cellular coverage.

Importance of coverage and eSIM

Commercial trucking fleets often traverse geographical areas that offer varying levels of cellular coverage. Fleets can travel through rural and metropolitan areas and across borders, entering and exiting regions with different national operators and 4G, 5G, or LPWA coverage ▶

and availability. These vehicles must have connectivity throughout, as many fleet management use cases require uninterrupted, real-time insights into the vehicle's location, health and performance.

Given these requirements, it is natural that MVNOs would be fleet management partners. MVNOs specialise in aggregating operator profiles on a single subscriber identity module (SIM) and aggregating connectivity from different operators' networks on a single profile. This enables a device to seamlessly move between carrier networks, creating an uninterrupted chain of connectivity across various regions and countries.

Cross-carrier connectivity has become even more flexible as MVNOs have transitioned to eSIM. eSIM allows customers to remotely provision SIM cards after the point of manufacturing, meaning that customers can activate devices and provision them with new carrier profiles, over-the-air (OTA) and remotely. The technology eliminates physical SIM swapping and network profile lock-in, allowing users and their MVNO suppliers to dynamically change networks depending on their needs. Fleet managers can now easily change their devices' network profiles depending on a fleet's route or uniformly administer remote updates to a large group of devices.

This touchless, single-stock keeping unit (SKU) approach to global connectivity is not only capable of switching networks OTA, but can also support adherence to data sovereignty and localised access, while removing dependency on roaming.

What combines the strengths of an embedded universal integrated circuit card (eUICC) with remote, automatic switching on networks is a multiple international mobile subscriber identity (multi-IMSI) approach that uses eUICC. A multi-IMSI technology solution is all managed through a single connectivity provider, which holds the existing relationships with multiple network operators, each providing its international mobile subscriber identities, and then held in a single SIM. When devices need additional coverage or a network fault is detected, these profiles can be switched OTA, allowing for remote SIM provisioning of the new IMSI, in real-time.

This easy management and uninterrupted coverage will become even more impactful as fleet management use cases require more real-time data processing and decision-making. As a result, more fleet managers will seek out a partner with nationwide coverage and a global footprint that supports connectivity in as many countries as possible across all network types, including 2G, 3G, 4G, 5G, NB-IoT and LTE-M network coverage.

Connectivity and platform providers

Enterprises can take several approaches when crafting a connectivity strategy for their fleets. Companies can purchase connectivity and a CMP separately or they can buy a bundled connectivity and CMP offering from an operator or MVNO. Each approach has advantages, but purchasing both elements separately, or buying from an MNO, can be limiting for fleet managers when facing a new range of applications that require guaranteed connectivity and uniform management.

Purchasing connectivity and platform separately

Purchasing connectivity and a CMP from two separate suppliers is an approach that can be adopted in the industry. If an enterprise has specific demands for both its connectivity and management platform, and is aware of all the available suppliers, it can feel empowered to handpick the two offerings it believes are best for its company goals. Companies that purchase the two separately typically lean on SIs to guide and integrate their purchases.

Purchasing connectivity and a CMP from two separate suppliers leaves enterprises in a scenario where the dependency on SIs to guide and integrate their purchases can arise. Only a limited number of companies choose this option, as merging a connectivity offering with a separate connectivity platform requires an immense amount of time and money, and has a great risk of failing if the wrong supplier is chosen or the systems are not tightly integrated. An enterprise that chooses this option must integrate different operator connectivity profiles on a single, third-party platform to ensure device visibility and control across networks and coverage areas. These integrations would be extremely complex and time consuming.

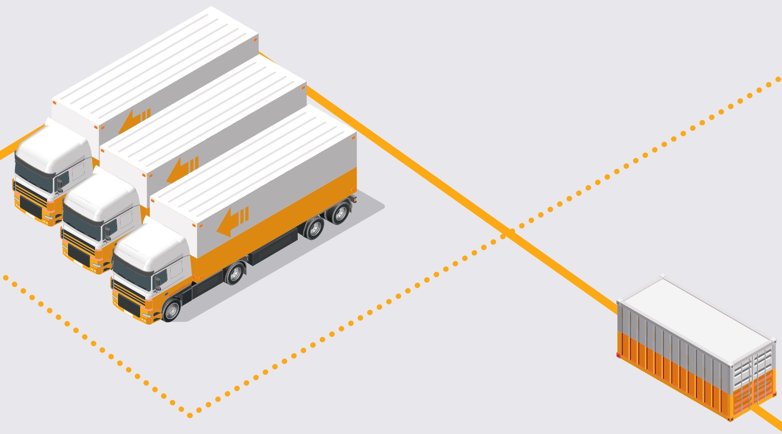
As a result, this option is mostly reserved for large companies with a strong incentive to control every part of their connectivity and platform system, and may simply have been an inconvenient necessity in the early days of fleet management when no end-to-end suppliers existed. Today, however, most companies choose an end-to-end supplier that typically provides a bundled connectivity and CMP offering.

Choosing a company that specialises in CMPs, especially one that can provide customers with SIMs (either multi-IMSI or eUICC), creates a streamlined, fast time to market approach. In addition, when selecting a provider, being able to bring your own connectivity enables customers to bring their own IMSIs to integrate into the provider's SIM profile and CMP. In doing so, there is no need for an external SI.

Purchasing connectivity and a platform from an MNO

MNOs are often large organisations with an extensive history of providing connectivity to a range of enterprises and consumers. Fleet managers might look to an MNO's experience and be enticed by their bundled connectivity and platform options, particularly if a fleet is expected to stay in the home country of a national MNO. MNOs have also traditionally promoted themselves on the grounds of longevity, as they have been in business for so long. They are, therefore, likely to be in the market to support a fleet manager for the duration of their vehicles' lifetimes.

However, there are several drawbacks to this approach, especially when considering fleet management use cases that require uninterrupted connectivity across ▶



various regions and networks. MNOs do not typically have roaming agreements with other operators domestically, meaning fleet managers who choose an MNO as their connectivity and CMP supplier would be locked into a single operator's network for all national deployments. In addition, an operator's global connectivity is typically dictated by its roaming agreements with international partners, potentially leaving coverage gaps in key international areas. It is also more difficult for customers to achieve the same quality of service (QoS) and platform functionality from an MNO when operating on its international partner's network. These disadvantages could have severe implications for fleet management use cases that require continuous coverage and uniform connectivity management across borders.

Purchasing connectivity and a platform from an MVNO

Enterprises can also purchase a bundled CMP and connectivity offering from an MVNO. As connectivity resellers, MVNOs can aggregate many operator networks on a single SIM and create a global coverage portfolio. MVNOs also combine these networks together into a single platform and can offer the same platform features, performance and user interface across regions and network connectivity types. Virtual operators can guarantee this international connectivity and connectivity management at a regulated price point that is not subjected to complicated roaming fees or shifting partnerships.

For MNOs, connectivity is frequently the end game, with their existing platforms allowing customers to manage connectivity for the sake of selling IoT tariff plans. For MVNOs, connectivity is just the starting point and is the building block on which they create value through the guaranteed continuity of service availability, at a predictable price point, and often with specific vertical- or application-specific experience. MVNOs are in the business of conducting all the back end plumbing, so that their customers do not have to and can purchase services that they know will 'just work'.

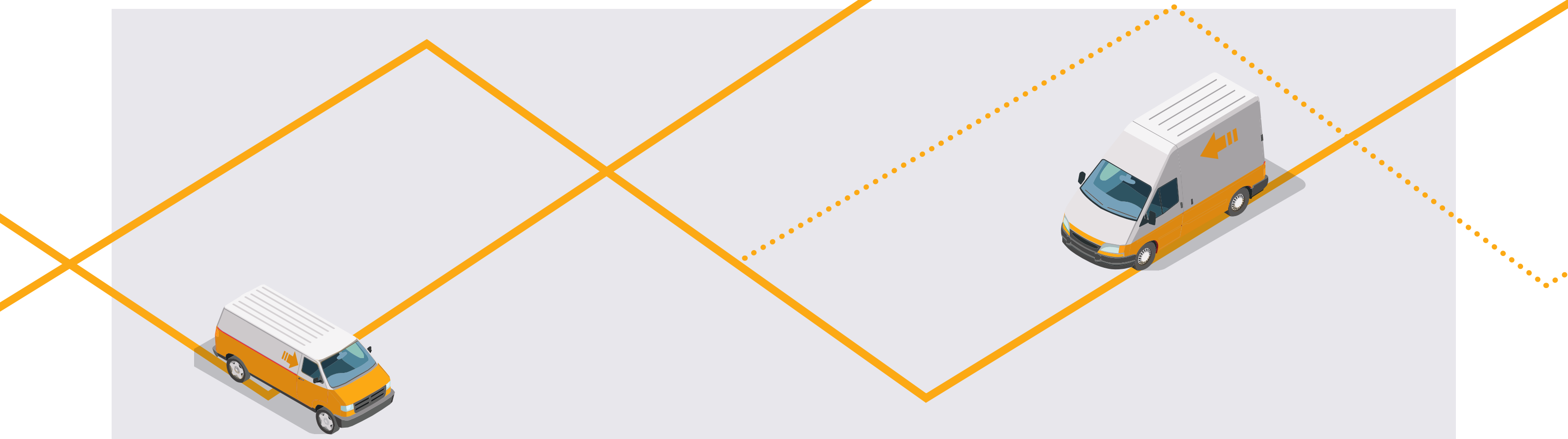
Many current fleet managers already benefit from MVNOs' carrier-agnostic platforms and connectivity services. But future fleet management use cases will require something even greater. As the fleet management market evolves to include more advanced use cases, fleet managers will require a next-generation connectivity provider - merging the best of both MNO and MVNO worlds - that can deliver ultra-low latencies and effective localised, yet global performance across different networks, countries and device types.

Next-generation connectivity and platforming

The right MVNO partner for fleet managers in the future must establish a unique global presence in the IoT industry by building a network of highly resilient connectivity with a maximal number of local PoPs around the world. This arrangement results in fast local connectivity, globally. This type of localised global footprint will enable MVNOs to lead the way in supply-side provisioning for fleet management by guaranteeing the effectiveness of applications, including video monitoring, that increasingly require low-latency data communications. This, in combination with eSIM for ultra-flexible connectivity around the world, will provide the back end support that fleet managers need as they prepare their vehicles to travel into and out of new areas around the world and in different networks.

However, fully redundant, highly available and high-performance connectivity is only really usable in combination with a cutting-edge CMP designed to oversee large-scale fleets of devices on the move. Granular visibility will be necessary across a range of device types, monitoring data usage, device behaviour and connectivity performance, while managing OTA configurations and administering continual security checks and tests. A full breadth of connectivity, monitoring and security services will be needed to allow fleet managers to receive real-time insights into their fleets around the world, and is necessary to optimise the performance of those devices that enable business-critical use cases; for example tyre, engine and fuel monitoring. Such an offering will be a necessary support system today in order for enterprises to prepare for the next wave of fleet management innovation.

A key consideration in fleet telematics is the need to balance capturing real-time information with battery optimisation. Latency is a crucial element in this balance, ▶



particularly when considering low-power telematics use cases, where the expectation is that the battery lasts the entire device lifecycle. Locally derived connectivity significantly decreases latency, compared to roaming, and can shorten data communication time by a third. While this might not seem like much at first glance, this can ultimately double the lifecycle of a device's battery - just through latency alone. Other technologies like extended discontinuous reception (eDRX) and power saving mode (PSM) when implemented alongside LPWA networks can deliver on the balance of pertinent data insights, while also optimising battery life.

Case study: A competitive edge in automotive IoT with floLIVE

AutoMobility is a leading distributor and manufacturer of automotive aftermarket electronics. Its extensive product portfolio includes dash cameras, app-based remote vehicle starters and security features. The company has innovated its products as customer demand for connected devices has grown. For example, the company has integrated its remote vehicle starter capabilities into a smartphone application that also measures vehicle metrics. This solution requires resilient mobile communications between sensors, the vehicle and the user's smartphone(s). With **floLIVE**, AutoMobility could offer its customers consistent global coverage for seamless user experience and simplified management. In addition, by using floLIVE's integrated platform, alongside its connectivity services, AutoMobility accelerated its time to market and now has comprehensive visibility into its devices and network behaviour. What AutoMobility gained from this partnership specifically is:

Robust connectivity: floLIVE offers a large IMSI library supported through UICC, eUICC and multi-IMSI, which offers both a single-SKU SIM approach for streamlined logistics and allows AutoMobility to achieve worldwide connectivity through a wide choice of network operators.

Single SKU: Instead of going from provider-to-provider to source connectivity, AutoMobility can utilise floLIVE and have access to a global connectivity library supported on floLIVE's own mobile core network infrastructure - and all profiles are available on a single SIM, removing the complexities associated with managing multiple SKUs.

Application programme interface (API) integration: For increased flexibility and interoperability, floLIVE exposes its API for back end integration across technologies and hardware.

Visibility and management: floLIVE's connectivity management platform makes it possible for AutoMobility to achieve granular visibility in device and network behaviour for comprehensive support and management.

Summary

The fleet management market has matured from simple track and trace use cases to advanced video-based monitoring and autonomous applications. Ushered in by improvements in IoT and wireless communication technologies, this new era of innovation will call for even greater advancements in sensors, cloud services and connectivity technology.

Each fleet management vertical will undergo some digital transformation as new FMSs and wireless communication networks like 5G and satellite become more available. As fleet managers assess connectivity and CMP suppliers for the future, they will choose a partner that can offer uniform management across a fleet of devices and facilitate the quick, global connectivity that will be foundational to fleet management's evolution. ■

IoT anywhere: Harnessing satellites for global IoT coverage

Satellites have been used for decades in applications such as navigation, weather forecasting, surveillance and TV broadcasting. But what about IoT, asks Sarah Woon, a research analyst at Beecham Research, explores where IoT fits in

In 2022 the number of satellite-IoT connections was estimated to be 5.23 million - less than 0.04% of the number of IoT device connections worldwide. Seen as a costly alternative, satellite use is currently low.

However, with demand for remote IoT deployments growing rapidly and terrestrial networks covering less than 20% of the earth's surface, satellite is fast becoming a necessity in global IoT solutions. This is encouraging the market to come up with more cost-effective options.

This short article identifies three developments facilitating this change. For more details, see Beecham Research's new free report – 'IoT Anywhere: Wireless Data Wherever You Need It'[1].

Increased compatibility with low-power technologies

Historically, satellite connectivity has been limited to proprietary technologies, reducing the potential for low unit costs.

Now, compatibility with standards-based technologies such as NB-IoT and LoRaWAN creates opportunities for lower cost, low-power, low-data IoT satellite solutions. This is intended to make it more feasible from a business perspective to deploy IoT in locations that terrestrial networks cannot reach.

Small-sat operators on the rise

Although the market is currently dominated by a few major satellite operators, there is growing momentum from small-sat operators. Many of these ▶

[1] http://www.beechamresearch.com/iot-anywhere/

SPONSORED ARTICLE

players specialise in ultra-low orbit nanosatellites that are relatively cheap to make and launch.

This enables them to offer more affordable satellite subscription services.

Hybrid networks provide satellite coverage at a fraction of the cost

Roaming devices pose a particular challenge for IoT connectivity. Crossing borders can create disruptions since it may take time to configure to a new network. Alternatively, if the device is required to traverse the ocean or a remote area where there is no terrestrial connection, no data can be collected during this time.

Now, multi-profile SIMs can be implemented in IoT devices enabling them to connect to terrestrial networks wherever available and satellite where they are not. Since subscriptions to terrestrial services remain cheaper than satellite subscriptions, satellite access 'only when needed' is a much more cost-effective solution than employing solely satellite.

As well as a variety of cellular hybrid satellite options (including 5G), LoRaWAN inter-satellite networks can be created to provide low-power global coverage.

To understand the connectivity choices now available and read more about satellite-IoT, including independent market research and insights from industry experts, download and read Beecham Research's new free report – IoT Anywhere: Wireless Data Wherever You Need It.

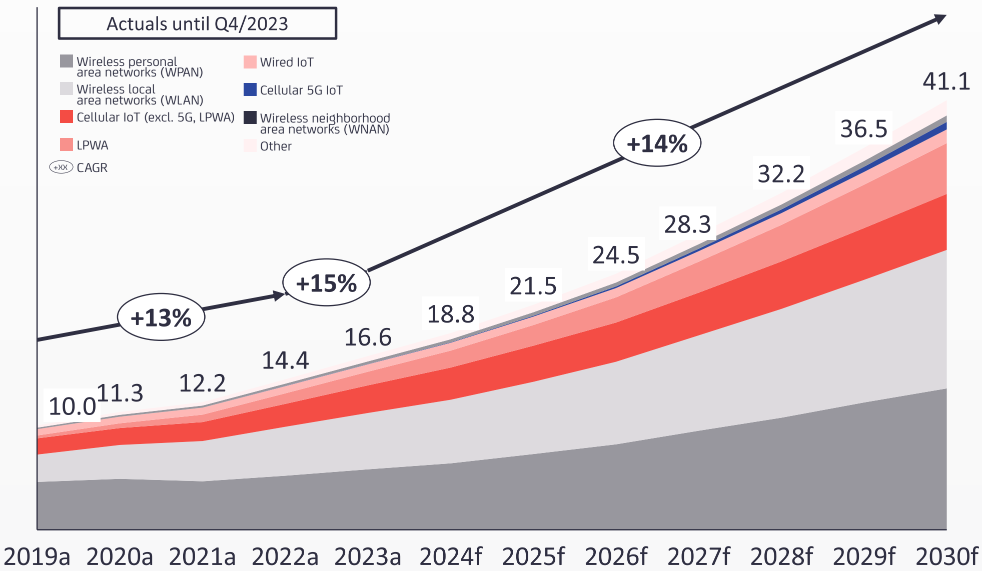
www.beechamresearch.com/iot-anywhere/

Now, multi-profile SIMs can be implemented in IoT devices enabling them to connect to terrestrial networks wherever available and satellite where they are not

IOT ANALYTICS

STATE OF IoT 2024: NUMBER OF CONNECTED IoT DEVICES GROWING 13% TO 18.8 BILLION GLOBALLY

Number of global active IoT connections (installed base) in billions



Source: IoT Analytics Research 2024—State of IoT Summer 2024.

ANALYST OPINION

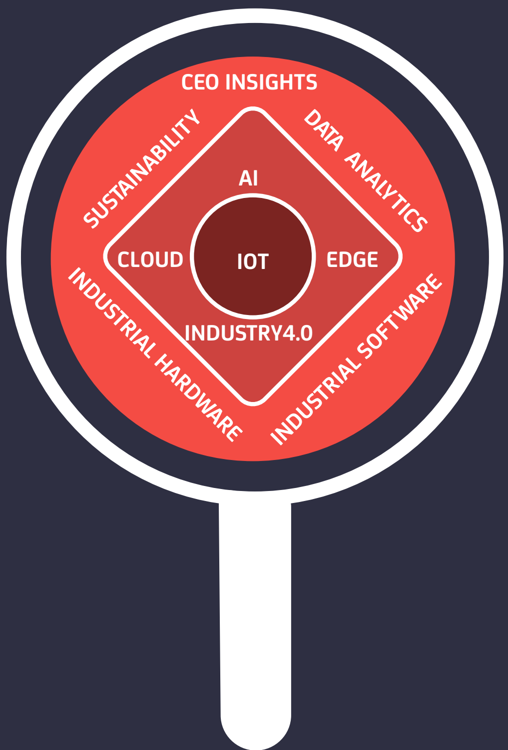
"Edge AI is fundamentally transforming the IoT landscape by allowing edge IoT devices to process data locally, reducing latency and enabling real-time responses. The integration of AI technologies, including generative AI and edge AI, is a significant trend in 2024, highlighted by increased discussions among corporate leaders. With companies like NVIDIA and AMD heavily investing in edge AI, the convergence of these technologies with IoT will drive the development of more intelligent and autonomous devices, leading to broader adoption of IoT solutions across various sectors."

-Satyajit Sinha, principal analyst at IoT Analytics

IoT ANALYTICS: ENABLING INFORMED IoT DECISIONS THROUGH QUALITATIVE AND QUANTITATIVE MARKET RESEARCH

RESEARCH AREAS (SELECTION)

- 5G IoT and private 5G
- Cellular IoT module and chipsets
- Edge computing
- Generative AI
- IoT connectivity
- IoT semiconductors
- LPWAN
- Operator pricing
- Satellite IoT
- eSIM and iSIM



CUSTOMER (EXAMPLE)

HOW CLIENTS LEVERAGE OUR MARKET RESEARCH

CLIENT

Multinational MNO

PURPOSE

Staying attuned to industry trends and making more informed decisions, ensuring their solutions are aligned with market dynamics

QUOTE

"Your content blows the other reseachers out of the water. If I have a question based on a report, the answer is almost always within the report".

- Product manager, leading chipset manufacturer

QUOTE

"IoT Analytics doesn't just provide high-quality data. Their valuable insights enhance our understanding of the ever-changing market dynamics, leading to impactful actions."

