IoT Now: ISSN 2397-2793

Q4 2023 • VOLUME 13 • ISSUE 4

# IoTNOW

## HOW TO RUN AN IoT ENABLED BUSINESS

## INTERVIEW

**Thales' Eva Rudin says secure connectivity enablement guarantees IoT success at scale**

**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**
Will module makers take on integrated IoT connectivity?
Read the IoT Now report at www.iot-now.com

**TRANSPORT**
Does greater complexity demand simpler cellular connectivity?
Read the IoT Now report inside this issue

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

**PLUS:** The Definitive Guide to iSIM • Trains, planes and water meters • Kigen chief explains why trusted data is at the heart of IoT success • Berg Insight details how cellular connectivity will enhance EV charging in exclusive report • Wireless Logic on anomaly detection as an identifier of security breaches • Guy Denis reveals Bosch's top tips for achieving operational excellence in digital manufacture • Event previews • Latest News, Features and Interviews online at **www.iot-now.com**


Unlock the full potential of your business with Bosch Global Software Technologies and embark a journey of digital excellence!

Get in contact with us!
bosch-iot-suite.com
contact.BGSG@bosch.com

Bosch Global Software Technologies
alt_future
25 YEARS

# CONTENTS



## IN THIS ISSUE

# Kickstart, bootstrap – what century are we in?

In efforts to sound more exciting and dynamic, the technology industry sometimes gets its words in a muddle. Just saying the words – often a lot - doesn't make them mean something else.

**George Malim,** managing editor

We see it all the time in press releases and hear it interviews; "We're kickstarting our growth with this new product introduction", "This is really going to kickstart uptake", some companies are even funded via Kickstarter. The reality is that a kickstart is a rubbish way of starting an engine and anyone who has used a 20th century moped will know you're as likely to skin your ankle as provoke it into life using a kickstarter.

There's nothing innovative, clever or fast-paced about a kickstart in an era when you simply walk up to a vehicle and start it with the press of a button thanks to the proximity dongle in your pocket. I suppose saying "We've sat down and pressed start on our growth curve" or "We've hit the button to begin soaraway sales" loses something but at least it's a comparison from the 21st century.

There's lot about SIM technology in this issue and this always brings up an even older word – bootstrap. The meaning behind this is that you resolve a situation by using the resources at hand. In some long-forgotten 19th century gold rush I'm sure boot straps were used for everything from temporary tent repairs to strapping up broken limbs but the ideal that someone has self-funded development of a product or company with a bootstrap seems about 200 years out of date.

IoT isn't composed of teenagers riding archaic, underpowered motorcycles, nor starving prospectors who need to make a temporary catapult so let's try to use the language of the present, if not the future.

Enjoy the ~~magazine~~ content!

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

## CommScope and STMicroelectronics partner for IoT security integration

**CommScope** and **STMicroelectronics** have partnered to integrate CommScope's PKIWorks IoT security platform with ST's STM32WB microcontroller unit (MCU). This collaboration provides device manufacturers with a comprehensive answer for developing secure IoT devices that comply with the Connectivity Standards Alliance's (CSA) Matter standard.

"As a CSA promoter, ST is committed to making Matter development seamless for all device makers," said Nathalie Vallespin, the STM32 connectivity product line manager at STMicroelectronics. "Our expertise in secure elements positions us to combine our deep understanding of device-makers' challenges and strong knowledge of Matter to create unique collaborations like this one with CommScope. This will accelerate the adoption of Matter through an easy and secure process for credential provisioning."

**Bart Giordano**
CommScope

Bart Giordano, the president for networking, intelligent cellular and security solutions at CommScope, added: "By integrating the CommScope Sentry PKIWorks platform with ST's popular MCU platform, we're offering our customers a turnkey solution to alleviate the challenges of Matter adoption, while handling the complexity, scale and cost. CommScope and ST have a long-standing collaborative relationship, making it easy to meet growing demand for new Matter IoT devices with the expertise of two industry leaders with decades of experience at the forefront of digital security, semiconductor solutions and device manufacturing."

## Turkish delight for floLIVE, Kigen and Protahub as local IoT connectivity launches

**floLIVE**, **Kigen** and **Protahub** have concluded procedures so they can offer localised connectivity services in Turkey. floLIVE is now offering local cellular IoT connectivity in Turkey to its global customers through a single global stock keeping unit (SKU) number. With its partner Kigen, floLIVE has spent many months building the ecosystem and integrating the necessary systems and platforms to serve its global customers in Turkey. The companies teamed up with Protahub to create a complete, end-to-end solution that will allow OEMs, global enterprises and mobile operators alike to obtain local IoT connectivity in Turkey via their existing embedded universal integrated circuit card (eUICC)-compatible SIMs.