- Marketing manager

AVERAGE CUSTOMER SATISFACTION SCORE: 4.5/5

ALL CUSTOMERS RATE US 3 OR ABOVE WITH 60% RATING US 5 OUT OF 5

Customer Satisfaction Survey 2023

IoT Now: ISSN 2397-2793

2024 • VOLUME 14 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

Ryan Keefe explains why it's time for SIMPL IoT connectivity

IoT Now CEO Guide to Mitigating Roaming Risks 2024

PLUS: How to navigate the multicarrier management maze • Have permanent roaming regulatory issues been resolved? • Mobile operators to cash-in on IoT roaming • How to unlock the future of agriculture with eUICC • Is IoT data and security management ready for cloud-connected IoT devices? • Read the latest News, Features and Interviews at **www.iot-now.com**

It's time for IoT connectivity to keep it SIMPL

Ryan Keefe, the chief operating officer of SIMPL, tells Matt Hatton, the founding partner of Transforma Insights how the company is disrupting the permanent roaming market by preloading its SIM card with native operator profiles. This brings flexibility and choice with an easy-to-use management via the SIMPL platform

The biggest misunderstanding or unknown or maybe intentional omission from some providers is not sharing that roaming agreements between MNOs are not perpetual

Matt Hatton: At Transforma Insights we do a lot of work looking at how cellular-based IoT connectivity is delivered, including our recent Communications Service Provider IoT Peer Benchmarking report. One of the things that comes up is that there is continuing friction around both roaming and the emerging eSIM localisation. How do you see it?

Ryan Keefe: Our view is that there's a natural friction between the emerging technologies we are working with and some of the existing permanent roaming solution providers in the space. They've spent a lot on capital investment in infrastructure and until now it did require heavy integration. For every carrier you want to deploy an international mobile subscriber identity (IMSI) with, you typically need a subscriber management data preparation + (SM-DP+) integration. One of the challenges with some of the existing players in the space is that domestic US mobile network operators (MNOs) are not willing to license or lease IMSIs. So, most end up with IMSIs from international carriers to roam back into the US, where there is high risk of permanent roaming. But with the evolution of the GSMA standards it's much easier to localise and be disruptive.

The localisation that we provide is for specific carriers in the US pre-loaded at time of manufacture, and then the ability using SGP.22+, we refer to it as .22+ or 22 1/2, and with work in progress to use SGP.32, to be able to localise with activation codes rather than doing a full SM-DP+ integration.

With the SIMPL solution we can get an activation code from any MNO and download it to the SIM alongside the preloaded **T-Mobile** and **Verizon Wireless** profiles. The activation code is essentially the extracted QR code string.

What we've done is disruptive to the permanent roaming models. Our SIM card comes preloaded with T-Mobile and Verizon profiles and new profiles can be added with a carrier activation code. If it's a carrier that we already contract with, then they can buy services from us. If the customer has their own carrier agreements, they can bring their own commercials and manage it in our single pane of glass, SIMPL, side-by-side.

MH: Thinking specifically about permanent roaming, what are the big problems? And specifically problems in the US.

RK: The biggest misunderstanding or unknown or maybe intentional omission from some providers is not sharing that roaming agreements between MNOs are not perpetual. Customers and solution providers will be very exposed to increased rates, capped usage, capped number of SIMs or termination of agreement between MNOs.

And one of the things that most people aren't familiar with is QCI which stands for quality- ▶

SPONSORED INTERVIEW

of-service class identifier. There are nine classes of SIM priority. In the US, roaming SIMs are QCI 9. For context, a conversational voice connection is typically a QCI 1 priority on the network. First responders in the US are often on QCI 6, which is still pretty high. Most of the rest, where consumer, wholesale and business sit, are QCI 6 or 7. QCI 9 is where all roaming traffic resides, this traffic has the lowest priority assuming there's room on the network, translating into reduced reliability and high latency.

There are numerous permanent roaming customers with buyer's remorse, citing latency and reliability issues. They're looking to come back to domestic networks in the US, but they want to be able to use a single SIM with multiple carriers and download more if they need more. This is really impacting a lot of businesses. Customers are definitely feeling that pain in the US and Canada. That's why we prefer the localisation and why we've built what we've built.

Another thing to consider is quality of revenue, a term more common with private equity. The economics of roaming SIMs generally look better than domestic, so naturally as you're building out your business model and looking at recurring costs, your goal is better margins. But that's not the whole story. I've personally been hired by private equity firms to perform due diligence, and increasingly they scrutinise the risks associated with the revenue derived from permanent roaming agreements. ▶

Ryan Keefe
SIMPL

In one case I know of, it reduced the valuation by 45% because they couldn't guarantee the SIMs would be out there in 30, 60 or 90 days after closing

For instance, roaming agreements between operators is best case a three-year term. But in many cases the carrier can't and won't tell how much time is remaining. So, you may be building a business today in security or point-of-sale where devices might be out there 5-10 years, and you have no idea how long is left on the roaming agreement upon which your connectivity provider is relying. And for someone looking to invest in that kind of company and starting to ask those questions it can be a heavy hit to your valuation. In one case I know of, it reduced the valuation by 45% because they couldn't guarantee the SIMs would be out there in 30, 60 or 90 days after closing. It's something else to consider in the US. And I get it, as a start-up or enterprise venturing into new connected devices, you'll take all the margin you can get. But five years later you have a base built on roaming and PE now has this type of research on their due diligence check list.

MH: What about some horror stories? Do you have some specific examples?

RK: I don't know if I can name names but I have many examples. While working for a mobile virtual network operator (MVNO), I was engaged in a dispute between a US and Canadian carrier where the MNVO's costs increased 25x overnight. In another case, there was a dispute between two MNOs where the main carrier being roamed onto increased rounding up from 1KB to 100KB sessions.

I've also experienced a tier 1 US and a tier 1 EU MNO getting into dispute over 40,000 connections, which by today's standards isn't very much. The US MNO sent a cease-and-desist with 48 hours' notice terminating SIMs that were permanently roaming. Can you imagine the pain the MVNO, and underlying customer went through? This is not an isolated incident.

As you're no doubt aware, the tier 1 US MNOs have become much more aggressive at terminating permanent roaming agreements over the last few years as they seek to stop the revenue bleed they're experiencing from unapproved practices. This has significant downstream effects and has resulted in more than one solution provider filing for bankruptcy

And in yet another experience, several years ago, a Tier 2 US operator roaming onto a Tier 1 operator's network with 500,000 devices was given notice to cease and desist. And the same thing happened again last year with a different Tier 2 operator.

MH: Has the situation changed in the last couple of years? How does the landscape change with eSIM localisation and how do you see the network operators' approach evolving?

RK: This is interesting. Over time you can see the pendulum swing back and forth between the carriers and the aggregators. For instance, initially the carriers would send the business towards the aggregators. Then we saw the carriers invest heavily in IoT, for instance in connectivity management platforms like **Jasper**, **Ericsson**, and **Vodafone** building GDSP and signing customers directly. And they reduced the commitments so anyone could sign direct. What's been interesting with localisation is the pendulum is swinging back to aggregators. We see the MNOs wanting to partner with them for localisation. One big reason is that the carriers won't agree to purchase orders with each other for profiles, so they need to partner. And then the aggregator can work to develop the agreements for the other operators.

And the world has changed. Back 15-20 years ago most of the solution providers had no existing base but today they do. If you're trying to get into disrupting the space now you have to account for that. Most people don't have an escape plan between operators. The buyers don't want a new platform or new application programme interfaces (APIs). So, the big question is how do you manage multiple carriers with legacy and new SIMs on 'day two'? So, we put a big emphasis on that part, creating that horizontal experience with SIMPL.

MH: That brings us on to the topic of the single pane of glass interface across multiple connectivity providers, right?

RK: Yes, that's what I'm talking about. The eSIM evolution solves the localisation problem. But the 'day two' item on the list is how to manage it across all those operators. The SIMPL approach was to integrate with all the platforms, the ▶

customer can bring their own connectivity or buy from SIMPL. All with the same horizontal experience for diagnostics, alerts and automation, and cost savings dashboard enabling them to manage both old and new SIMs together and gives the industry a plan for moving on from using other carriers.

MH: Can I ask you also about online channels? This seems to be a big feature of the SIMPL approach. We see some connectivity providers shy away from online because of most customers' requirements for customisation. But for other customers it's exactly what they want. Is that how you see it?

RK: We identified this as a need in the market after doing a lot of research. One thing we discovered was that according to **Gartner** 80% of research by the next generation of buyers is online. And 44% don't want any interaction with a salesperson at all, and for it to be completely self-serve. We estimate that for 60% of new generation buyers and heavy influencers we have a silver bullet with online channels. The other 40% need more touch points, and those are usually bigger clients. We launched our B2B ecommerce platform 90 days ago and we already have people coming in and buying in a completely self-serve way. These customers can log into our B2B commerce site and have SIMs and service the same day vs. weeks or months from other providers.

MH: One trend we see is that a sophisticated online channel capability is giving customers some confidence of efficient and joined-up fulfilment. Is that how you see it too?

RK: We think it is. We have some ecosystem clients who are more hardware oriented. And we're finding it good to push to these online channels. So, it's not just a joined-up mechanism for us internally but also including the client processes too. I've been joking for years that you can **Uber** a helicopter faster than you can purchase SIMs. That's the reason for us pushing the B2B commerce experience.

MH: Talk me through some of the other features that you see as being the ones that customers really value from a connectivity standpoint.

RK: In addition to the other aforementioned features, mid-cycle billing changes is a big one. It's something the MNOs allow but the MVNOs often don't. A few of our competitors have changed their approach because SIMPL has been offering this. We've even alerted customers before a billing cycle ended, giving them the chance to resolve an issue and avoid a million-dollar overage.

One key advantage we offer is helping customers identify SIM bleed or dormancy waste - an insight that some competitors only share with c-level approval. In addition, our transparency sets us apart; we openly share data on over- and under-utilised pools, whether the carriers are purchased from us or ones you've brought yourself, along with automation tools that drive savings.

Finally, we expose a single API and SIM lifecycle experience connecting to 100 MNOs and delivering 200 built-in key performance indicators (KPIs) with interactive analytics. Customers can also buy or bring their own MNO. Interactive is the key word with our analytics experience.

MH: As another part of our research we've found an increasing importance for connectivity providers to also get involved with the device side of things, is that also part of your experience?

RK: We do offer full kitting and staging and fulfilment for connected things. The client buys the hardware, drop ships it to SIMPL and as orders come in, we fulfil, insert the SIM, provision, update firmware, test and handle support, return merchandise authorisations (RMAs) and even potential churn and saves when a customer calls to cancel.

MH: What message can enterprise buyers take away from our conversation?

You no longer have to be handcuffed to the risk and inflexibility of permanent roaming but can instead now benefit from the power of localisation and data transparency to improve quality and revenue. ■

I've been joking for years that you can Uber a helicopter faster than you can purchase SIMs. That's the reason for us pushing the B2B commerce experience

https://simpliot.com

Navigate the multicarrier maze: How SIMPL revolutionises IoT and fixed wireless deployments

In today's hyperconnected world, where devices outnumber people and the Internet of Things (IoT) is rapidly expanding, managing multiple mobile network operators (MNOs) for IoT and fixed wireless deployments has become an intricate, almost Herculean task. Each MNO operates within its own technological bubble, offering proprietary platforms that vary in protocols, application programme interfaces (APIs) and management tools. For companies looking to scale across regions, the complexity can be overwhelming. Enter **SIMPL** – a **SIM PL**atform that's taking the chaos out of multicarrier management and making global IoT deployment not just possible, but streamlined, efficient and cost-effective

Picture this: You're deploying IoT devices across the US, Europe, and Canada. In the US, you're deployed with the **Cisco Jasper** platform. Cross the Atlantic, and you're working with **Vodafone**'s GDSP. Up north in Canada, you're **Ericsson** DCP. Then, add the intricacies of integrating home grown platforms such as **T-Mobile's Netcracker**'s deployment, **Verizon**'s Thingspace, and **Telefonica**'s Kite, and it becomes clear - this isn't a simple game of plug-and-play.

Each of these platforms is like a distinct language. Getting them to communicate with each other, without data loss or service disruption, requires not just technical expertise, but a considerable investment of time and resources. For companies operating on tight deadlines and even tighter budgets, the stakes are high. A delay or disruption could mean the difference between market leadership and playing catch-up. ▶

SPONSORED ARTICLE

SIMPL: The unifying force in a fragmented landscape

SIMPL's platform has been designed from the ground up to integrate seamlessly with all major MNO platforms. Whether it's T-Mobile Netcracker, Cisco Jasper, Verizon Thingspace, or Vodafone's GDSP, SIMPL brings them together under one roof, offering what the industry so desperately needs - a single, unified pane of glass.

SIMPL's platform isn't just about integration; it's about simplification. With one-touch onboarding, businesses can deploy their IoT devices across multiple carriers without getting entangled in the technical complexities that typically bog down such operations. Imagine a world where your IoT devices can be activated, managed, and scaled with the ease of flipping a switch - that's the reality SIMPL is making possible.

A blended buy and bring your own MNO experience

In addition to its integration capabilities, SIMPL also offers a unique bring your own MNO experience. This feature allows companies to ingest SIMs from their existing MNO platforms, managing both legacy SIMs and new SIMs from SIMPL within the same unified platform. Whether you're dealing with a legacy SIM estate or rolling out new deployments, SIMPL's platform provides a seamless, single-pane management experience. This ensures that companies can maintain continuity and control over their entire SIM portfolio, regardless of the MNO, all while benefiting from the advanced features and streamlined operations that SIMPL delivers.

Ensure quality of service across the globe

One of the biggest concerns in managing IoT and fixed wireless deployments across multiple MNOs is maintaining consistent service quality. While network performance - such as coverage, latency, and bandwidth - can vary greatly between MNOs, SIMPL focuses on what it can control: the behaviour of your SIMs. Through its advanced analytics and algorithms, SIMPL can detect when SIMs start to behave abnormally, whether they become overly chatty, experience connection failures or exhibit inefficient packet sizes and high usage patterns. This proactive approach allows businesses to quickly identify and address issues that could impact customer experience, ensuring performance is optimised across all regions and carriers.

Scalability and flexibility: the hallmarks of a future-proof solution

In the fast-paced world of IoT, the ability to scale quickly and efficiently is crucial. However, scaling across multiple MNOs is no easy feat. Each platform has its own limitations and scaling strategies, which can lead to bottlenecks and inefficiencies.

SIMPL's platform is built for scalability. By integrating with all major MNOs, SIMPL allows companies to scale their operations without being held back by the limitations of any single MNO platform. Moreover, SIMPL's flexible architecture means that businesses can switch between MNOs as needed, ensuring that they always have access to the best possible service and pricing.

Navigate permanent roaming waters with confidence

In the tangled web of global IoT, permanent roaming regulations can feel like walking a tightrope without a net - one misstep and you're in trouble. SIMPL shines a light on which networks you're roaming on, for how long, and how much data you're using, so you have the opportunity to stay in step with regulatory and contractual requirements.

For businesses expanding across borders, SIMPL ensures you can play by the rules. Consider it your compliance safety net - no matter where in the world your devices wander, we've got your back.

The future of IoT is SIMPL

In a world where managing multiple MNOs has traditionally been a complex, resource-draining endeavour, SIMPL is rewriting the rules. By offering a platform that integrates seamlessly with all major MNOs, unifies APIs, simplifies billing and ensures compliance, SIMPL is not just making IoT and fixed wireless deployments easier - it's revolutionising them.

As the IoT landscape continues to evolve, companies need solutions that can keep pace with their ambitions. SIMPL is that solution. It's more than a platform; it's the future of multicarrier management.

For companies looking to navigate the multicarrier maze and emerge victorious, SIMPL offers the map, the compass, and the key to unlocking their full potential. The future of IoT is interconnected, it's global, and with SIMPL, it's finally within reach.

For companies looking to navigate the multicarrier maze and emerge victorious, SIMPL offers the map, the compass, and the key to unlocking their full potential

https://simpliot.com

Unlock the future of agriculture with eUICC and SIMPL

As the agriculture industry faces increasing pressure to optimise resources, reduce environmental impact, and meet growing global food demand, the integration of connected solutions becomes paramount. Among these technologies, embedded universal integrated circuit cards (eUICC) for both physical (pSIM) and embedded SIM (eSIM) stand out as a transformative tool, enabling seamless connectivity for a wide range of agricultural applications. By adopting pSIM and eSIM technology, the agriculture sector can make use of connected solutions to monitor, analyse and manage various aspects of farming, without the frustration caused by inconsistent cellular coverage, writes Ryan Keefe, the COO of SIMPL

As this equipment migrates across different farms or various sections of large properties, maintaining consistent network coverage becomes a critical challenge

This article explores the benefits of eUICC for the agriculture industry, discusses specific use cases, and highlights the importance of future readiness for **GSMA** specifications, particularly LPAe .22 (although not official, we refer to it as .22+ or .22.5) and .32. We will delve into how eUICC can address critical challenges in agriculture and contribute to a smarter and resilient industry.

The evolution of agriculture and the need for connectivity

In today's rapidly evolving agricultural landscape, even small-scale farmers may depend on over 100 pieces of equipment - ranging from man-powered and robotic tractors to advanced irrigation pumps. This figure represents nearly double the machinery in use just 15 years ago. As this equipment migrates across different farms or various sections of large properties, maintaining consistent network coverage becomes a critical challenge. If a device moves to a new location and loses coverage without the ability to switch network profiles, it effectively becomes a useless brick in the field. Historically, agriculture has been slow to adopt cutting-edge technology, but that's no longer the case.

eUICC in AgTech makes network switching seamless. The future belongs to solution providers who can offer seamless connectivity across multiple native networks, using the latest eUICC technology to ensure that no piece of equipment - and no farmer - is left behind.

The benefits of eUICC in agriculture

1. **Seamless connectivity:** eUICC allow devices to switch between mobile network operators (MNOs), ensuring continuous connectivity in areas with limited coverage. This minimises downtime and ensures data flow across large, geographically dispersed agricultural operations.
2. **Remote management:** eUICC enables remote management of devices, allowing farmers to update network profiles, change service providers and adjust settings without physical intervention. This reduces costs and simplifies managing large fleets of connected devices.
3. **Scalability:** As connected solutions proliferate, eUICC supports the scalable deployment of new devices, crucial for large-scale farming operations with hundreds or thousands of sensors and IoT devices.
4. **Enhanced security:** eUICC offers enhanced security features, such as encryption and authentication, to protect the sensitive data transmitted by agricultural devices, especially for monitoring critical resources like water usage and soil health. ▶

SPONSORED CASE STUDY

Use cases of eUICC in agriculture

1. **Water level monitoring in soil:** Efficient water management is crucial for sustainable agriculture, especially in regions prone to drought or water scarcity. eUICC-enabled soil moisture sensors can continuously monitor the water levels in the soil, providing real-time data to farmers. This data can be used to optimise irrigation schedules, ensuring that crops receive the right amount of water at the right time. By preventing over-irrigation, farmers can conserve water resources and reduce costs.

2. **Water usage monitoring:** In addition to soil moisture monitoring, eUICC technology can be used to track overall water usage on the farm. Connected water meters equipped with eUICC can provide detailed insights into how much water is being used for irrigation, livestock, and other agricultural processes. This information can help farmers identify inefficiencies and implement strategies to reduce water consumption.

3. **Livestock monitoring:** Livestock health and productivity are closely tied to their environment. eUICC-enabled sensors can be attached to animals to monitor their vital signs, movement patterns, and overall well-being. For example, temperature sensors can detect signs of illness early, allowing for prompt intervention. GPS tracking can also be used to monitor the location and movement of livestock, reducing the risk of loss or theft.

4. **Crop monitoring:** eUICC technology can also be applied to monitor crop health and growth. Connected drones equipped with cameras and sensors can capture high-resolution images of fields, which can then be analysed to detect signs of disease, nutrient deficiencies, or pest infestations.

5. **Climate monitoring:** Weather and climate conditions play a significant role in agricultural productivity. eUICC-enabled weather stations can be deployed across farms to monitor temperature, humidity, wind speed, and precipitation. This data can help farmers make informed decisions about planting, harvesting, and protecting crops from adverse weather conditions.

Future readiness with GSMA specifications LPAe .22 and .32

As eUICC technology continues to evolve, it is essential for the agriculture industry to stay ahead of the curve by adopting solutions that are future-ready. The GSMA specifications LPAe .22 and .32 introduce new features and capabilities that will further enhance the benefits of eUICC in agriculture.

LPAe .22: This specification focuses on improving the interoperability of eUICC devices across different networks and service providers. For agriculture, this means that eUICC-enabled devices can seamlessly switch between networks, even in regions with limited connectivity options. This is particularly important for ensuring continuous operation in remote or rural areas.

GSMA Spec .32: The .32 specification introduces enhanced security features, such as improved encryption and authentication protocols. These features are critical for protecting the vast amounts of data generated by connected agricultural devices. With the increasing prevalence of cyber threats, adopting .32-compliant eUICC solutions can help safeguard sensitive information and maintain the integrity of agricultural operations.

The adoption of eUICC technology in agriculture presents a significant opportunity to revolutionise the industry by enabling more efficient, sustainable, and connected farming practices. From monitoring soil moisture and water usage to tracking livestock and crop health, p/eSIM provides the seamless connectivity and remote management capabilities needed to optimise agricultural operations.

As the industry continues to embrace digital transformation, it is crucial to consider future readiness by adopting solutions that comply with the latest GSMA specifications, such as LPAe .22 and .32. By doing so, agricultural businesses can stay ahead of the curve, ensuring that their operations are not only efficient and sustainable but also secure and resilient in the face of evolving challenges.

In the years to come, eUICC technology will undoubtedly play a central role in shaping the future of agriculture, driving innovation and enabling a smarter and more connected world.

The adoption of p/eSIM technology in agriculture presents a significant opportunity to revolutionise the industry by enabling more efficient, sustainable, and connected farming practices

https://simpliot.com

Permanent roaming for IoT: a regulatory issue finally resolved?

One of the major challenges for deploying multi-country cellular-based IoT connectivity has been the restrictions placed by regulators and host operators on the use of permanent roaming. In this article, Matt Hatton, the founding partner of Transforma Insights, explores the current status of permanent roaming, the recent strides made by IoT connectivity providers to deliver compliant services, the impact of the shift from roaming to eSIM localisation, and the continuing challenges in the space

Permanent roaming: the constant challenge

A recent Transforma Insights report 'Regulatory landscape for the Internet of Things'[1] analysed the various regulations that affect deployments of the Internet of Things and the associated provision of connectivity, device functionality, and management of data, as well as regulatory drivers and barriers to IoT adoption, as illustrated in **Figure 1**.

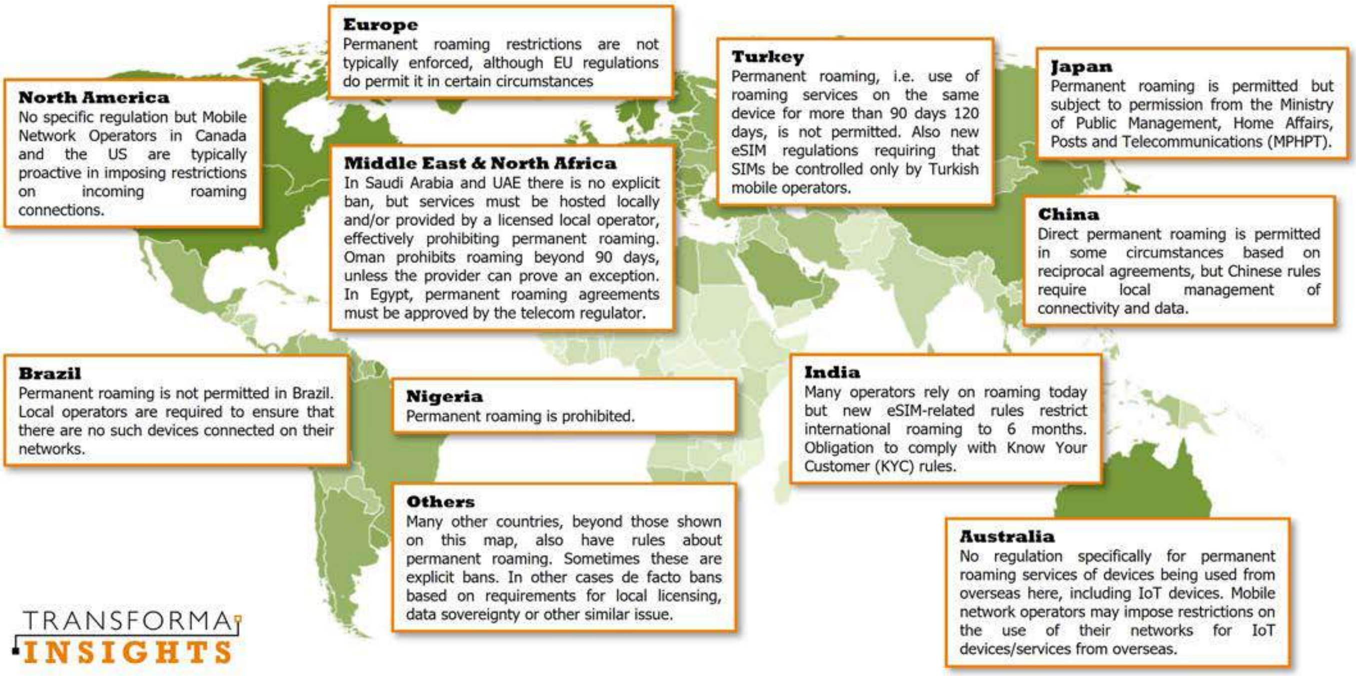
One particularly relevant set of regulations for supporting IoT relates to 'extra-territorial use of E.164 numbers' (which is generally referred to as 'permanent roaming'). Many, perhaps most, IoT deployments using cellular connectivity involve ▶

Figure 1: Seven key regulatory areas for the Internet of Things
[Source: Transforma Insights, 2024]

Hardware and spectrum	There are many long-standing regulations related to factors such as RF regulations, device certification and product safety which are relevant to IoT. Recent years have seen a flurry of regulations related to energy efficiency and sustainable disposal. We also consider import/export controls.
Licensing and permanent roaming	Relates specifically to the provision of public networks (most usually cellular networks) and very specifically the restrictions that might apply to extra-territorial use of E.164 number (otherwise known as 'permanent roaming').
Privacy	Some of the first regulations affecting IoT data were those related to data privacy more broadly, which address the collection, storage, and processing of personal data. This includes the EU GDPR regulation and various consumer privacy regulations around the world.
Security	The last few years have seen a major expansion in the amount of legislation related to cybersecurity in general and IoT device security particularly. There are also numerous examples of codes of practice pertaining to cybersecurity topics such as passwords and firmware updates.
Data sovereignty and access/portability	Many countries have particular rules about the circumstances in which data may or may not be accessed by government, shared within countries and sent overseas. This includes the US CLOUD Act and various EU regulations such as the Data Act and the Data Governance Act.
National resilience	As a further evolution on the requirements for device security and data sovereignty, an increasing number of countries are implementing stricter rules related to national resilience and protection of critical national infrastructure (CNI), including rules around procurement.
Regulations in vertical sectors	As well as the general regulations related to IoT and associated fields outlined under the headings above, there are also numerous vertical-specific regulation which can also be relevant for IoT, including in automotive, energy, financial services and the public sector.

[1] https://transformainsights.com/research/reports/regulatory-landscape-iot

Figure 2: Permanent roaming rules around the world
[Source: Transforma Insights, 2024]



connecting devices in multiple countries. Many have specific rules about how that connectivity is supported, in particular whether cellular-connected devices could exist in a state of permanent roaming, i.e. whether a device that is connected by a connectivity provider that is not licensed in the territory could use its roaming agreements with local licensed operators to support a connection that was not simply temporarily roaming but would be present on a permanent basis in that country.

During the 2010s, many regulators, for instance in Brazil, China, India and Turkey, introduced, or more rigorously enforced, rules that prohibited permanent roaming. Sometimes the rules were explicitly against permanent roaming and in other cases were based on local registration requirements or tax obligations. The regulators are often motivated to protect the local market and enforce local rules with which a roaming connection may not comply, such as lawful intercept. Besides this, roaming was never envisaged to include a foreign device permanently being in a state of roaming.

Measures to restrict permanent roaming can come in various guides, for instance related to licensing, taxation, rules on management of eSIM localisation, or know your customer (KYC) rules, all of which can act to effectively prohibit the practice. In many cases, the issue relates to licensing, i.e. the company providing the services needs to be a locally licensed legal entity in the country.

Limitations on permanent roaming are not solely the preserve of regulators. There were also commercial equivalents, particularly in the US and Canada, where the operators themselves in some cases prohibited their roaming partners from having devices permanently roaming on their networks.

Figure 2 presents a summary of some of the rules. We should add the caveat that the rules do change often and there are often exceptions whereby permanent roaming is permitted despite seemingly explicit restrictions to the contrary.

Problem solved?

The limitations on permanent roaming have caused some headaches. Historically, roaming was the main – and certainly the simplest – mechanism used by MNOs and MVNOs to support connections across multiple territories. However, over the last decade IoT connectivity providers have made great strides in addressing the challenge.

In July 2024, Transforma Insights published its annual 'Communications Service Provider (CSP) IoT Peer Benchmarking report'[2] which analyses the capabilities and strategies of 25 of the world's leading IoT connectivity providers. As part of that research, we assess the ability of the companies to provide compliant connectivity around the world. Specifically this year, we asked each of the CSPs about their ▶

[2] https://transformainsights.com/research/reports/csp-iot-peer-benchmarking-2024

The compliance situation in India is in flux with ongoing changes to requirements related to eSIM localisation; as a result it's very hard to identify which CSP offerings are currently compliant or will be in the near future

Figure 3: Approaches of communications service providers to IoT connectivity in selected geographies
[Source: Transforma Insights, 2024]

	Brazil	China	EU	India	Turkey	US
1NCE	●	◕	●	○	○	●
AT&T	●	◕	●	◑	◑	●
BICS	◕	◕	●	◑	◔	●
DT IoT	◕	●	●	◑	◕	●
Emnify	●	◑	●	◑	○	●
Eseye	●	◕	●	◕	◑	●
floLIVE	●	●	●	◕	●	●
KORE	◕	◑	●	◑	○	●
KPN	◕	◑	●	◑	○	●
NTT	●	◑	●	◕	◕	◕
Pelion	◑	◕	●	◑	◑	◕
Semtech	◕	◕	●	◑	◕	●
Singtel	◑	◕	◕	◑	○	◕
Soracom	●	◑	●	◑	○	◕
T-Mobile US	◕	◔	●	◑	◕	●
Tele2	◑	◕	●	◑	◕	●
Telefónica	●	◑	●	◕	◑	●
Telenor	●	◑	●	◑	◑	●
Telia	◕	◕	●	◔	○	◑
Telit Cinterion	◕	◕	●	◕	◑	●
Velos IoT	◕	◕	●	◑	○	●
Verizon	◕	◔	●	◑	○	●
Vodafone	◕	◕	●	◕	●	◕
Wireless Logic	●	●	●	◑	◕	●

● Full support, multiple networks ◕ Compliant capability ◑ Compliant offering coming soon or otherwise limited
◔ Supported but long-term compliance in doubt ○ Not supported

TRANSFORMA INSIGHTS

approach to addressing connectivity in each of six countries/regions (Brazil, China, EU, India, Turkey, US) for permanently located devices. In **Figure 3**, we provide a summary of the approach of the 25 CSPs profiled.

The general trend is that CSPs have largely resolved the challenges in the most relevant countries. Compliant connectivity in the EU and US is more or less universal. Brazil, which has historically been the market most commonly quoted as being a challenging market, is now very well addressed by almost all CSPs. China continues to represent a few challenges, but where CSPs wish to address it there are commercial mechanisms for working with Chinese MNOs to support compliant connectivity. ▶

But it's not all plain sailing. The compliance situation in India is in flux with ongoing changes to requirements related to eSIM localisation; as a result it's very hard to identify which CSP offerings are currently compliant or will be in the near future. The current strict rules about localisation within Turkey are also causing significant friction, with many providers unable to support connectivity in that country other than through the use of local SIMs. There are suggestions that the regulatory environment there might need to adapt to be rather less onerous on non-Turkish operators.

It is important to note that in almost all cases, the CSPs concerned would be in a position to negotiate and implement fully compliant solutions for specific clients regardless of current capability. The aim of **Figure 3** is to illustrate the current state of the off-the-shelf offerings of the various players.

eSIM: a universal panacea?

Perhaps the most significant mechanism used for supporting compliance with permanent roaming rules is through the increasing use of some form of SIM localisation, so moving away from relying on roaming using a foreign international mobile subscriber identity (IMSI) to the use of a local IMSI (as part of a multi-IMSI offering) or switching of the eSIM profile to that of a local operator. In the last few years, the technology landscape related to eSIM has changed dramatically and we anticipate an ongoing impact on how global connectivity is delivered. To date there have been three main standards unveiled for remote SIM provisioning (RSP). Each of the three standards established slightly different mechanisms for the user or owner of a device to change the SIM profile while the device is deployed in the field.

Transforma Insights has explored in detail the capabilities and implications of the three standards in great detail, including in the June 2024 Position Paper 'Key considerations for Enterprises looking to adopt SGP.32'. In summary, the SGP.02 (or M2M) standard was introduced in 2014. This was a 'push' model, whereby the donor and recipient network providers would act together to replace the SIM credentials on the device. The challenge with SGP.02 is that it requires cooperation between the subscription management infrastructure of the donor and the recipient networks to perform the hand-over. This was followed in 2016 by the SGP.22 (Consumer) standard where the end user can, via direct intervention using the device user interface (UI), 'pull' a new profile from a chosen provider down to the device. The limitation here was the need for an advanced UI as well as user intervention, neither of which are typically available on any IoT device. The SGP.32 (IoT) third variant, unveiled in 2023, was aimed at resolving some of the limitations of the earlier versions. It effectively amended the SGP.22 technology to allow for remote management. Compliant devices can be expected in 2025. In addition, several connectivity providers have developed variants on SGP.22 that place an agent on the device, removing the requirement for user intervention; these approaches effectively work in the same way as SGP.32, although with some element of proprietary technology.

While the new remote SIM provisioning technology might be well-defined, what is not yet entirely clear is what commercial models will prevail to make use of the new technology. What is completely clear, based on the research that Transforma Insights has done for the aforementioned CSP IoT Peer Benchmarking, is that the view from the CSPs is that they are willing, and in many cases keen, to work with the technology.

The big change, in the context of addressing permanent roaming, is that SGP.32 (and to a lesser extent variants on SGP.22) allow for much easier recredentialling of SIMs to a local profile. Local, compliant profiles are relatively easily swapped in. However, we should add a caveat or two here. Most pertinently there is still a requirement to establish a commercial relationship with the network onto which the connection will be transferred. Some enterprise customers may well have these in some circumstances, which accounts for the increasing relevance of bring-your-own-connectivity (BYOC) offerings. However, in most cases enterprises will still have requirements for someone to negotiate commercial relationships with appropriate network operators for connectivity and ideally act as a single point of contact. And, furthermore, simply switching between networks is not the only consideration, there is a further requirement to orchestrate data flows and back-end processes to ensure a seamless transition between carriers. Simply put, the provision of compliant cellular-based IoT connectivity will need to be delivered as a managed service, albeit one where much of the friction of localisation and compliance is removed.

While the new remote SIM provisioning technology might be well-defined, what is not yet entirely clear is what commercial models will prevail to make use of the new technology

[3] https://transformainsights.com/research/reports/key-considerations-enterprises-adopt-sgp32

Plenty of action in the IoT data management and protection market

SIMPL, among other solutions, supports the rapid creation of cloud-connected IoT devices from the ground up, while fully securing them to send and receive data in the cloud. Antony Savvas looks at the state of the IoT data security and management market

According to analyst firm **MarketsandMarkets**, the global IoT security market is projected to grow from US$24.2 billion in 2024 to US$56.2 billion by 2029, at a compound annual growth rate (CAGR) of 18.4% during the forecast period.

This market includes identity and access management (IAM), data encryption and tokenisation, device authentication services, secure communication protocols, private key infrastructure (PKI) certificate lifecycle management, security analytics and virtual firewalls.

And according to **Mordor Intelligence**, the IoT data management market is expected to grow at a CAGR of 16.6% between now and 2026. This growth covers solutions including data integration, security, analytics and storage solutions.
Market drivers

When it comes to security spending, the growth is down to organisations facing significant financial losses and reputational damage because of increasing cyber attacks on IoT devices. The particular risk in the IoT sector is that every device and every system usually have their own specific firmware, which is software that controls the device or facility itself.

And since hardly any guidelines or binding specifications have existed in this area for device manufacturers to boost security, hackers and criminals have been attacking the unprotected. ▶

This may change with the European Commission's Cyber Resilience Act (CRA), for instance, which is intended to address data security problems surrounding devices and systems with network connections, from printers and routers to smart household appliances and industrial control systems.

To press manufacturers, distributors and importers into more protective action, with the Cyber Resilience Act, they face significant penalties if security vulnerabilities in devices are discovered and not properly reported and mitigated.

"The pressure on the industry is growing immensely," says Jan Wendenburg, CEO of cyber security firm **ONEKEY**. "The financial fines for affected manufacturers and distributors are severe: up to €15 million or 2.5% of global annual revenues."

Under the Act, suppliers active in the European Union market, must now prepare to complete a Cyber Resilience Readiness Assessment, if they want to avoid facing large fines. That said, the market sales for IoT security show organisations are already increasingly adopting security solutions to help protect against threats like device hijacking, data theft, supply chain intrusions, and widening ransomware attacks.

Key players

Key players in the IoT security market, says MarketsandMarkets, include **Microsoft**, **Fortinet**, **Amazon Web Services**, **IBM**, **Intel**, **Cisco**, **Thales Group**, **Infineon**, **Atos**, **Palo Alto Networks**, **Mobileum**, **Entrust**, **NXP Semiconductors**, **MagicCube**, **Claroty**, **Ordr**, **Armis**, **Nozomi Networks**, **Keyfactor**, **Particle Industries** and **Forescout**, among others.

Microsoft, for instance, offers capabilities for its Defender security protection that promise to bring the same level of vulnerability management, threat detection and response for enterprise IoT devices, previously only available for managed endpoint devices.

The Defender for IoT offering provides extended detection and response (XDR) coverage to IoT devices like digital signage, conference room systems and operational technology (OT) devices, which have all been prone to software vulnerabilities and attacks from cyber criminals.

With Defender for IoT, agentless monitoring secures 'things' connected to IT networks, voice over IP systems, printers and smart TVs, for instance. And it allows firms to gain the essential visibility into devices without additional configuration, through a deployable network sensor that can collect all network data needed for discovery, behavioural analytics and machine learning. Microsoft adds that artificial intelligence (AI) is being used to augment IoT threat intelligence generally.

Government agencies, such as US National Institute of Standards and Technology (NIST), are also investigating IoT security technology on a number of fronts, including protocols, security assurances, use cases, applications and current services, to help drive further data security development to better protect companies and end users.

Zero trust

An emerging concept to help improve data protection is zero trust, which eliminates implicit trust from IT systems, and assumes that every user and every thing on the network is a threat to data security. It treats all data traffic as untrusted, requiring strict identity verification for every user, device and process before granting any permissions.

Such an approach acknowledges that the biggest threats to security can come from lateral movement within a network, so if something untoward is detected on it, then it has to be stopped and quarantined there and then. Companies accepting this principle are now adopting zero trust network access (ZTNA) systems.

Network segmentation

As a first step to adopting ZTNA, organisations should move towards network segmentation. This is the practice of dividing networks into different logical segments, such as IoT connected portions, and having complete control of the traffic going through and between those segments. It is designed to reduce the attack surface, preventing threats from spreading laterally throughout an organisation.

To do this, businesses need a full view of all networks within the organisation. You must have visibility into the network, application, workload and process levels, as well as a view into multi-clouds or on-premise data centres where data assets are distributed across all geographies.

However, while technology methods like ZTNA are expected to become essential, it isn't just technology that is needed to protect apps and data, it is also policy. IT governance, audit and compliance policies as part of a framework must be adopted by organisations with the full backing of their boards.

By combining ZTNA, for instance, and working to a framework, companies can potentially see costs related to any data breach coming down. Spiralling cyber insurance costs are a problem across industries, as a result of wider and more serious cyber security threats. Organisations working to a framework may well see their cyber insurance costs better controlled, as they can demonstrate to insurers that they are more prepared to deal with a breach, and therefore have a better chance of curtailing it, and reducing its damage.

While the IoT data management and protection market may well be growing, now is the time for the whole ecosystem to step up to the plate to help keep out the rogues.

Government agencies, such as US National Institute of Standards and Technology (NIST), are also investigating IoT security technology on a number of fronts

IoT roaming set to drive revenue growth for mobile operators

With IoT connections now composed of various different technologies from non-terrestrial networks to low power wide area networks, cellular connectivity offers a sweetspot for devices that move between different countries or that are designed as part of global deployments. For communications service providers (CSPs), supporting IoT roaming can be an appealing generator of revenue but assuring connectivity is available in multiple countries is complex and involves navigating a complex web of commercial and regulatory conditions

The priorities of many mobile operators and their IoT businesses are becoming increasingly misaligned as the telecoms industry focuses on consolidation of operations to their main markets but IoT demands global connectivity

The growth of IoT is resulting in increased connectivity revenue. IoT market research firm **Berg Insight** has reported that global IoT connectivity revenues increased 16% to reach US$13.82 billion in 2023. As IoT has matured, the firm says there is greater focus on reliability, security and support for international deployments, contributing to new types of market dynamics for cellular IoT connectivity providers. By 2028, the firm projects that there will be six billion IoT devices connected to cellular networks worldwide, generating annual connectivity revenues of US$23.41bn.

The top ten mobile operators reported a combined active base of 2.9 billion cellular IoT connections at the end of 2023, accounting for 88% of the total 3.3 billion connections. **China Mobile** is the world's largest provider of cellular IoT connectivity services with 1.32 billion cellular IoT connections. **China Telecom** and **China Unicom** ranked second and third with 527 million and 494 million connections respectively. **Vodafone** ranked first among the Western operators and fourth overall with 184 million connections, followed by **AT&T** with 128 million in fifth place. **Deutsche Telekom** and **Verizon** had in the range of 50–57 million cellular IoT connections each. **Telefónica**, **KDDI** and **Orange** were the last players in the top ten with about 41 million, 40 million and 37 million connections respectively. The growth in the installed bases of the largest mobile operators varied, reports Berg Insight, with changes ranging from a 1% decrease to a 31% increase year-on-year.

International connectivity constitutes one of the largest and fastest growing segments of the cellular IoT market. Mobile operators with regional and multi-regional operations are naturally well-positioned to offer IoT connectivity services for international deployments at competitive rates, utilising their network footprints and ability to negotiate favourable roaming agreements.

The priorities of many mobile operators and their IoT businesses are becoming increasingly misaligned as the telecoms industry focuses on consolidation of operations to their main markets but IoT demands global connectivity. This has led to a greater separation between mobile operators' IoT businesses and network operations, resulting in more open approaches to global network access in line with the strategies of IoT managed service providers, says Berg Insight.

Established IoT managed service providers however typically have more advanced localisation capabilities through international mobile subscriber identity (IMSI) and embedded SIM (eSIM) profile donor agreements. Berg Insight believes that the separation of IoT connectivity businesses and networks will continue, driven by changing industry dynamics and a shift to new eSIM technologies. This implies a strong case for global consolidation of cellular IoT connectivity platforms.

There is significant growth in the number of connections and **Juniper Research** has uncovered that the number of roaming IoT connections will ▶

Figure 1: Roaming IoT Connections to Grow 300% by 2028 - At what cost to subscribers?
Average cost per MB of data generated by roaming IoT connections in 2028 ($)

grow 300% over the next five years; from 145 million in 2023, to more than 600 million by 2028. **Figure 1** details the average cost per megabit of data generated by roaming IoT connections in 2028.

A study by the firm has found the global number of 5G IoT roaming connections will rise from 15 million in 2023 to 142 million by 2027, representing over 27% of all 5G roaming connections in four years. It predicted that this growth will be driven by the acceleration of 5G standalone (SA) deployments, with intensifying roll outs in home markets providing increased momentum and a strong value proposition for 5G SA-specific roaming agreements.

The research forecast that 21% of global 5G IoT roaming connections in 2027 will be found in West Europe, despite that region only accounting for 5% of the global important for to incentivising IoT users to implement a roaming business model, thus driving growth of IoT roaming connections.

Report author Elisha Sudlow-Poole commented: "To further capitalise on the growth of 5G IoT roaming in West Europe, operators must form roaming agreements that utilise standalone 5G networks to improve network performance for roaming connections, and provide the same level of service when roaming as they do on home networks."

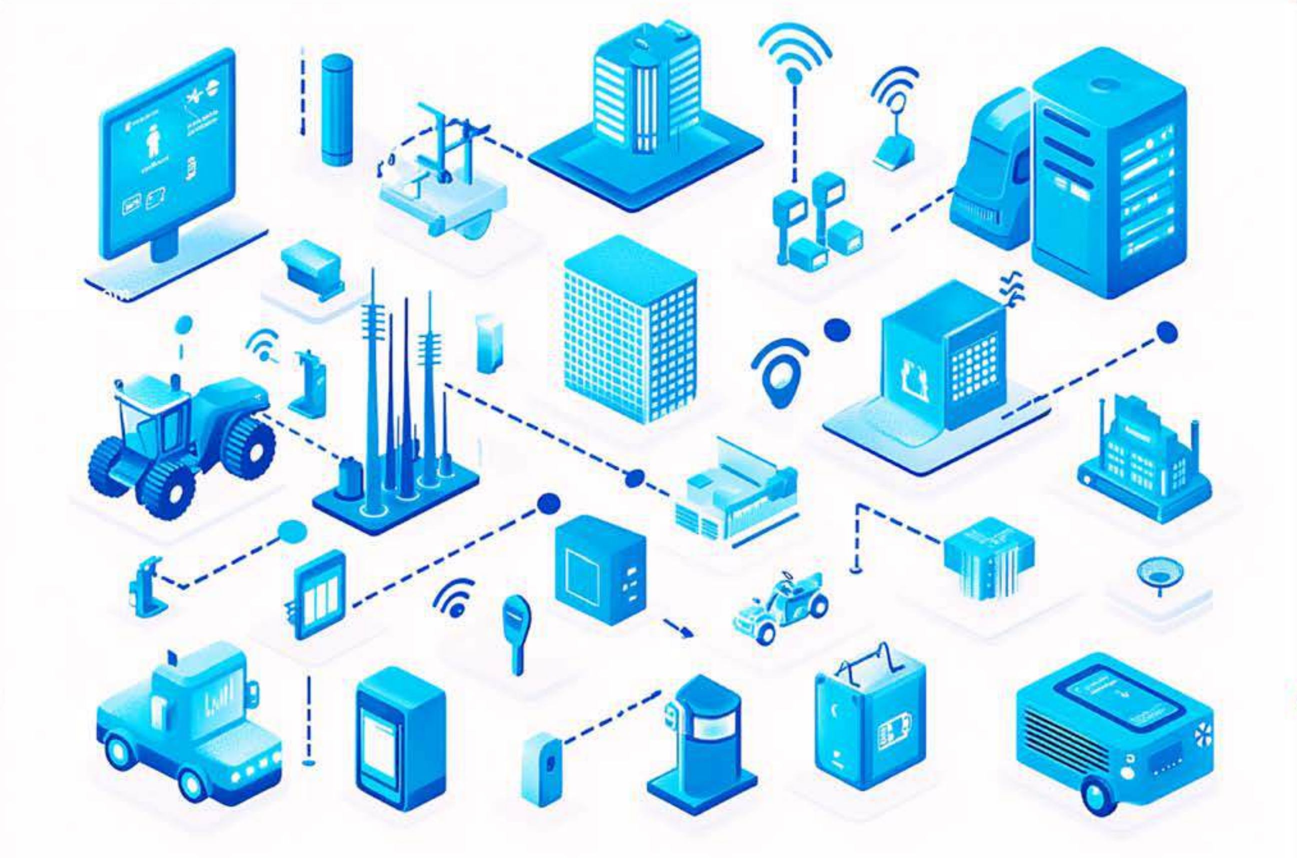
Operators look to add value

In addition to 5G standalone-specific roaming agreements, the report urged operators to implement roaming analytics tools that use AI to maximise roaming revenue, as they enable operators to efficiently assess the significant amount of roaming data generated by 5G roaming connections in real-time. The report anticipates key verticals, such as autonomous vehicles, will necessitate advanced roaming solutions, owing to their data-centric nature. The research emphasised that roaming analytics must be integrated directly into platforms to maximise their value proposition to network operators, and enable swifter reconciliation of clearing for stakeholders.

IoT roaming will remain a key driver of revenue with **Kaleido Intelligence** finding in a recent operator survey that 64% of respondents see IoT roaming use cases as the main driver of roaming revenues over the next three years. Research from the firms has forecast that combined wholesale and retail roaming revenues generated by consumer and IoT mobile connections will reach US$45 billion in 2024. That represents a 47% increase compared to pre-pandemic levels.

The firm says the increase will be driven by rising data roaming activity, primarily fuelled by consumers transitioning to 5G roaming services. This anticipated expansion in both consumer and IoT roaming data usage is expected to soar by 36% annually, reaching close to 5,000 petabytes in 2024.

IoT roaming will remain a key driver of revenue with Kaleido Intelligence finding in a recent operator survey that 64% of respondents see IoT roaming use cases as the main driver of roaming revenues over the next three years



Hyperscale IoT demands an open, horizontal management toolset

With IoT now being deployed at scale, the management burden has increased significantly, with a magnifying effect on errors that occur across large IoT device estates. Efficient management of IoT deployments in the hyperscale era requires a toolset capable of supporting a variety of devices and connectivity standards. Nick Gyles, the chief product officer at Daizy, tells George Malim, the managing editor of IoT Now, that standardised, intuitive-to-use IoT management tools are essential for IoT success

George Malim: Why is it important to ensure broad interoperability across the IoT architecture?

Nick Gyles: There are two aspects to this, one involves equipment and devices and the other addresses the connectivity mechanism. For devices, we're seeing commoditisation and maturing of hardware. Five years ago, IoT devices were typically proprietary, but now large manufacturers are creating highly sophisticated sensors at scale. While this commoditisation has lowered the cost of delivering IoT solutions, device manufacturers are interpreting IoT standards in different ways, right down to the way payloads are constructed. Although solution providers are keen to take advantage of the latest technology, they are often hamstrung by a legacy approach of 'hardwiring' their applications to a specific brand of device, and adding new device types can mean rewriting whole swathes of underlying code.

From a connectivity perspective, we're seeing increasing demand for solutions that support multiple connectivity standards. LoRaWAN, for example, is great for large buildings or scenarios with high levels of sensor density, while NB-IoT and LTE-M offer flexibility for dispersed sensor deployments or for mobility use cases. Increasingly we're seeing deployments that require both LoRaWAN and NB-IoT. Monitoring for damp and mould in social housing is a great example of a ▶

We place a lot of emphasis on contextualisation. You need to be confident that the device is where you think it is and the data provided is valid.

Nick Gyles
Daizy

need to deliver a low-cost multi-connectivity solution across a diverse range of premises - from blocks of flats through to separate houses in more rural environments.

With multiple device types and connectivity technologies in use, solution providers are likely to end up with multiple management solutions to capture data. This is why interoperability is important and an open toolset like Daizy provides a much better alternative than segmented vertical stacks. Regardless of which device or network technology is used, data delivered through Daizy is standardised and ready to be consumed.

GM: Why is standardised service delivery critical for delivering IoT at scale?

NG: By adopting a more horizontal approach, Daizy standardises sensing metrics such as temperature, electricity metering, positional information, air quality and many others. We have a standardised schema of how that data gets presented - we decode the manufacturer-specific data payloads and ensure the data is easily consumable via standard technologies that developers understand.

www.daizy.io

We've engaged with many organisations who have approached IoT with a single use-case in mind. However, end-customers will ultimately be looking at multiple use-cases across their estate, and the last thing they need is multiple platforms for data, devices and connectivity. With a standardised approach to deploying and managing IoT projects, issues such as in-life maintenance requirements, monitoring and the ability to add other capabilities across the IoT service stack can be streamlined and aligned with existing technology asset management.

IT departments are really good at managing servers and desktops but they don't have the resources or tools to manage a broad range of low-cost IoT devices at massive volume. The advantage of a toolset like Daizy is that you can monitor energy usage, water levels, humidity or any other metric in the same centralised operating environment.

GM: In what ways will being prepared for AI and digital twins help to drive growth?

NG: We place a lot of emphasis on contextualisation. You need to be confident that the device is where you think it is and the data provided is valid. Within Daizy there are checks on location, checks that installation has been performed correctly and checks on the device identity and various attributes. In smart bin deployments, for example, the depth of the bin is vital information because the system can't know the fill level without knowing the bin's dimensions and the position of the sensor at the point of installation.

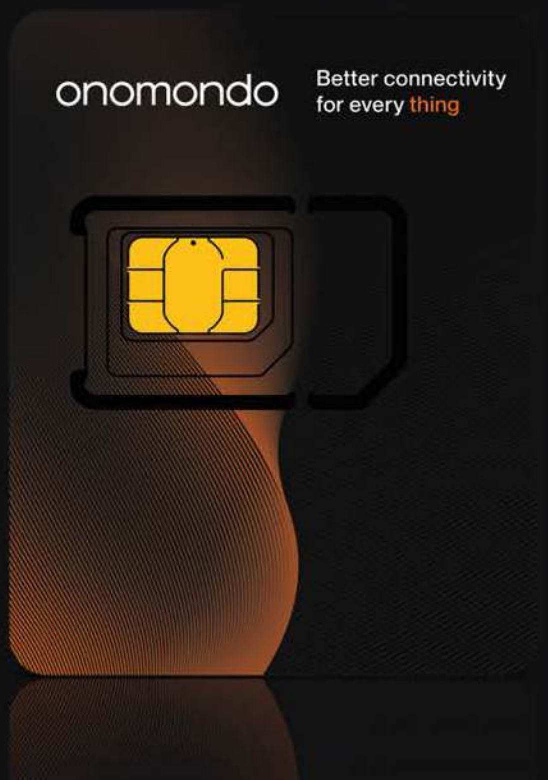
Rich context and the interoperable data pipeline we support create normalised data structures that make it straightforward to enable a digital twin. High quality structured data ensures a really high-fidelity sensor model which is resilient to project changes such as faulty device swap-outs.

Our goal is to do all the non-differentiated activity so our partners have access to a foundational data environment that eliminates the huge inefficiencies in today's IoT operations. Every piece of equipment in Daizy has an auditable asset history from original installation through to end-of-life. That completeness is essential to effective IoT project management and handling the immense scale of deployments.

Connectivity is often overlooked when designing an IoT device - something expected to 'just work'. But your choice of connectivity profoundly affects everything from device troubleshooting and power efficiency to security, future-proofing, and total cost of ownership

Connectivity Web Summit promises insights on LTE, eSIM IoT, cellular trends and cross-border connectivity

The Connectivity Web Summit is a free online event designed to help IoT businesses future-proof their connectivity strategies. Connectivity affects every aspect of your IoT device - from power consumption to customer satisfaction - so this summit is your chance to gain insights from industry leaders with deep experience in building and delivering IoT solutions. You can join one or multiple sessions based on your interests from 2pm CET/ 8am EDT on 15 October 2024



Whether you're tackling the complexities of multi-country connectivity, diving into the latest developments with SGP.32, or looking to optimise your remote device management strategies, this summit offers practical, actionable insights. Stay ahead with expert discussions on emerging technologies like LTE Cat 1 Bis, LPWAN, SoftSIM and the future of SGP.32. These sessions are designed to give you the tools and knowledge to enhance your IoT strategy immediately.

Hosted by **Onomondo**, a global MVNO, and **Valid**, a SIM manufacturer, this summit features guest speakers from **Nordic Semiconductor**, **Maersk**, **Treon**, **Murata**, **Ignion** and **Agurotech**. Network with hundreds of IoT professionals from around the world, all from the convenience of your home office or workspace.

Connectivity is often overlooked when designing an IoT device - something expected to 'just work'. But your choice of connectivity profoundly affects everything from device troubleshooting and power efficiency to security, future-proofing, and total cost of ownership. This summit brings together experts from across the IoT ecosystem to share key insights on creating a robust, future-ready connectivity strategy.

- **Emerging Market Trends in Cellular Technology** – featuring Martin Lesund (Nordic Semiconductor). Join us for an insightful session with Nordic Semiconductor, where you'll gain valuable knowledge on the latest trends in cellular technology and their impact on the IoT industry.

- **Connectivity Across Borders** – featuring Jacob Jagger (Onomondo), Bruno Cunha (Ignion), and Find Bengtsson (Maersk). This session will cover the challenges and solutions associated with international roaming, SIM steering, and best practices for deploying IoT solutions across multiple countries.

- **Building a Robust Cellular Tech Stack: A Case Story** – featuring Mattia Fiumara (Agurotech). This session will cover the setup of a cellular tech stack and how features like IoT connectors, traffic monitoring, web-hooks and VPNs play into launching a product.

- **LTE-M vs LTE Cat 1 Bis** – featuring Alejandro Pulido (Valid), Antti Kangaskoski (Treon), and Farhad H. P. Shirvan (Onomondo). This discussion will explore different LTE standards, such as LTE CAT1, LTE CAT 1bis, and LTE-M, examining their advantages, limitations, and use cases.

- **The Future of eSIM IoT and SGP.32** – featuring Alejandro Pulido (Valid), Shohei Kawanaka (Murata), and Wanig Le Pennec (Onomondo). This panel discussion will cover the new SGP.32 standard and its implications for device management, security, and deployment, focusing on the evolving landscape of eSIM technology in IoT.

Ready to secure your IoT future? Join us at the Connectivity Web Summit on 15 October 2024 for expert guidance and practical insights that will set your business up for success in the evolving IoT landscape. ■

Register today at **https://onomondo.com/video/cellular-connectivity-web-summit-2024/**

IoT Now: ISSN 2397-2793
2024 • VOLUME 14 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

Trasna's Stéphane Fund targets eSIM success with Workz acquisition

The IoT Now Guide to Cloud-Based eSIM 2024

PLUS: How iONLINE is improving business connectivity and sustainability with eSIM • Inside 1oT's launch of eSIM Core • Is the jury still out on eSIM uptake? • How Monogoto is driving business flexibility with cloud eSIM • Trasna details African water management project • Virgin Mobile MEA turns to EcosSIM • See the latest News, Features and Interviews at **www.iot-now.com**

It's full steam ahead for Trasna and Workz in the evolving IoT market

To fully support the rapid evolution of IoT technologies, suppliers usually have to offer a varied portfolio and have an expansive view of the market. Antony Savvas speaks to Trasna CEO Stéphane Fund, whose company has also been acquisitive to fully address the demands of the IoT market

"Trasna" is Irish and means "to go across". It reflects our mission

In 2018, Fund, a seasoned tech entrepreneur who had sold his previous software business to UK chip giant **ARM**, envisioned a future brimming with trillions of connected devices. The IoT market, poised for explosive and unprecedented growth, presented a golden opportunity. Seeing the challenges of device makers and network operators with heavy expenses, slow implementations, and a fragmented vendor landscape, here was a chance to build the foundation for an alternative future for the Internet of Things.

So, that same year, Fund established **Trasna**. With a vision to harness the power of semiconductor and mobile technologies, Trasna then strategically acquired **Elatec** (Germany) and **SAFE-IoT** (France), gaining crucial expertise in hardware and software, and uniting some very bright minds.

Five years on, in 2023, the company achieved a milestone producing its first SIM chip. The same year, it developed its own RISC-V core processor, a testament to its commitment to in-house innovation. By then, it had also designed and deployed more than 40 secure microcontrollers across smart cards, point-of-sale terminals, secure readers, smart meters and security devices.

Then came the acquisition of cloud eSIM specialist, **Workz**, in February 2024. This marked a giant step towards Trasna's vision of vertical integration. From chip design to product lifecycle management, the company was taking control of its destiny to guarantee customers complete efficiency, quality and security.

With headquarters in Cork, Ireland, and innovation hubs in France, Dubai and Tunisia, plus GSMA-certified production facilities in Dubai, the company has now built a platform to serve the global market. With a range of innovative products, from its core processors and microcontrollers, to its multi-eSIM orchestration hub and IoT eSIM remote manager, its portfolio addresses the market's evolving needs.

This trend is expected to continue, with the company currently developing its own System-on-Chip (SoC), that incorporates an integrated SIM (iSIM). This innovation has the potential to significantly disrupt the IoT market.

Employing over 400 dedicated specialists, supporting the development of semiconductors, SIMs, eSIMs, a SoC platform and iSIM technologies, the firm clearly provides a complete end-to-end solution to support the rapid changes and needs in IoT communications.

IoT Now: So Stéphane, Trasna has wide-scale industry and geographical involvement, why was

SPONSORED INTERVIEW

Trasna's headquarters located in Cork, Ireland?

Stéphane Fund: "Trasna" is Irish and means "to go across". It reflects our mission: to seamlessly connect people and devices with transformative experiences for mass IoT. So I guess it is only fitting we have our headquarters in Ireland. It also has a strong tech ecosystem, established infrastructure, supportive business policies and a talent pool that makes it an ideal location. Nevertheless, as you point out, we are a global company now with a semiconductor R&D centre in France, an IoT development centre in Dubai, and a second one to be opened in India in October.

IoT Now: Last year, Trasna launched its Secure SIM Chip family for the telecoms market. In a market that has seen many chip capacities impacted by production shortages, how did the firm mitigate this issue? On the other hand, was the demand there from potential customers, as some would point to relatively weak demand for new 5G/IoT connections globally?

SF: Generally speaking, the higher the chip grade, the higher the impact on production. Chips in SIM cards are less complex than those in high-end electronics, which have faced more of the ripple effects of the broader shortage.

Trasna has not seen much disruption as it strategically manages chip production challenges by securing multi-sourcing agreements with foundries and prioritising supply chain resilience. With our strong partnerships, we have maintained a steady flow of products, and demand for our SIM chips remains strong, driven by our clients' ongoing investments in 5G and IoT.

IoT Now: At the same time, working with Secure-IC, Trasna developed PUF IP that can generate one or several unique IDs or keys without the need for any cryptographic enrolment phase, while being integrated into a Trasna all-in-one NB-IoT SoC. How significant has this been to the business so far?

SF: The development of physically uncloneable function (PUF) IP in conjunction with Secure-IC has been crucial for Trasna. Integrating this technology into NB-IoT System-on-Chips provides enhanced security without the need for cryptographic enrolment, which is a differentiator for us in the IoT market. It is an example of the technology-focused approach at Trasna, and we are receiving a lot of interest in the product. ▶

Stéphane Fund
Trasna

IoT Now: Now the recent acquisition of Workz, why did you want this company, is it a case of creating a one-stop-shop, from design and security to chip service deployment and management, for instance?

SF: The acquisition of Workz was a strategic move to support our goal to become the market leader within five years. It creates a secure, comprehensive, end-to-end IoT solution from chip design to deployment.

By integrating Workz's expertise in subscription management, we create a full end-to-end supply chain for telcos, device manufacturers and IoT providers, enhancing our capability to deliver seamless and scalable IoT connectivity solutions. This aligns with Trasna's vision of providing holistic, innovative services that meet the evolving needs of the IoT ecosystem.

Workz and Trasna are a perfect fit, with no overlap and complementary offerings, meaning the overall value of our IoT offering to customers is significantly strengthened.

IoT Now: Will the more customer-facing Workz give Trasna a higher profile in the industry perhaps? If that's the case, how will you measure that – marketing and web presence, industry shows profile, social media and shared industry intelligence or collateral?

SF: Yes, I would imagine so, particularly at the beginning. Workz has a very strong reputation in the market, having over 25 years in operation and almost 200 clients in the telecoms sector. Our ambition is to be the market leader in the mobile or cellular IoT market within five years, so our offering needs to be highly compelling. The growth of our customer base will be one of the biggest testaments to this.

Currently, Trasna operates with a flexible go-to-market model that uses partnerships with telcos, IoT providers, system integrators and other service providers

IoT Now: On the business operations side, how will Workz help Trasna grow in terms of things like sales, compound annual growth rates, increased profits, increased profit margins, growing headcounts, wider office footprints for engineering, sales and marketing?

SF: The synergy between the two companies is expected to drive growth through increased capabilities, greater economies of scale, and enhanced revenues. Workz's integration will allow Trasna to expand sales channels, allow access to a broader customer base and improve market penetration. Additionally, it will support Trasna's plans to scale its workforce, extend its geographical footprint and strengthen its engineering and support capabilities.

IoT Now: And on the go-to-market, what is the model at the moment, and how do you see this developing in terms of partner numbers, whether they are global system integrators, managed service providers, telcos, mobile virtual network operators or other service providers?

SF: Currently, Trasna operates with a flexible go-to-market model that creates partnerships with telcos, IoT providers, system integrators, and other service providers. Trasna aims to expand its partner ecosystem and market demand from the OEMs and device manufacturer segment is expected to grow substantially. We aim to deepen collaborations, enhance service delivery and extend reach into new markets, positioning Trasna as the number one choice in the mobile IoT landscape.

IoT Now: Looking at the eSIM market overall, not only is it a crowded market, it is also one that probably hasn't grown as fast as was expected. Why is there limited consumer/ business end customer demand despite Apple backing it and the general hype?

SF: They say that for any new technology, two things are generally true: One, its speed of adoption is overestimated, and two, its impact is underestimated. eSIM appears no different in that respect.

Yes, the expected growth in the eSIM market has taken longer than originally expected. In the case of the consumer market, this can be attributed to a combination of factors such as low user awareness, low penetration in the lower-priced device segments, and some carriers being slow to make the investment.

In the enterprise IoT market, however, things are different. The current GSMA M2M standard has not worked and has had a very low uptake, with relatively few implementations. But the new eSIM standard for IoT devices, SGP.32, will ▶

dramatically change connectivity in the IoT space, and it is a hugely exciting and dynamic opportunity, on which we are ready to help our customers capitalise.

IoT Now: Is this now eSIM's time? If so, what are your predictions for industry growth, and what specific market targets do you have for Trasna/Workz over the short to medium-term?

SF: One of Trasna's principles is that we are a technology-agnostic provider, meaning we do not have a vested interest in any specific technology or format. We find the best way to address our customers' needs and achieve their mobile connectivity goals, whether it be a traditional SIM card, an embedded chip, an integrated SIM or a System-on-Chip solution. Without a doubt, there is a shift towards digital formats, such as eSIMs. When considering the developments in the eSIM IoT model it is understandable why many market analysts are forecasting significant growth. Trasna aims to be at the forefront of this and capture a substantial market share. Short to medium-term goals include expanding market penetration, launching new products, and increasing customer acquisitions in the Americas and APAC regions, specifically in India.

IoT Now: And how about the product roadmap over the next two to three years, what is planned and where do you think you are going as a company, when it comes to targeting new product markets and new geographical markets?

SF: Last year, the company achieved a milestone with its first SIM chip produced. The same year, it developed its own RISC-V core processor, a testament to its commitment to in-house innovation.

Trasna plans to continue to build on this success and expand its product portfolio with innovations in SIM, eSIM and integrated SoC solutions. The three market approaches (SIM card, eSIM, and SoC) will coexist for several years. It is essential to address them in parallel despite differences in product and implementation. Their primary function remains the same: enabling connectivity, and customers expect flexibility.

Our roadmap includes developing secure SIM technologies that capitalise on the opportunities created by next-generation mobile networks such as 5G and NB-IoT and combine our expertise in semiconductor design, secure software, edge computing, AI, and blockchain to deliver highly innovative solutions.

Geographically, Trasna is focused on strengthening its presence in Europe, North America, and, like I said, India, where we see high growth potential in the IoT market for these technologies.

IoT Now: Finally, what would you like the readers to take away from this interview when it comes to key Trasna/Workz messages for telcos, service providers and end business customers?

SF: Trasna and Workz are committed to helping our customers drive the future of IoT with secure and innovative solutions, that offer them complete control and efficiency. We are a forward-looking, technology-driven company. Additionally, we are much leaner and more agile than some of the traditional market players, we are seeing that customers really appreciate the value that we provide them in terms of innovation, collaboration and agility.

One of Trasna's principles is that we are a technology-agnostic provider, meaning we do not have a vested interest in any specific technology or format

www.transna.io

David Farquharson
iONLINE

Improve business connectivity and sustainability with eSIM

"Trasna was uniquely positioned to help us develop customised solutions to meet our clients' needs, and in them, we found a supplier and like-minded ally to achieve our global IoT vision. Their dedication, innovation and collaborative spirit resonate deeply with our values at iONLINE. Their SIMs are manufactured on site with sustainability front of mind, ensuring minimal environmental impact."

David Farquharson, CEO of iONLINE

"We enjoyed working on this project with iONLINE. Their willingness to utilise new technology encouraged us to push the boundaries. It's been great to see how companies use our technology to protect their assets, react quicker to situations and gain greater visibility of their business. This partnership provides a springboard for us both as we continue to help businesses gain a competitive advantage from IoT."

Robert Varty, CSO of Trasna

Challenge

Companies managing connected assets on the move face significant challenges, including high roaming costs when leaving subscribed coverage zones, loss of signal in low coverage areas, and operational inefficiencies due to the need for dedicated resources to manage these issues. These challenges can lead to decreased device visibility and disrupt critical business tasks.

Partnership

The collaboration with **iONLINE**, a global IoT connectivity solutions provider, resulted in the development of FlexiSIM — an advanced hybrid eSIM solution. This partnership uses a cloud eSIM platform, enabling remote network switching and enhancing connectivity.

Solution and results

The hybrid eSIM solution enables businesses to automate network switching based on real-time conditions, significantly lowering running costs and avoiding service disruptions. The eSIM technology allows on-demand network selection, freeing companies from being locked into predefined network options. Additionally, the solution supports sustainability efforts by using 50% less plastic than traditional SIMs and enables remote updates, eliminating the need for physical SIM replacements.
As a result, iONLINE's private network now provides secure, high-speed connectivity in over 190 countries across more than 700 carrier networks. Launched in 2023 in South Africa, the UK and later the US, FlexiSIM is already benefiting companies such as **Fujifilm**, **AIoTSense**, **BrightBlue**, **Trellis Works**, **Online Direct**, **Amber Group** and **Fidelity ADT**, enhancing their connectivity and operational efficiency.

David Farquharson, CEO of iONLINE, said he approached several SIM manufacturers when first investigating options but that none brought the flexibility he wanted for the product.

Mark Kroodo
1oT

Reduce the time and cost of IoT connectivity

"We see Trasna as the perfect fit for 1oT to allow us to deliver faster connectivity to our clients. Their certified SIMs and supporting technical services give us a full flush of GSMA-certified products as well as the agility to scale up or down as needed, without some of the industry's usual heavy commitments required or competitive restrictions."

Märt Kroodo, co-founder and CEO of 1oT

"Our goal is to make it easier and cheaper for telcos to deploy connectivity. Whilst the SIM form factor has evolved over the decades, the process for generating their data has remained the same and is generally perceived as time-consuming. Our Data-Generation-as-a-Service cuts SIM development time and cost allowing telcos to activate connections and revenue far quicker."

Robert Varty, CSO of Trasna

Challenge

IoT-focused businesses attempting to digitise operations face challenges deploying secure and cost-effective IoT connectivity due to the complexities, time and costs associated with traditional SIM management.

Partnership

The partnership with **1oT**, an IoT connectivity provider combines 1oT's M2M global connectivity solutions with GSMA-certified eSIMs and Data Generation as a Service, streamlining the connectivity process for 1oT's enterprise customers.

Solution and results

The collaboration led to the launch of 1oT's eSIM Core, a remote SIM provisioning platform designed to simplify and reduce the costs of IoT device connectivity. Since its **GSMA** certification, eSIM Core manages over 1.4 million connected devices in over 170 countries in sectors such as micromobility, smart cities, autonomous vehicles, air monitoring and agricultural appliances.

Data-Generation-as-a-Service has further enhanced the offering by significantly cutting down SIM development time and costs, allowing telcos to deploy connections more efficiently. As a result, businesses can scale their connectivity solutions flexibly without the usual industry constraints, activating new connections and generating revenue much faster.

Itamar Kuni
Monogoto

Drive business growth with the flexibility of cloud eSIM

"We are proud to partner with Trasna and offer our customers a new platform for eSIM. Moving over to the eSIM cloud was easier and a lot quicker than expected. The move gives Monogoto the agility to address the evolving connectivity needs of our customers and partners as they arise."

Itamar Kunik, CEO of Monogoto

"eSIM adoption is rising rapidly as the opportunity for operators across consumer and M2M verticals expands – developments such as the first eSIM-only iPhone launched this month will only heighten this. Our cloud-based solution is designed to enable innovative connectivity providers like Monogoto to scale up quickly in this new market allowing them to move fast, grow and achieve a tangible return on investment."

Robert Varty, CSO of Trasna

Challenge

As the demand for connected devices continues to rise, **Monogoto**'s clients across 180 countries face challenges in managing multiple network profiles and ensuring seamless connectivity for both consumer and M2M devices. There was a need for a scalable and flexible eSIM solution to support diverse applications such as point-of-sale systems, ATMs, wearables, smart lighting and vehicle fleets.

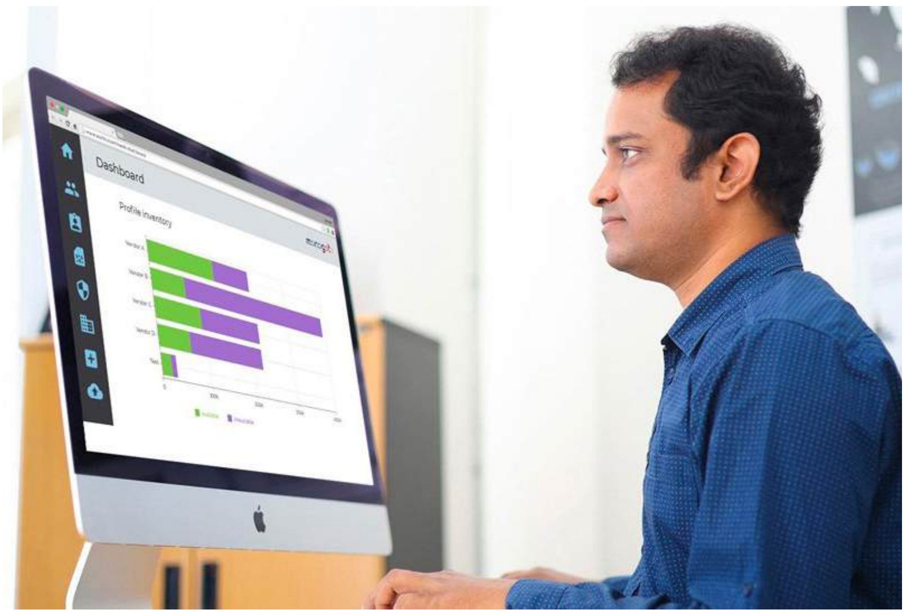
Partnership

This project with Monogoto, a global connectivity provider, established a cloud-based platform for managing consumer and M2M eSIM devices. This partnership utilises a GSMA-certified eSIM management platform to offer scalable and secure eSIM solutions.

Solution and results

The cloud platform developed through this partnership allows Monogoto's customers to easily manage eSIM profiles and install SIMs in QR code-supported devices, providing unprecedented flexibility in changing network profiles. This eSIM technology solution enables Monogoto to provide connectivity services for devices such as point of sales, ATMs, wearables, smart lights, fleets of cars and packages.

The collaboration has positioned Monogoto to cater to the rapidly growing eSIM market. The platform's flexibility and scalability enable Monogoto to provide enhanced connectivity services, helping clients seamlessly adapt to the evolving IoT landscape and driving the company's growth strategy.



Robert Varty,
Trasna

Revolutionise water management with eSIM

"We are delighted to be a part of such a large-scale government venture that uses new eSIM technology to make such a significant impact on people's quality of life. Our aim as a company is to provide quality and rapidly deployable solutions and, alongside our team in Africa, we have been able to quickly get this project off the ground and make it a full-scale reality."

Robert Varty, CSO of Trasna

Challenge

In many African regions, access to clean drinking water is a critical issue, with poor water management contributing to health crises such as cholera outbreaks. To address this challenge, a large African government aimed to implement a smart water management solution that could improve the availability and quality of drinking water for its population.

Partnership

Working with a leading African network operator and government, this multi-party venture aimed to deploy embedded SIM (eSIM) technology in smart water meters. As the only GSMA-certified eSIM manufacturer in the Middle East and Africa, Trasna provided the eSIM modules and remote provisioning solutions necessary for this large-scale project.

Solution and results

eSIM technology, from the SIM chips to their remote SIM provisioning cloud platform, plays a key role in supporting this government's smart city initiative, enhancing water management infrastructure, and improving public health conditions. The project launched in 2019 and has significantly enhanced the quality of life by making clean water more accessible and supporting the broader goal of sustainable urban development.

Rob Beswick,
Virgin Mobile UAE

Increase telco sustainability and reduce plastic usage

Challenge

Every year, an estimated 14 million tons of plastic end up in the oceans, harming fragile ecosystems. With around six billion SIM cards produced annually, the telecom industry significantly contributes to global plastic waste. Virgin Mobile MEA aimed to address this environmental challenge and reduce its plastic footprint across its operations.

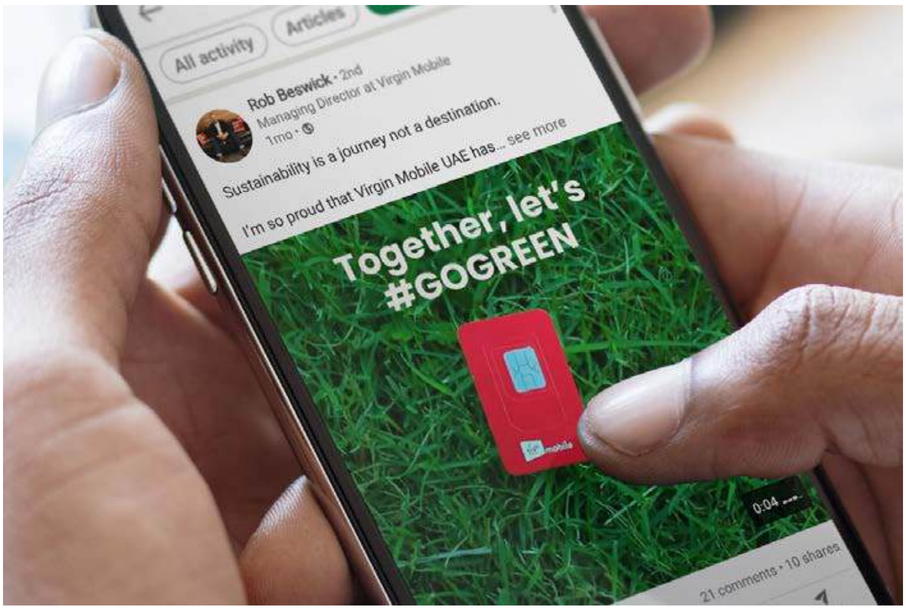
Partnership

Virgin Mobile MEA turned to its long-term partner to tackle the plastic waste issue. Over their twelve-year partnership, the companies have collaborated on various initiatives to reduce environmental impact across the telecom supply chain. This time, they focused on introducing an eco-friendly alternative to traditional SIM cards.

Solution and results

Virgin Mobile MEA became one of the first mobile network operators in the Middle East to adopt **EcoSIM**, a biodegradable SIM card made from oxo-biodegradable plastic. Unlike standard SIM cards that take hundreds of years to decompose, the EcoSIM breaks down in landfills within 18-30 months. This environmentally conscious initiative aligns with Virgin Mobile MEA's commitment to becoming carbon negative.

EcoSIM not only reduces the plastic footprint but also incorporates sustainable practices, such as using recycled paper packaging, reusable wooden pallets for transportation, and supply chain optimisation to lower carbon emissions. The adoption of EcoSIM has allowed Virgin Mobile MEA to take a leading role in promoting sustainability within the telecom industry, significantly enhancing its eco-friendly brand credentials while contributing to global plastic waste reduction.



"As consumers are becoming more environmentally conscious, the onus is on companies to innovate and introduce sustainable alternatives to ensure a collective effort towards building a better future. Our new sustainable SIM cards are another key step in the right direction."

Rob Beswick, managing director of Virgin Mobile UAE

"We're delighted to have achieved yet another market-first with Virgin. We are currently seeing a sharp rise in interest from network operators worldwide for more sustainable alternatives such as biodegradable SIMs and eSIM – this can only be a good thing. What this project with Virgin demonstrates is, that with a dynamic, forward-thinking approach, just how quick and significant the impact can be."

Robert Varty, CSO of Trasna

Toby Gasston,
Wireless Logic

Itamar Kunik,
Monogoto

Nick Earle,
Eseye

Is the jury still out on how far the eSIM market will rise?

Market estimates for the size of the embedded SIM (eSIM) market are varied among analysts, but one thing that is certain, is that it's growing. Antony Savvas looks at the driving forces behind this growth and considers whether the technology really will hit critical mass this time, after a pretty long run-up

An eSIM can offer enterprises and consumers the freedom and flexibility to roam through different territories using the same SIM credentials, without having to use a changeable physical SIM card. A prime advantage is that an eSIM can also connect to the best performing network at the best price, well that's the theory anyway.

Enabling a major shift

As analyst **Statista** outlines, an eSIM is a technology enabling a major shift in the way cellular plans are activated and transferred. An eSIM functions as a digital SIM card embedded within a device, and offering greater ease of use, security and sustainability benefits, when compared to a traditional, physical SIM card.

While eSIM usage is expected to become commonplace in smartphones, their use extends to all manner of connected devices that use a cellular network, such as connected cars, drones and smartwatches. According to Statista, the market for eSIMs is forecast to 'explode' alongside the rise of IoT devices.

It says the eSIM market was valued at US$4.7 billion in 2023, and is expected to grow to US$16.3bn by 2027. Other analysts have other estimates.

According to **Fact.MR**, the eSIM market was valued at US$7.3bn in 2022, and is forecast to grow to US$22.2bn by 2032. And, **Grand View Research** says the market was worth US$8bn in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 7.9% from 2023 to 2030.

Citing other sources, Grand View estimates there were 1.2 billion eSIM-enabled devices in 2021, with that number expected to climb to 3.4 billion by 2025. Other estimates point to six billion devices, covering smartphones, consumer electronics, health monitoring, transport and smart energy, using eSIMs by 2025.

Pioneering Apple

Apple has been a pioneer of consumer eSIM transition, particularly in the US, where it has just released its third consecutive eSIM-only iPhone. Eric Morhenn, chief operating officer at eSIM provider **Nomad eSIM**, says: "Apple's decision to produce and sell only eSIM-compatible iPhones for the US market is another step towards a wider global strategy. Apple's vision is to move away from physical SIM cards completely within the next few product cycles." ▶

The benefits of eSIMs have led Apple to shift to eSIM not only in its iPhones, but across the product range. For instance, the 2024 iPads are now eSIM-only worldwide, and as Morhenn notes: "Apple is likely to expand this shift to other devices, with Apple Watch and even MacBooks using eSIM functionality as the norm, which then will end up creating a fully connected ecosystem."

This interconnectedness simplifies how users manage devices, network access and data across Apple's ecosystem, enhancing both the user experience and device performance, as well as keeping Apple customers ever closer to the company, of course.

As IoT ecosystems expand, businesses will need to adapt to new technologies, evolving market conditions and different MNO priorities

Moreover, the global adoption of eSIM aligns with Apple's environmental and privacy goals. The removal of physical SIM trays reduces electronic waste and allows for better water and dust resistance, making devices more durable. In addition to these hardware benefits, the digital nature of eSIM also enhances security by reducing the risk of SIM swapping attacks, which is a common form of fraud in the industry.

While Apple has pioneered the move towards eSIM-only phones in the US, the company is expected to expand this strategy globally. Morhenn says: "We can expect Apple to make the same move – starting as early as the iPhone 17 or 18 – in international markets like Europe, Japan, and Singapore, where the digital infrastructure is strong."

Apple is likely to continue to monitor global market readiness and gradually introduce eSIM-only devices in emerging markets once more carriers and regulators adapt to the technology. Apple isn't the only one leading this change though. **Samsung** has already taken its first step towards this transition by recently announcing that its new Galaxy S24 series will include built-in eSIM capabilities.

Morhenn maintains: "The complete transition to eSIM globally is not a question of 'if', but 'when', but Apple is taking the lead in this change."

Factors affecting the market

As always though, various factors can affect any new market. Toby Gasston, the mobile core product lead at **Wireless Logic**, says: "When looking at the difference between local and global deployments, it's easy to forget that any deployment of IoT devices is challenging at scale. For example, a rollout in a local market requires consideration of a variety of factors, such as coverage, the appropriate technologies and local regulations."

"These factors can vary significantly based on geographic and technical conditions, from network availability to compliance with specific regulatory standards," he adds.

However, when deployments expand to a multi-national or global scale, the complexity increases exponentially, he says. Not only must businesses address the same local challenges across multiple regions, but they must also account for additional variables, such as managing diverse regulatory frameworks, roaming agreements and operational differences across countries.

"Moreover, the global connectivity landscape is always shifting, with new technologies, changing market conditions and shifting operator partnerships," says Gasston. "The ability to maintain seamless, reliable connectivity while adapting to these dynamic conditions is critical for the success of global IoT deployments."

Remote provisioning

Remote SIM provisioning (RSP) was initially presented as a step change in the market, promising customers the ability to take control of their connectivity provider options throughout the lifespan of their devices.

"However, with the introduction of the SGP.02 standard [ten years ago], it quickly became apparent that the reality was far more complex, requiring expensive integrations between providers to bring this functionality to life," Gasston adds.

Now, with SGP.32, it seems the same excitement is being generated within the industry "without sufficient considerations beyond the technology itself", he maintains. RSP and embedded universal integrated circuit cards (eUICC) and eSIMs serve as delivery mechanisms, which means they do not resolve issues like contractual ownership changes or the practicality of end customers managing devices in the field.

Market confusion

While connectivity providers can address some of the challenges around RSP and SGP standards, the confusion in the market extends beyond remote SIM provisioning, Gasston adds. "Although 3GPP and GSMA are doing excellent work defining the future of IoT, a recurring issue remains. Mobile network operators (MNOs) around the world have differing priorities and approaches to making these technologies available in their respective markets. As a result, module manufacturers often find themselves ahead of MNOs in adopting and implementing new technologies."

And, while we'll see more advanced solutions being developed, they are likely to come with new challenges. Global deployments will demand seamless connectivity across regions, with evolving standards like SGP.32 helping to improve interoperability. However, addressing non-technical issues like regulatory compliance and ownership rights will remain critical.

"As IoT ecosystems expand, businesses will need to adapt to new technologies, evolving market conditions and different MNO priorities," says Gasston. "Collaboration between industry stakeholders will be essential to ensure that the promise of flexible, global connectivity becomes a practical reality."

A mixed picture

A recent industry podcast covered the importance of SGP.32, but also outlined the mixed picture when it came to building eSIM success around the standard.

On **Eseye**'s IoT Leaders podcast, Matt Hatton, founding partner at analyst **Transforma Insights**, says: "SGP.32 has generated significant interest and confusion within the industry. While some see it as a panacea for all IoT deployment issues, the reality is more nuanced. But still, there's been a rush of startups and companies experimenting with this next-generation eSIM standard."

The GSMA developed SGP.02 for M2M communications back in 2014, followed by SGP.22 for consumer devices in 2016. Each had its limitations, prompting the need for a more versatile standard, hence the introduction of SGP.32 in 2023. "The ongoing efforts to improve IoT connectivity have been essential, hence the introduction of SGP.32, particularly in areas where traditional SIM solutions have fallen short," Hatton explains.

Flexibility

Flexibility has been critical for businesses needing to deploy IoT devices in diverse and often challenging environments where past connectivity solutions have struggled. One of the most notable advancements in SGP.32 is the introduction of the IoT profile assistant (IPA), which acts as a user to pull profiles from chosen providers. This mechanism simplifies switching operators, addressing the clunkiness of previous standards and making it easier for businesses to maintain consistent connectivity across their IoT deployments.

"SGP.32 is not just an incremental upgrade, it's a significant leap forward in IoT connectivity," says Nick Earle, the chief executive of Eseye. "It is designed to be more flexible and lightweight than its predecessors. It supports a variety of deployment scenarios without the need for SMS and offers reduced footprint requirements, making it suitable for constrained IoT deployments."

But, as promising as SGP.32 may be, it's essential to understand its current limitations, Earle says. "SGP.32 is not yet fully available. Standards are still being finalised, and we don't expect full SGP.32 capabilities until early 2025."

Navigating issues

It is essential therefore, that enterprises know that any solutions marketed as SGP.32 today are likely pre-standard versions with significant potential interoperability issues. Although the transition to SGP.32 will not be without its challenges. These can be effectively navigated with proper planning and support though.

"Ensuring consistent APN settings and properly notifying the current operator to avoid continued billing are just a few of the considerations that businesses need to manage," Earle adds. "Managing the transition from existing standards to SGP.32 will be complex and likely require a managed service provider. This approach ensures all aspects of connectivity, including access point name (APN) settings, local breakout and service level agreements (SLAs) are properly handled."

Deployments

Despite the issues though, there's still plenty of business of course being built around eSIMs. International connectivity provider **Monogoto**, for instance, is partnering with global eSIM provider **Workz**, to establish a cloud platform to manage both consumer and M2M eSIM devices for its client base across 180 countries.

Monogoto uses eSIMs to provide connectivity services for devices such as point-of-sale systems, ATMs, wearables, smart lights and car fleets, among other applications. Workz has launched a cloud-based eSIM management platform for networks, which is certified by the **GSMA**.

"Moving over to Workz's eSIM cloud was easier and a lot quicker than expected," says Itamar Kunik, the chief executive of Monogoto. "The move gives Monogoto the agility to address the evolving connectivity needs of our customers and partners as they arise."

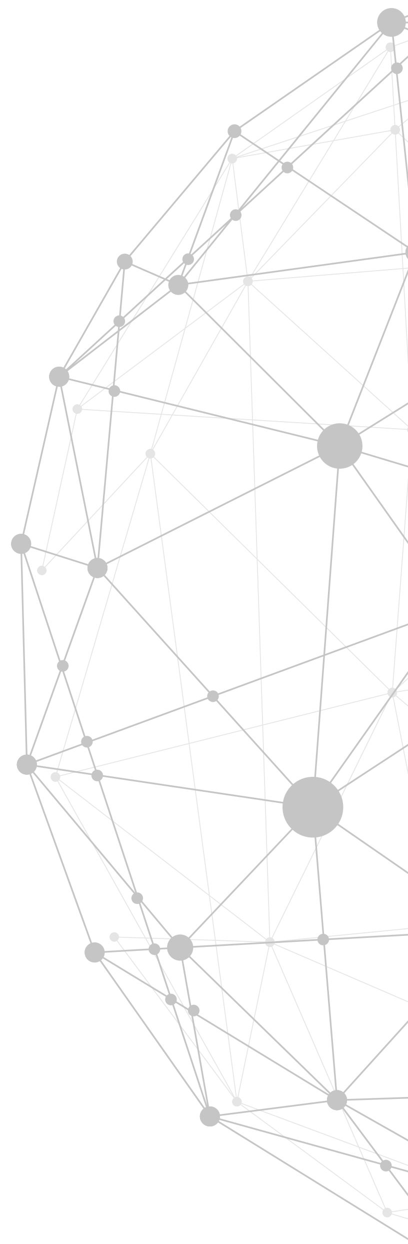
Another eSIM player is **u-blox**, a provider of positioning and wireless communication services through the use of connected and secure modules in various form factors.

Wireless Logic's IoT connectivity network, Conexa, has been integrated into u-blox's cellular modules. The integration provides customers with enhanced control and visibility over their IoT deployments, allowing them to manage connectivity directly through Wireless Logic's platform. Additionally, they can benefit from various complementary service extensions, such as anomaly detection offered by Wireless Logic.

"By combining our technologies, we are enhancing the value proposition for IoT deployments, providing unmatched connectivity, security, and flexibility," says Martin Leach, the head of the u-blox cellular business unit.

According to the GSMA, even in 2022, eSIM services had already grown 500% over the previous three years, with more than 230 network providers in 80 countries catering for the next-generation technology. So, the eSIM obstacles that do exist, were and are, being overcome one way or another.

Flexibility has been critical for businesses needing to deploy IoT devices in diverse and often challenging environments where past connectivity solutions have struggled



IoT Now: ISSN 2397-2793

2024 • VOLUME 14 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

COVER INTERVIEW

Giesecke+Devrient Mobile Security's CEO explains how IFPP embeds secure and flexible device connectivity in the factory

The IoT Now CEO Guide to IFPP 2024

PLUS: How in-factory profile provisioning is helping OEMs address the need for greater manufacturing speed • Inside Giesecke+Devrient's AirOn360 IFPP system • Why connected device makers should take a closer look at IFPP • Will IFPP help accelerate eSIM adoption? • Read the latest News, Features and Interviews at **www.iot-now.com**

IFPP embeds secure, flexible device connectivity in the factory

In-factory profile provisioning (IFPP) has been created to enable the secure loading of mobile network operator (MNO) profiles onto consumer and IoT devices during manufacture. The technology promises to streamline embedded and integrated SIM (eSIM and iSIM) integration, enabling business benefits such as a single global stock-keeping unit (SKU) to be accessed. Here Dr. Philipp Schulte, the CEO of Giesecke+Devrient (G+D) Mobile Security, tells George Malim, the managing editor of IoT Now, how IFPP is transforming device manufacture

IFPP enhances security by ensuring that devices are protected from the outset, minimising the risks associated with manual configurations and physical SIM handling

George Malim: Please can you tell us what IFPP is and explain the benefits to OEMs?

Dr. Philipp Schulte: IFPP is an innovative solution that allows device manufacturers to securely load MNO profiles onto consumer and IoT devices during the manufacturing process. This means that when devices leave the factory, they are already equipped with the necessary connectivity, ready to function immediately upon activation. At G+D, we say that these devices are 'Born Connected'.

Until now, manufacturers were often working with different physical SIM cards from their preferred MNOs, which needed to be inserted manually into the device. Even when working with eSIM technology, manufacturers needed to prepare different modem SKUs depending on the target destination.

By digitalising these processes, IFPP offers several key benefits to OEMs. It enables devices to be pre-configured with eSIM profiles, providing instant connectivity straight out-of-the-box, which significantly enhances the end-user experience. The solution also streamlines the deployment process by embedding connectivity during production, thereby reducing the need for post-purchase configuration and accelerating time-to-market.

Furthermore, IFPP enhances security by ensuring that devices are protected from the outset, minimising the risks associated with manual configurations and physical SIM handling. Finally, by eliminating the need for manual SIM card installation and activation, OEMs can achieve substantial cost savings, allowing them to allocate resources more effectively towards innovation and scaling their operations.

As the producer of the first commercial SIM card and a pioneer in eSIM management, G+D is currently the only provider in the market to have rolled out a large-scale commercial deployment of more than 100 million profiles to a leading global consumer OEM.

GM: What technologies have made IFPP a reality?

PS: IFPP is based on eSIM technology, which is now taking off in the consumer as well as the IoT space. eSIM allows for secure and remotely programmable SIM profiles, eliminating the need for physical SIM cards. This is further enhanced by remote SIM provisioning (RSP) which enables the remote management and updating of these eSIM profiles over-the-air (OTA).

IFPP is based on the newest standard for RSP currently being finalised by the GSMA (SGP.42), which is closely linked to the SGP.22 (consumer) and SGP.32 (IoT) standards. These use a common technology base which makes IFPP easily scalable for MNOs and device manufacturers that already work with these standards. When combined with SGP.22 or SGP.32, IFPP also gives maximum flexibility to the end user, who can then make further changes to the profile once the device is in the field.

In addition, advancements in secure manufacturing processes and cloud-based management platforms have played crucial roles in making IFPP viable. These technologies ensure that the profile provisioning process is not only secure but also scalable and efficient, meeting the rigorous demands of modern OEMs. ▶

SPONSORED INTERVIEW

Dr. Philipp Schulte
G+D Mobile Security

GM: How do you foresee mainstream adoption of IFPP accelerating?

PS: Mainstream adoption of IFPP is likely to accelerate as the demand for connected devices continues to grow across various industries. With the proliferation of IoT devices, the need for efficient, secure and scalable connectivity solutions is becoming increasingly critical. IFPP addresses this need by simplifying the onboarding process, reducing deployment times and ensuring secure connections from day one.

Furthermore, as more OEMs recognise the operational and cost efficiencies associated with IFPP, adoption is expected to increase. Regulatory standards and industry collaborations will also play a role in accelerating mainstream adoption, as they establish a unified framework that drives confidence and adoption across the ecosystem.

For example, G+D has already seen significant interest from OEMs, with the first large-scale commercial deployment in the consumer space, which has proven to be very secure and scalable. While the GSMA standard is still in progress, G+D's solution is ready for deployment and we also see demand from IoT markets such as the smart metering and automotive sectors.

GM: How will it be applied to existing products and use cases and what types of new use cases do you envisage? ▶

PS: IFPP can be applied to a wide range of existing products across various sectors, such as consumer electronics, automotive, utilities and industrial IoT. For example, in the automotive industry, OEMs need to manufacture vehicles for distribution all over the world, making local connectivity per country a pre-requisite. Whereas previously this could only be done by deploying different SKUs for different countries. IFPP saves time and money by allowing them to use a single SKU for all vehicles and include the eSIM profile during the manufacturing process. Vehicles can therefore be delivered with global-ready connectivity, enabling seamless communication and telematics for vehicles on the go.

In smart metering, for example, utilities companies can pre-configure meters with network profiles during the manufacturing process, enabling the meters to automatically connect to the network upon installation. This eliminates the need for technicians to manually configure or activate the devices in the field, resulting in faster deployment, reduced operational costs and a more seamless integration of smart metering solutions into energy grids.

As for new use cases, we envisage applications in emerging fields such as smart cities, where connected infrastructure could benefit from out-of-the-box connectivity, and in smart agriculture, where sensors and devices could immediately connect to monitor and optimise crop production. The scalability and flexibility of IFPP opens up possibilities for numerous innovative use cases across industries.

GM: What differences are there for consumer, IoT and automotive OEMs?

PS: While the core principles of IFPP remain consistent across various sectors, the requirements and advantages can differ depending on the specific vertical and type of OEM. For consumer electronics, the focus is primarily on providing instant connectivity for devices such as wearables and smartphones. For these high-convenience consumer devices there is often a requirement to connect directly out-of-the-box without the need to use Wi-Fi. IFPP helps to enhance the user experience by eliminating set-up steps as well as ensuring seamless connectivity across different regions.

In the IoT sector, IFPP is particularly beneficial for OEMs that produce devices like smart meters, industrial sensors and logistics trackers. Using IFPP based on eSIM to pre-configure these devices with connectivity during production simplifies the deployment of large fleets of devices by eliminating the need to manually insert plastic SIM cards.

The automotive sector has its own unique set of needs. IFPP allows automotive OEMs to equip vehicles with global-ready connectivity right from the production line, facilitating essential functions such as telematics and vehicle-to-everything (V2X) communication. This capability is crucial for OEMs aiming to standardise vehicle connectivity across various markets. Combined with a private network, IFPP can help transfer large amounts of data. This helps OEMs to streamline their production and achieve their goals for the software-defined vehicle.

While the underlying technology of IFPP is the same, its application is tailored to meet the distinct demands of each sector, whether it's enhancing user experience, ensuring real-time data connectivity, or enabling seamless global communication.

GM: What is G+D's approach to IFPP and how does your experience ensure IFPP is secure, scalable and simple to deploy?

PS: G+D's approach to IFPP is rooted in our extensive experience in secure communications and our deep understanding of the mobile connectivity landscape. We have designed IFPP to be a seamless, end-to-end solution that integrates security, scalability and simplicity.

Security is paramount in our solution, which is why we utilise GSMA-certified standards and secure elements to protect the eSIM profiles during provisioning. Our cloud-based infrastructure ensures that the process is not only scalable but also flexible, ▶

The G+D AirOn360 portfolio complements IFPP by providing a comprehensive suite of services for secure connectivity management

accommodating the needs of OEMs regardless of their production volumes. In addition, our global presence and partnerships with MNOs allow us to offer a solution that is both universally applicable and tailored to specific market needs.

The simplicity of deployment is another key aspect. We've designed IFPP to integrate easily into existing manufacturing processes, minimising disruption and enabling OEMs to quickly realize the benefits of in-factory provisioning.

GM: What other offerings in the G+D AirOn360 portfolio enhance the functionality of IFPP and enable new use cases?

PS: The G+D AirOn360 portfolio complements IFPP by providing a comprehensive suite of services for secure connectivity management.

Firstly, the G+D eSIM chip enables the service, in combination with our AirOn360 IoT Suite eSIM management solution and the GSMA SGP.22 and SGP.32 standards which give customers the freedom to change the operator while the device is in the field. RSP allows for the OTA management of eSIM profiles, enabling OEMs to update or switch profiles post-deployment, thus enhancing the flexibility and longevity of connected devices.

In addition to the eSIM solution, the OEM must have access to the right connectivity agreements globally. To ensure scalability and end-to-end security, it's important that all these elements are centrally managed by the same provider. G+D can provide global multi-network connectivity on over 600 networks in 185 countries, ensuring that the OEM has the best connectivity solution, wherever the devices are deployed.

Additionally, our AirOn360 IoT Suite platform includes advanced analytics and lifecycle management tools that help OEMs monitor and optimise the performance of their devices in real-time. This not only improves operational efficiency but also opens up new possibilities for use cases that require dynamic management of connectivity, such as pay-per-use models or location-based services.

Together, these offerings ensure that IFPP is not just one solution but part of a broader, integrated ecosystem that supports the evolving needs of connected devices across industries. ■

www.gi-de.com

IFPP helps OEMs address the need for greater speed in IoT device manufacturing

In-factory profile provisioning (IFPP) enables OEMs to embed cellular SIM profiles into devices on the factory floor, thereby accelerating and opening up embedded and integrated SIM benefits. Simply put, IFPP embeds SIM functions into devices at the point of manufacture so configuration isn't needed outside the factory at the point of deployment

A key benefit of IFPP is that it enables a manufacturer to flash various SIM profiles to the device in production depending on the requirements of the deployment

Provisioning of SIM cards in the field or national distribution centres is time-consuming and expensive. It is also inflexible because installation of SIMs doesn't allow for the device to change mobile network operator unless it has a new, alternative SIM installed. To address this and take advantage of the flexibility that embedded and integrated SIM (eSIM and iSIM) offer, OEMs have been looking to install SIM functionality into devices at the factory, during the manufacturing process.

The technology is based on the upcoming GSMA SGP.42 specification which is being developed currently. This specification will simplify loading of operator profiles during manufacturing and ensure security is maintained. However, SGP.42 remains more than a year away, even though IFPP-enabled options are already on the market from players such as **Thales, G+D** and others. These offerings provide an upgrade path to IFPP when it arrives and, in the meantime, allow OEMs to access the benefits of IFPP.

Streamlined manufacturing

A key benefit of IFPP is that it enables a manufacturer to flash various SIM profiles to the device in production depending on the requirements of the deployment. This allows a product to have a single global stock-keeping unit (SKU) number and eliminates the need to manufacture regional variants with localised SIM cards inside. Plastic cards and all the inventory headaches they necessitate become a thing of the past thanks to eSIM and iSIM but IFPP makes adoption simpler and more flexible and therefore has the potential to drive uptake.

A further benefit is the flexibility that IFPP brings to the manufacturing process. IFPP IoT products are pre-configured to connect to the optimum network on activation and therefore there is no need for the SIM to update via a bootstrap profile or to be pushed an initial over-the-air (OTA) profile update via remote SIM provisioning (RSP). This offers advantages in terms of power saving because the battery-hungry RSP process isn't utilised.

In addition, the removal of cumbersome OTA and RSP processes greatly simplifies initial introduction of an IoT device, reducing the need for operators to support bootstrap profiles on the home subscriber server (HSS). The acceleration of the manufacturing, deployment and installation process that IFPP helps contribute to is becoming of increasing importance as development lifecycles for IoT deployments grow longer.

Research firm **IoT Analytics** has reported that this has seen the average time from the start of the project to the first paying customer increasing from 23 months to 41 months. Given the intensely competitive IoT landscape and the sheer volume of devices and applications being introduced, time-to-market of more than three years is unacceptable for IoT-connected products. According to the firm's survey of 100 senior executives and department leaders at OEMs, queried as part of the IoT Analytics' 206-page 'IoT Commercialisation and Business Model Adoption Report 2024', companies took an average of 18.5 months to go from project kick-off to proof of concept, with business case development and stakeholder alignment taking a large chunk of the time. It then took 22.8 months from proof of concept to the first paying customer.

The firm goes on to say that the 80% increase in time-to-market has occurred in spite of recent technological developments that would be expected to have resulted in better tools and hardware to help accelerate product introduction. Although the 80% increase in product time to market appears on the high side, the team at IoT Analytics has had several discussions with various market actors who shared that they have seen OEMs taking longer to get their products to market as well.

More complete, more complex deployments

For example, a senior manager at an edge computing software provider recently shared that customers are spending more time addressing ▶

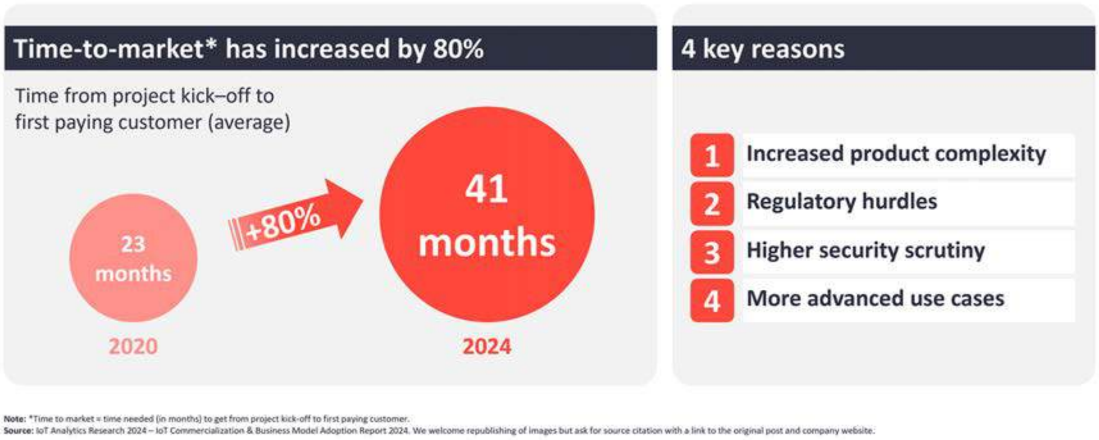


Figure 1: Time to market for IoT-connected products

Source IoT Analytics

security requirements and developing value-adding features, capabilities and analysis tools. A senior manager at a cloud-based IoT platform provider added that their clients' average project team size increased from 14 team members in 2014 to 20 in 2024, leading to increased complexity. This demonstrates that greater maturity in IoT is leading to more complete yet more complex products and services being brought to market.

More features and stronger security take longer to develop so increased time-to-market isn't a surprise. However, clawing back the lost time is desirable and IFPP provides a means to do this alongside its other benefits.

Berg Insight sees RSP and IFPP, both of which are being worked on by GSMA, as significant contributors to SIM-related efficiencies. Most industry participants foresee the new GSMA IoT eSIM specification (SGP.32) for RSP to replace the M2M eSIM specification (SGP.22) over time and contribute to higher eSIM adoption, the firm says. It expects commercial implementations to start in the first half of 2025, assuming no further delays occur.

The eSIM working group in GSMA has also started working on IFPP of consumer and IoT devices. The specification (SGP.41/42) will help simplify the loading of profiles at the manufacturing stage but is at an earlier stage of development with commercial implementations a few years out, says Berg Insight. The major SIM vendors are in various ways helping customers to prepare and transition to the next generation of eSIM solutions. **Eseye** for example has announced that it is working with Thales to test IFPP and utilises the Thales Adaptive Connect solution to support SGP.32-type remote provisioning.

The GSMA specifications simplify SIM provisioning and the outline capabilities of IFPP detail how iSIM profiles can be allowed to be uploaded to a device during production. As a result of this increased convenience, the **Juniper Research** predicts that the number of iSIM connections will rise to 210 million by 2028 globally. The firm identified use cases such as smart energy meters and remote logistics as being primed for immediate adoption; owing to requirements for power-conscious and small form factor devices.

In order to prepare for this growth, report author Elisha Sudlow-Poole recommended: "eSIM vendors must ensure that they provide standard-agnostic platforms that are flexible to upcoming form factors, standards and use-case demands. Additionally, eSIM vendors must develop trusted partnerships with manufacturers to ensure adoption of iSIM connectivity services once it becomes demanded in the market."

Berg Insight sees RSP and IFPP, both of which are being worked on by GSMA, as significant contributors to SIM-related efficiencies

Revolutionise device connectivity with in-factory profile provisioning

With IoT reshaping industries, the demand for seamless, secure and ready-to-use connectivity is more urgent than ever. IoT devices, along with consumer electronics such as smartphones and smartwatches, require efficient, secure and immediate network access the moment they leave the factory

Traditional device provisioning requires a second-step connectivity setup after production

Giesecke+Devrient (G+D) utilises in-factory profile provisioning (IFPP) technology in its AirOn360 In-Factory eSIM solution, which addresses these challenges by allowing mobile network operator (MNO) profiles to be directly installed into devices during production, enabling devices to be connected straight out of the box.

The use cases in this article highlight the benefits and real-world applications of IFPP technology in IoT and consumer electronics. Focusing on telecommunications, smart metering and consumer devices, we show how IFPP streamlines device deployment, improves user experience and drives new business models.

Why is IFPP better?

Traditional device provisioning requires a second-step connectivity setup after production. Customers must configure devices to connect to Wi-Fi, Bluetooth, or mobile networks, adding time, effort and potential security risks during onboarding. For MNOs leasing or selling smartphones and connected devices, this means the devices aren't immediately network ready. The complexity caused by this extra setup step causes delays, higher support costs and a less optimal user experience.

SPONSORED CASE STUDY

In contrast, IFPP integrates MNO profiles directly into devices during manufacturing, enabling them to access mobile networks instantly without additional configuration. This pre-provisioned connectivity simplifies user onboarding and enhances security, as devices connect to secure networks from the start.

The challenge

Before the advent of IFPP, manufacturers and MNOs faced several key challenges:

- **Complex configuration:** Traditional IoT and smartphone onboarding requires manual network setup, which can be time-consuming and confusing.
- **Delayed access:** Devices often lack pre-installed network profiles, causing service delays, especially for MNO-supplied devices.
- **Increased support costs:** MNOs face increased support costs as users struggle with initial network connections.
- **Security concerns:** First-time setup can expose devices to vulnerabilities, especially when connecting to unsecured networks.

G+D's AirOn360 In-Factory eSIM

G+D's IFPP solution, AirOn360 In-Factory eSIM, addresses these challenges by provisioning MNO profiles directly into devices during production, offering key benefits for MNOs and device manufacturers. This simplifies logistics and allows sale of connectivity-enabled devices directly, such as through flagship stores. Conversely, MNOs can sell devices that are enabled for their network.

How it works:

- **Ordering:** Typically, the device manufacturer orders a connectivity service and cellular eSIM profiles from the MNO, which commissions G+D to create the eSIM profiles and produce the eSIM modules. These eSIM modules are equipped with the G+D SIM-OS, but without MNO credentials. MNO-specific eSIM profiles are delivered digitally to the manufacturer via a secure transfer channel, while eSIM modules are shipped through standard logistics.
- **Device production:** Profiles are securely loaded onto the eSIM during production, without needing a permanent online connection or GSMA Security Accreditation Scheme (SAS) certification of the manufacturing landscape.
- **Shipment:** Completed devices are dispatched to the target destination.
- **Streamlined deployment:** After the device leaves the factory, it is fully configured for the designated cellular network, offering instant connectivity to end users.

This method ensures devices are pre-configured to connect directly to the MNO's network without needing Wi-Fi or Bluetooth. Smartphones, smartwatches, and IoT devices can immediately start using cellular networks for sending and receiving data.

Real-world applications

Telecommunications (MNO-supplied devices)
MNOs, especially those selling or leasing smartphones, benefit most from IFPP. Customers often receive phones with pre-installed SIM cards or must configure them before connecting to the MNO's network.

With IFPP, MNOs can ship fully pre-configured devices with a suitable cellular profile, allowing customers to use them immediately without visiting a store or following complex setup instructions. This can drastically reduce activation times for customers, resulting in higher customer satisfaction and lower operating costs, as there are fewer support calls related to the initial network setup, for example.

Consumer electronics (smartwatches and wearables)
For consumer electronics like smartwatches and wearables, IFPP ensures instant out-of-the-box functionality. This seamless integration benefits devices that rely on cellular networks for messaging, GPS and health monitoring.

Wearable vendors utilise IFPP to pre-provision devices with eSIM profiles for global MNO partners. This not only enhances the user experience but also allows the company to expand their global reach by shipping region-specific devices that are ready to connect to local mobile networks.

IoT device manufacturers (smart meters and industrial equipment)
In industrial IoT, devices such as smart meters, security cameras, and machinery sensors benefit from immediate network connectivity via cellular networks. IFPP eliminates the need for technicians to manually configure and connect devices at the deployment site, significantly reducing setup time and operational complexity.

For instance, a smart meter manufacturer integrates IFPP into its production process, allowing the meters to automatically connect to mobile networks upon installation in customer homes. This streamlined deployment process improves scalability, as technicians no longer need to spend so much time setting up devices on-site and it ensures a faster return on investment for utility companies.

Before IFPP, physical SIM cards would sometimes have to be exchanged in-field when updating the contracted MNO. By replacing this labour-intensive and error-prone process with a fully digital one, the manufacturer can reduce costs while providing a faster and more reliable service. Greater flexibility is still maintained by allowing seamless integration with multiple MNOs.

Benefits of G+D's AirOn360 In-Factory eSIM

The key benefits of our IFPP technology are:

- **Faster time-to-market:** Devices are immediately connectivity-ready, reducing lead times and accelerating product launches.
- **Reduced support costs:** Simplified setup processes reduce the need for extensive customer support, improving operational efficiency.
- **Enhanced user experience:** Customers enjoy instant network access with no need for complex configurations, leading to greater satisfaction.
- **Improved security:** Pre-configured devices reduce the risk of security vulnerabilities during initial network setup.
- **Scalability:** G+D's AirOn360 In-Factory eSIM enables manufacturers to deploy IoT and consumer devices at scale without the need for manual provisioning processes.

G+D's AirOn360 In-Factory eSIM revolutionises device manufacturing by loading network profiles during production. This technology reduces complexity, enhances user experience and improves security. As IoT grows and consumer expectations rise, IFPP helps MNOs and manufacturers stay competitive in a connected world. ■

__MNOs, especially those selling or leasing smartphones, benefit most from IFPP__

www.gi-de.com

What is in-factory profile provisioning and why is it useful for connected device makers?

Over the last couple of years, the topic of eSIM and remote SIM provisioning (RSP) has been a prominent one in the consideration of how to connect cellular IoT devices. The majority of the emphasis has been on in-field provisioning, i.e. changing the profile on the device after it has been deployed. However, in 2024 attention has also grown in the theme of in-factory profile provisioning (IFPP), which involves the secure loading of SIM profiles during the manufacturing and/or order fulfilment process, writes Matt Hatton, the founding partner of Transforma Insights

IFPP works by allowing the manufacturer to load an eSIM profile via a profile loader in the manufacturing line from a digital inventory of mobile network operator (MNO) eSIM profiles

In February, **Transforma Insights** and **Kigen** published a Position Paper 'In-factory profile provisioning (IFPP): new eSIM approach drives profitability and improves product performance in connected electronics manufacturing' examining the concept of IFPP as an emerging approach to remote SIM provisioning for IoT connected devices.

What is IFPP?

With the increasing prevalence of soldered eSIM chips, and the likely growth in the use of integrated SIM (iSIM) in future, combined with increasingly strict rules requiring network localisation in many countries, there was a requirement to develop the capability to switch the SIM profile in a way that did not involve the physical swapping out SIM cards. That mechanism RSP. In addition to some non-standard and pre-standard approaches, the **GSM Association** developed a set of standards for the eSIM/RSP architecture: SGP.02 ("M2M") introduced in 2014, SGP.22 ("Consumer") in 2016, and now SGP.32 ("IoT") which was introduced in 2023 and is currently going through final process of standardisation.

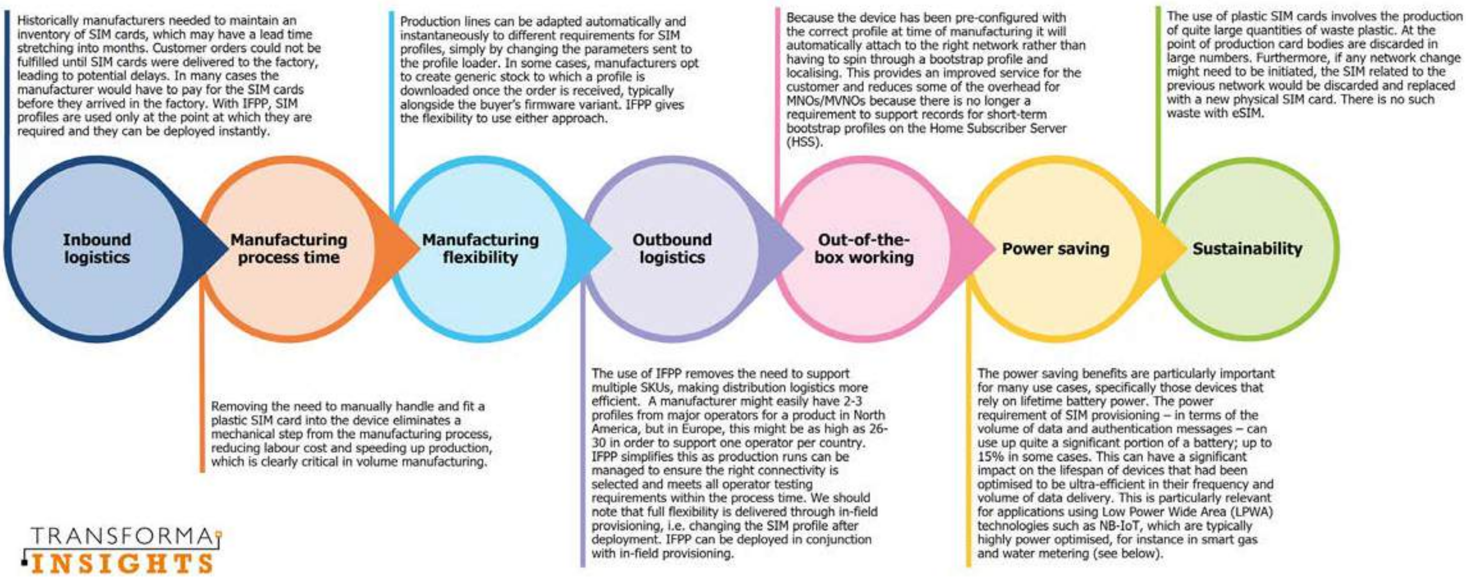
Beyond the in-field profile switching, there is another scenario in which SIM provisioning might be more effectively supported: to set the initial SIM profile(s) during the manufacturing process. This is known as IFPP. It is focused specifically on the secure loading of SIM profiles during the manufacturing and/or order fulfilment process. The profile installed on the device can be determined by the connected device manufacturer based on characteristics such as the device capabilities or the location in which it will be installed. And the GSM Association has also been active here, working on the SGP.41 specifications for an IFPP standard.

IFPP works by allowing the manufacturer to load an eSIM profile via a profile loader in the manufacturing line from a digital inventory of mobile network operator (MNO) eSIM profiles. The loader will use a set of pre-established parameters to apply the next appropriate profile. Usually, the application of the profile will happen at the same time as firmware/software loading or firmware updates during the personalisation of devices before they ship.

Why should connected device makers use IFPP?

Transforma Insights has identified seven key characteristics of IFPP from which manufacturers of connected devices, including benefits from IFPP specifically and remote SIM provisioning broadly.

1. **Inbound logistics** - Traditionally, connected device makers maintain an inventory of SIM cards, which they need to order from MNOs and the lead time for which can stretch into months. Many OEMs have found that customer orders have been delayed while waiting for the delivery of the SIM cards. With IFPP, SIM profiles are used only at the point at which they are required and they can be deployed instantly.
2. **Manufacturing process time** - The requirement to manually handle SIM cards and fit them into devices adds an additional step in the manufacturing process, increasing labour cost and slowing down production, which is clearly critical in volume manufacturing.
3. **Manufacturing flexibility** - With IFPP it becomes possible to automatically adapt production lines to make use of different SIM profiles, simply by changing the parameters sent to the profile loader. ▶



The seven benefits of In-Factory Provisioning (IFPP)

(Source: Transforma Insights, 2024)

4. **Outbound logistics** - By using IFPP the manufacturer does not need to maintain multiple stock-keeping units (SKUs) based on the SIMs installed in the device, making distribution logistics more efficient. IFPP simplifies this as production runs can be managed to ensure the right connectivity is selected and meets all operator testing requirements within the process time. Full flexibility is delivered through also using in-field provisioning, i.e. changing the SIM profile after deployment, in conjunction with IFPP.
5. **Out-of-the-box working** - With the device having been pre-configured with the correct profile at time of manufacturing it will automatically select the right network rather than having to spin through a bootstrap profile and localising. This improves the service for the customer and removes the need for short-term bootstrap profiles on the home subscriber server (HSS).
6. **Power saving** - One of the key benefits of IFPP for some applications is power saving. The power requirement of SIM provisioning – in terms of the volume of data and authentication messages – can use up quite a significant portion of a battery; up to 15% in some cases. This can have a significant impact on the lifespan of devices that had been optimised to be ultra-efficient in their frequency and volume of data delivery. This is particularly relevant for battery-powered applications using low power wide area (LPWA) technologies such as NB-IoT, which are typically highly power optimised, for instance in smart gas and water metering.
7. **Sustainability** - With the use of eSIM there is not the plastic waste associated with plastic SIM cards. At the point of production card bodies are discarded in large numbers. Furthermore, with plastic SIM cards, any network changes would require replacement and discarding of the old SIM card.

A valuable technology for volume manufacturing

The conclusion of Transforma Insights research on IFPP is that it offers volume electronics manufacturers multiple mechanisms for improving profitability and competitiveness, and making a better end product. Cost savings in production/fulfilment will have a notable impact on cost of operations, while reduced power consumption might make the difference between a product that meets deployment requirements and one that doesn't.

Volume manufacturers of cellular connected electronics devices will almost certainly benefit from the use of IFPP. The move from plastic SIM to eSIM is well under way, but there are still options for where provisioning happens, in field or in factory.

Connectivity providers need to adapt to the needs of manufacturers. The arrival of IFPP is in reaction to a real need from volume manufacturers for a more appropriate approach and they will embrace the new technology. Connectivity providers need to support the capability.

IFPP is particularly relevant for deployments that are power-constrained. Any cellular-enabled IoT device that runs on batteries will be, by definition, power-constrained and will benefit from eliminating the need for power-hungry in-field provisioning.

We should note that it's not really necessary to use a standard to benefit from IFPP. There are standards coming for IFPP in the form of SGP.41/42. However, in the same way that pre-standard versions of SGP.02 and SGP.32 have pre-empted the arrival of the standard, in the case of IFPP a non-standard approach is also valid. In fact, it is even more valid because the deployment is in a closed and highly managed environment, and manufacturers may be actively looking for their own 'special sauce' differentiator.

Connectivity providers need to adapt to the needs of manufacturers

Make eSIMs work easier and better with in factory profile provisioning

Service providers will soon be offering a streamlined way for organisations to quickly get the best out of their new IoT deployments, writes Antony Savvas

Use cases such as smart energy meters and remote logistics are "being primed for immediate adoption"

In factory profile provisioning (IFPP), according to the GSMA SGP.41/42 standard, allows the loading of device- and region-specific mobile network operator and mobile virtual network operator profiles, onto eSIMs and iSIMs during device production.

This process is designed to be secure and enables out-of-the-factory connectivity, flexible production, simplified logistics and reduced complexity in supply chains

Driving force

A recent study from **Juniper Research** found that the global number of integrated SIMs (iSIMs) installed in connected devices will rise from 800,000 in 2024 to over 10 million by 2026. It cited the GSMA's SGP.41/42 specifications, anticipated to launch by the end of next year, as a key driver for this 1,200+% growth. As a result of the increased convenience, it also predicts the number of iSIM connections will rise to 210 million by 2028 globally.

Use cases such as smart energy meters and remote logistics are "being primed for immediate adoption", says Juniper. Also, the automotive, fixed-wireless access and consumer electronics segments are among the areas to benefit too.

IFPP target industries, as cited by Giesecke+Devrient:

- **Consumer electronics:** Devices and wearables with pre-provisioned network profiles for instant cellular connectivity – no matter where
- **Transport and logistics:** Built-in and battery-operated trackers as well as IoT devices that connect immediately to monitor on the go
- **Smart metering:** Utilities meters that connect straight away, eliminating in-field set-up
- **Automotive industry:** Vehicles delivered with ready-to-go connectivity for global communication and telematics
- **Healthcare and well-being:** Medical and monitoring devices securely connecting wherever they are deployed for reliable data transmission and remote management
- **Industrial IoT:** Machinery and sensors supplied with ready-to-use connectivity for real-time reporting and control ▶

Power savings

IoT services firm **Eseye** says power is a key challenge that IFPP addresses as well. It says: “Even with the arrival of remote SIM provisioning (RSP), which oversees the secure storage, deployment and activation of multiple network operator profiles on embedded universal integrated circuit card (eUICC) SIMs, the focus has been on managing the SIM of a device after it has been deployed into the field, resulting in a not insignificant power draw. And in IoT, battery life is everything.”

While RSP in IoT enables eSIM profiles to be installed, switched and deactivated over-the-air when the device is in the field, the process can consume up to 15% of the battery’s capacity, says Eseye.

This can significantly reduce the lifespan of a low power wide area (LPWA) device that might be intended to be in-situ for up to ten years. But applying the appropriate SIM profile at the point of manufacture via IFPP, says Eseye, eliminates the need to push an update when the IoT device is activated in the field, conserving valuable battery capacity. And IFPP can still be used in conjunction with RSP, so updates can still be made after deployment.

Dynamic changes

IFPP manages and integrates eSIM profiles by way of an over-the-air profile loader in the manufacturing line. As relevant MNO or MVNO SIM profiles are loaded this way, it allows for dynamic changes to the production line, based on characteristics such as the geographic location into which the IoT device is to be deployed. Eseye says the standard is currently awaiting completion, with commercial implementations “still a few years out”. But while SGP.42 can be expected to arrive in “12-24 months”, it says, there are IFPP-enabled solutions already on the market, that will “bridge the evolution gap” and offer an “upgrade path”. Eseye and Thales are jointly working on such a solution.

Streamlined deployment

Because IFPP IoT devices are pre-configured to connect to the most relevant network on activation, there is no need for a bootstrap profile or to push an initial over-the-air (OTA) profile update via RSP.

This makes the initial deployment of an IoT device easier, and reduces the need for local MNOs and MVNOs to support bootstrap profiles on the home subscriber server (HSS), adds Eseye.

While in factory profile provisioning is certainly not here yet, in terms of widescale availability, it is certainly a technology that manufacturers, operators and IoT business users will be keeping a very keen eye on.

IFPP manages and integrates eSIM profiles by way of an over-the-air profile loader in the manufacturing line

Full IFPP benefits cited by IoT services provider Workz:

- Device manufacturers can save money by not needing to install SIM cards in devices during manufacturing
- Out-of-the-box connectivity, as IFPP offers an improved customer experience by making it easier for end users to activate their devices with pre-provisioned profiles on the device
- Provides OEMs and MNOs more flexibility in how they offer connectivity with pre-provisioned profiles, offering end-users more choices and being able to cater to different regions or usage requirements
- Fast offline process, as IFPP offers a high-speed offline process for provisioning of eUICC profiles, avoiding the slower option of online provisioning through a SM-DP+
- No certification costs compared to standard onsite SM-DP+ implementations, as providers can reduce cost and administration needs as the GSMA SAS (security accreditation scheme) certification is not required
- On-demand options, as IFPP enables last-mile offline provisioning, allowing providers to provision at a later stage in production if required
- IFPP offers late binding options that allow a profile to be linked to a specific device eID. This may be useful in cases such as enterprise deployments where profiles are required to be provisioned only on company devices
- IFPP is an alternative to purely relying on in-field provisioning, especially for applications using LPWAN technologies, including NB-IoT, which rely on devices with finite battery life

Massive IoT means new models, new technologies and new relationships

Introduction

IoT has overcome the barriers that have inhibited its growth and emerged as a hyperscale industry. It delivers on the promise of tens of billions of connected devices, supporting vast new business cases that benefit society, businesses and individuals. Innovative technologies and components drive the momentum behind this success. These can deliver secure IoT compliant with national and sector-specific regulations.

Massive IoT has not been an overnight success. It has suffered from repeatedly missed, overambitious analyst predictions for multibillions of connected devices five or even ten years ago. On the other hand, IoT has benefitted from its roots in the machine-to-machine (M2M) communications era that began more than two decades ago.

Those delays and that heritage have provided the foundation upon which massive IoT has been built. It comprises mature technologies, effective security and smooth interoperability that can be achieved at scale. M2M's long experience and additional development time caused by massive IoT's delay contributed to today's mature, mass-scale IoT solutions marketplace.

Tens of millions of modules have already been sold today. This expansive growth also increases the attack surface. Therefore, security and safety must be considered in massive IoT.

Telit Cinterion has a substantial repository of information from its 30 years of experience. The company addresses regulatory and compliance issues alongside security to enter new markets with new services. As IoT grows, these considerations become more important. Florian Denzin, the director of IoT product strategy at Telit Cinterion, says:

"IoT has evolved and become more dynamic. As deployments grow, exposure becomes greater. If you have large fleets, you have made large investments. That means you must protect assets to be productive and maintain flexibility to grab new business opportunities."

Scale impacts security and compliance

Efficiency with compliance and security has become a priority for organisations deploying IoT at a massive scale.

There are many factors to consider if you want to integrate IoT into a business, including:

- Your application's data needs
- The communication time required
- The specifics of your market
- Manufacturers' lead times and requirements
- Chipset selection

Moving IoT to the centre of your operations requires much consideration. Telit Cinterion helps its customers execute this with hardware solutions that span various modules. The company also provides global connectivity as an MVNO, covering over 200 countries. Its dedicated IoT solutions division helps with certification, electromechanical systems (EMS) and product design.

Telit Cinterion is an end-to-end solutions provider. It guides customers through the process, from selecting technology and designing the product to providing connectivity and getting certifications.

Partnering for success

Denzin points out that even massive IoT isn't necessarily an organisation's core business activity. Although IoT opens new business models and ways of competing, many businesses don't need to build massive IoT operations. Nor do they need to create teams of IoT developers to launch or support one or two connected product lines.

This is where experts like Telit Cinterion help accelerate time to market and streamline development. The company delivers cost-efficient solutions supported worldwide and backed by the company's decades of experience.

> **"You need someone close to you to do all this. We have field application engineers and salespeople in more than 100 locations. We also have more than 1,100 people and a very large engineering base. This is essential for deployments that could be in the field for a very long time."**

That model frees organisations to focus on their business and the new IoT-enabled model they are adopting. They don't need to reinvent the wheel or compete to build in-house IoT capabilities that are often only needed for a project's development and rollout phases.

For long-life deployments like smart meters, an in-house approach leaves the organisation with an expensive team of IoT experts it doesn't need once design and deployment are complete. Moreover, a single solution in one industry wouldn't justify building and retaining an IoT team. There is also concern that creating a small internal team might not result in the cross-industry IoT vision that a large vendor partner can provide.

> **"It starts with technology selection, then product design with network evolution and life cycle for the long term in mind. Technology can be activated across different features at various times. A strategy for rolling out fleets of devices must be set. It's not always a simple calculation of when to add more functionality. Issues like power consumption and battery life must be considered. Balance must be achieved to deliver performance, cost-efficiency and lifespan."**

As the hyperscale IoT era continues, the pressure will not lift. Supply chain challenges initiated during the pandemic affect component availability. This further constrains an organisation's ability to roll out fleets at a massive scale. These issues can be mitigated by careful component selection from vendors that have assured their supply chains. However, this adds a layer of complexity to the massive-scale IoT deployment challenge.

Shared risk and reward

Telit Cinterion recognises massive scale and has ensured its products are available in the customers' desired volumes. The company is also willing to share the risks of massive IoT deployment for appealing business cases with its IoT as a service approach. Denzin and his team envision models under which Telit Cinterion will supply a module and connectivity and share revenue from end-user subscriptions.

> **"There is an element of risk, but it's a no-pain-no-gain situation. We'll take some risk where we see interesting business prospects in the market that are stifled by the challenges of financing projects up front. It's a way for us to help scale the market by building a successful business model that is a win for us and our customers."**

Market Review

IoT maturity takes it past the mass-scale tipping point

2023 represented a tipping point for IoT when the sector stepped out from under the shadows of over-ambitious market size predictions and started to deliver on the promise of an IoT-enabled world. There's still a long way to go but mass-scale deployments are routinely happening and tens of billions of IoT connections are being added each year. This is being enabled by the confluence of available technology, wider choice of connectivity, especially in the cellular market, and more maturity in IoT security, certification, compliance and business models.

Mass-scale IoT has also benefitted from the flywheel effect of successful deployments fostering greater confidence in the landscape and, in turn, supporting further investment. On the flipside, the larger the deployments, the greater the investment required so work continues to optimise efficiency and reinforce the mass IoT business case. Overall though, IoT is more proven, more secure, more robust and more flexible than ever before and awareness of this is enabling organisations to commit to large-scale projects with confidence.

Although once bitten and twice shy, predictions relating to market size are returning. Analyst firm IoT Analytics has predicted the global number of IoT connections will double from 2022-2027. The firm reports that global IoT connections increased by 18% to 14.3 billion active endpoints in 2022, while for 2023, the firm predicted a further 16% growth to 16 billion active endpoints. At the end of its current prediction horizon, it estimates there will be more than 29 billion active IoT endpoints.

As always, such numbers should be taken with caution and definitions are important. Others have projected the size of the cellular IoT market alone. Omdia, for example, predicts there will be 5.4 billion cellular IoT connections by 2030. The firm sees 5G-related technologies such as 5G Red Cap and 5G Massive IoT driving much of this growth.

It is, however, clear that wider choice of technology is arriving in the cellular space. Red Cap is set to democratise access to 5G-like latency in a lower cost format, while LTE Cat 1 bis adds greater capability to LTE Cat 1, extending the applicability of LTE and opening up a range of IoT applications for the technology. The advanced cellular technologies available now widen choice and mean that organisations can select connectivity that provides a better fit than ever before for their use case.

This is an important driver for mass-market IoT because it means there is less wastage and organisations can readily make the trade-offs between cost, performance, security and power consumption for various cellular connectivity and select the option that matches their deployment best. This removes complexity from the IoT design and development phase and provides greater visibility into the whole-life costs of a deployment. This clarity aids financing and increases confidence of what return on investment looks like.

At the same time provisioning of connectivity has become radically simplified with the introduction of embedded and integrated SIM (eSIM and iSIM). These technologies allow the SIM to be embedded or integrated into the device at the point of manufacture with the connection initiated automatically at the point of deployment. This removes the need for a plastic SIM, the cost of a SIM tray and the management complexities of installing local operator

> **Mass-scale IoT has also benefitted from the flywheel effect of successful deployments fostering greater confidence in the landscape and, in turn, supporting further investment**

Market Review

SIMs at the point of deployment. This streamlining of the SIM process removes a further significant barrier to mass scale IoT.

With connectivity options at last becoming clearer and simple propositions now widely offered, organisations are now focusing on other critical capabilities. Security is an obvious concern because the more connected devices that make up a deployment, the greater the threat surface and the larger the risk. Security by design is embedding secure functions within devices before deployment and providing better security than retrofitted solutions, which are often too expensive or impractical for many IoT use cases to bear.

Security is significant not only for the obvious need to prevent hacks and frauds but also to assure connected device identity and inextricably link the data from the device that collected it and transmitted it. Confidence in IoT data that can be trusted is an essential part of the IoT value proposition and this is now well understood with effective solutions in place.

With connectivity simplified and security being continuously addressed, scalability challenges still exist. IoT organisations need to be able to access economies of scale in order to justify business cases and this means they need to accelerate and simplify certification, which is needed in national, regional and vertical markets in order for devices to be deployed. Certification and regulatory compliance still presents a significant bottleneck but organisations are increasingly relying on vendors to draw on their experience and smooth out the process.

There's a growing awareness that much of this can be replicated from one device to another and it's not necessary for every business that is engaging in IoT to become certification experts.

Similarly, organisations recognise they don't need to be device makers and are outsourcing their IoT device manufacturing to partners. This helps them to get to market fast and handle the scale of massive IoT.

This demonstrates a new willingness to collaborate within IoT. Where once organisations would focus on attempting to do everything themselves, they now realise that this is too slow, too expensive and too complicated. Instead, there is greater appetite to partner with experts from device design to deployment and beyond. By tapping into providers of IoT as-a-service, organisations can access optimised solutions for device development and certification, manufacturing, connectivity, roll-out and support and security. There is also greater willingness to share the risk and reward.

Turning to partners that can cope with mass IoT scale and bring in-depth understanding of IoT intricacies such as power consumption, cellular network variants or security, can radically accelerate time-to-market, result in significantly improved performance and deliver transformed business value. The bigger the volumes, the greater the risk but also the richer the reward is now the attitude that IoT innovators stepping into the hyperscale era of mass IoT are taking. It's an exciting landscape and the participants will get to success faster by travelling together.

Security is significant not only for the obvious need to prevent hacks and frauds but also to assure connected device identity and inextricably link the data from the device that collected it and transmitted it

Digital technologies deployed for intralogistics optimisation

The growth of the e-commerce sector has created considerable pressure for advances in logistics and supply chain processes, writes Suruchi Dhingra, a research director at Transforma Insights. Customers have come to expect ever greater speed of delivery creating a considerable incentive to accelerate fulfilment times and accurately predict delivery times. This has put a strain on existing infrastructure such as warehouses, encouraging greater efficiency in intralogistics operations which were already one of the most vital components of any company's supply chain

Intralogistics operations encompass the internal management of flows of materials, products and information within a facility. It includes all logistical operations from the receipt of raw materials to the completion of the final product and delivery into distribution networks, and encompasses multiple dimensions such as inventory management, internal transportation optimisation, workflow optimisation, order management and in-factory asset tracking and monitoring.

With rapid advances in digital technologies such as robotics, (specifically including autonomous guided vehicles and autonomous mobile robots), artificial intelligence (AI), and IoT, companies can now optimise their intralogistics processes more easily and achieve better results. The following sections focus on a range of key aspects that can be significantly improved by using digital technologies in support of intralogistics.

Warehouse management

Companies are aiming to increase the level of automation in warehouses to accommodate growing ecommerce demand and often also to mitigate challenges related to labour shortages. With automated guided vehicles (AGVs) and autonomous mobile robots (AMRs) companies can automate transportation, handling and replenishment of products and materials, and other repetitive and potentially strenuous warehouse activities.

For example, AGVs may be used to transport inventory from long term storage locations to forward-picking locations to replenish stock and ensure that adequate inventory is accessible to pickers, making the order picking process more efficient. Order picking is one of the most strenuous tasks in a warehouse and automating this process can relieve stress on workers and unlock significant improvements in worker▶

Companies are aiming to increase the level of automation in warehouses to accommodate growing ecommerce demand and often also to mitigate challenges related to labour shortages

The overall benefits of intralogistics optimisation are significant in terms of process efficiency, but securing the benefits depends on a range of sub-domains

productivity by minimising worker walking time and time spent carrying or pushing carts. For example, by deploying AMRs in its warehouse to handle workflows like order picking, US company **Ryder System** achieved a 25% increase in productivity and a 20% decrease in operational costs by reducing travel time in the warehouse. With automation, companies can achieve faster order fulfilment, improved order accuracy, and reduced picking error rates, which eventually help in increasing customer satisfaction levels and reduces costs resulting from the need to remedy any errors. Further benefits can be realised due to the reduced spacing that is needed between storage racks in warehouses that utilise AGVs; in some cases saving around 30% of floorspace.

Wearables (such as headsets, smart glasses, smart gloves, ring scanners and tablets) are often used in warehouses to optimise worker movements, enable picking and packing efficiency, and ensure worker safety. Wearables equipped with augmented reality technology can be used for navigation and guiding employees for picking and packing operations. These techniques yield benefits not only by speeding up processes and reducing errors but also by reducing employee training time.

Inventory management

Inventory management solutions that incorporate IoT and AI have considerable benefits for reducing employee workloads, freeing them up for other higher skilled tasks and reducing the errors associated with manual inventory management. Improved information about the stored quantity of goods and their flow enables the optimisation of inventories, allowing businesses to operate with a leaner inventory so reducing both the floorspace and capital dedicated to inventory, and allowing for a greater variety of goods for a given floor space. Based on our research, digitally enabled inventory management can reduce inventory levels (and associated holding cost) by 20%, on average. Efficient inventory management also impacts the value proposition of a company by increasing service levels and improving the proportion of deliveries made on time and in full.

To fully utilise the capabilities of inventory management in planning and supervising intralogistics processes, it is necessary to implement a system of IoT connected devices. Drones, beacons, shelf sensors and other IoT devices can be deployed to track inventory levels and locations in near real-time which, when combined with AI, helps in predicting inventory demand accurately, optimising inventory levels and also the management of inbound logistics. Additional benefits can clearly be secured through better integration to order management and production systems.

Transportation optimisation

Logistics planning is essential for trucks travelling between and within warehouses, retail stores, and other facilities, and that can often waste time and fuel sitting idle waiting for goods to be loaded or awaiting directions. Sometimes, these trucks also make ‘empty runs’ because of lack of visibility into the location of goods. IoT tags can be used to identify the location of trucks within facilities and by combining this data with information about the loading for each truck, significant reductions can be achieved in the amount of time wasted idling or waiting for directions, and routes can be optimised.

The benefits and risks of intralogistics optimisation

The overall benefits of intralogistics optimisation are significant in terms of process efficiency, but securing the benefits depends on a range of sub-domains as described above. These technologies enhance visibility of operations by enabling real-time monitoring at every stage of production, right from the raw material supply stage up to the final delivery of the manufactured goods stage, which in turn can enhance efficiency and reduce downtime and production cost. Intralogistics optimisation can also reduce workers’ fatigue and eventually increase their productivity and performance.

Similarly, the complexity of the technology used for intralogistics optimisation can vary significantly based on the scale of deployment and the industry in which it is applied. For example, implementing autonomous vehicles and asset tracking and monitoring can be complex, requiring significant time and effort. However, if digital technologies are integrated gradually into an existing facility, existing processes can serve as a fallback, thereby reducing risks.

This article is inspired by Transforma Insights’ report ‘Digital Transformation in the Transportation and Sector’[1] that identified seven key domains of change within the sector, that are enabled by disruptive technologies such as the Internet of Things, artificial intelligence and edge computing.

[1] https://transformainsights.com/research/reports/digital-transformation-transportation-storage


Navigate the connected world with us
Berg Insight™
info@berginsight.com | Phone +46 31 711 30 91 | www.berginsight.com

Our pick of the IoT industry's upcoming events

Innovate Americas 2024
24-25 September 2024
Dallas, Texas, USA
https://www.iot-now.com/event/innovate-americas-2024/

Data2030 Summit
24-26 September 2024
Stockholm, Sweden and online
https://www.iot-now.com/event/data2030-summit/

AI & Big Data Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/ai-big-data-expo-europe-2/

Cyber Security & Cloud Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/cyber-security-cloud-expo-europe/

Intelligent Automation Conference Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/intelligent-automation-conference-europe-2024/

Unified Communications Conference Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/unified-communications-conference-europe/

IoT Tech Expo Europe
1-2 October 2024
Amsterdam, The Netherlands
https://www.iot-now.com/event/iot-tech-expo-europe-3/

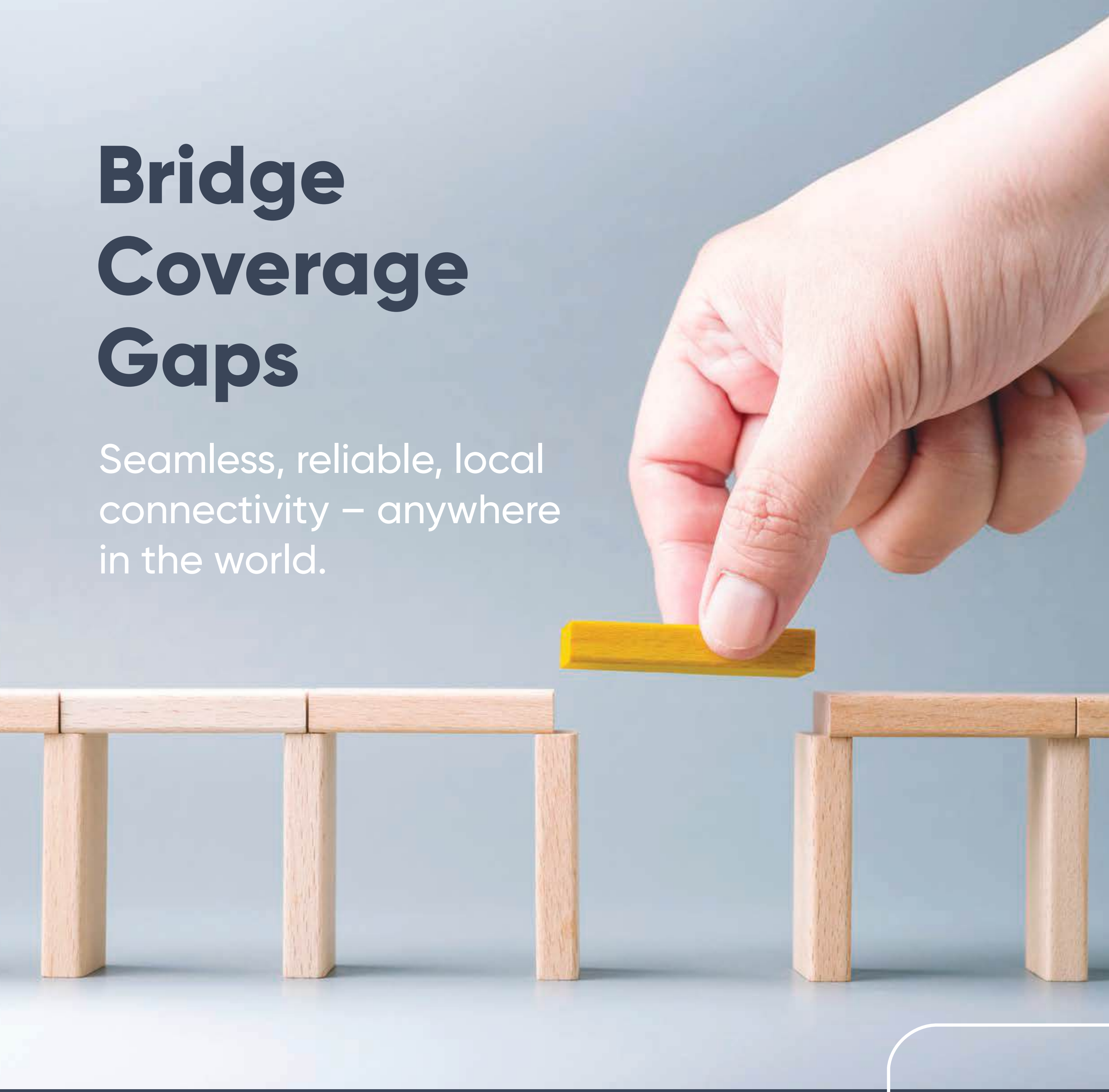
Momentum AI London 2024
2-3 October 2024
London, UK
https://www.iot-now.com/event/momentum-ai-london-2024/

Network X
8-10 October 2024
Paris, France
https://www.iot-now.com/event/network-x-2/

MWC Las Vegas
8-10 October 2024
Las Vegas, Nevada, USA
https://www.iot-now.com/event/mwc-las-vegas/

Bridge Coverage Gaps

Seamless, reliable, local connectivity – anywhere in the world.



Coverage gaps are inevitable, especially in certain environments and geographies. But with floLIVE, you can ensure you have always-on connectivity.

It's time to close the gaps.
Connect with us today

info@flolive.net | www.flolive.net

flo. LIVE