The collaboration has been a complex endeavour because Turkey has unique requirements for local cellular connectivity, where permanent roaming is impossible and IP data must be routed locally, in-country. "Traditionally, anyone who needed connectivity in Turkey had to approach the MNOs in-region directly and purchase SIM cards to install in their devices," explained Nir Shalom, the chief executive of floLIVE. "They needed to engage in a separate contract with the local MNO, use separate application programme interfaces (APIs) for integration, and at the end of the day they ended up with very limited management and control."

The process flow in Turkey is unique and involves floLIVE providing customers with a standard eUICC SIM which, when it arrives in Turkey, is detected via floLIVE's connectivity management platform (CMP) which identifies its location and initiates a local profile download using Kigen's remote SIM provisioning (RSP) platform. A subscription manager secure routing (SM-SR) swap then takes place between Kigen's SM-SR and Protahub's SM-SR. Finally, Protahub initiates a profile download to the eSIM and validates both Kigen's RSP and floLIVE's CMP.

**Nir Shalom**
floLIVE

**Vincent Korstanje**
Kigen

"floLIVE and Kigen are working closely together on numerous initiatives and projects, and are looking to replicate this success in other regions so that global deployments are achievable with a single SKU and a unified experience," added Vincent Korstanje, the chief executive of Kigen. "With an eSIM, you have a strong foundation for trusted devices across multiple geographies, while complying with the local regulations."

## News in Brief

### GreaseBoss helps eradicate industrial downtime

Australian company **GreaseBoss** has launched a flow meter designed to ensure appropriate machinery and equipment maintenance in manufacturing, mining and utility applications. The GreaseBoss Endpoint sensor is placed in line with grease points on machinery to monitor the flow of industrial lubricant. This helps companies remotely monitor their equipment, ensuring grease is being applied evenly and identifying any auto-lubricator reservoirs that require refilling.

The GreaseBoss Endpoint integrates Nordic Semiconductor's nRF52833 system on chip (SoC) for data collection and sensor interface management, before relaying key metrics to a GreaseBoss gateway using its Bluetooth Low Energy (BLE) connectivity. "The GreaseBoss system focuses on empowering small teams to remotely manage the greasing of massive fleets of machinery amongst other duties in their daily workflow," said Peter Condoleon, the CTO and co-founder of GreaseBoss.

The large number of sensors required, and their often hazardous or hard-to-reach placement, means that achieving a long battery life is essential for this application. The GreaseBoss Endpoint achieves this, partly thanks to the energy-efficient nature of the nRF52833 SoC and the performance monitoring capabilities of Memfault. GreaseBoss also used the Nordic Power Profiler Kit II (PPK2) to run various power consumption scenarios to ensure that the devices can continuously function for several years.

# News in Brief

## Scenera to acquire Seoul-Based TnM AI

**Scenera** has announced that it has entered into an agreement to acquire **TnM AI**, a South Korean artificial Intelligence of Things (AIoT) company, for an undisclosed amount. Stemming from the long-time collaboration between the two companies, the deal consolidates the companies' resources.

"With the combination of our strong development teams and global deployment, we are mutually committed to providing optimal solutions that address the growing problem of how to best allocate AI analytics in edge-to-cloud computing," said David Lee, the CEO of Scenera. "Together, we can create and deliver unparalleled value and optimal solutions for our customers and partners."

## LPWAN will reach 5.3bn connections in 2030, says ABI Research

**ABI Research** has predicted that low-power wide area networks (LPWAN) will reach 5.3 billion connections in 2030. LPWAN companies are competing in integral IoT applications such as smart metering, asset tracking, and condition-based monitoring, with a vendor's competitive advantage often hinging on factors beyond a network's technical capabilities.

"The business environment surrounding a networking technology can be as influential to its success as its data rate, bandwidth and power requirements," said Lizzie Stokes, an IoT hardware and devices and IoT networks and services analyst at ABI Research. "As new connectivity technologies enter the market and others pivot or leave entirely, it is important to understand how various market dynamics such as regional availability and stages of development impact a technology's successes and failures."

## Kinéis uses satellite-based IoT connectivity for early forest fire detection

**Kinéis** has announced that its spatial connectivity is helping to revolutionise forest fire prevention using early detection. **NewSpace** technologies and satellite-based Internet of Things (IoT) capabilities are contributing to better prevention in detecting forest fires and reducing their impact on the environment. Kinéis global connectivity enables it to track and monitor objects in remote areas without coverage by terrestrial networks. In addition, frequencies used in the 400 MHz bandwidth have signal penetration in the canopy-covered environment.

The company used its expertise in the ARGOS system, founded by CNES (the French Space Agency) and historically operated by Collecte Localisation Satellites (CLS) to develop a reliable technology for providing easy access to useful satellite data. It locates and connects objects wherever they are on the planet, simplifying and multiplying their use by professionals and private individuals alike.

Using its constellation of 25 nanosatellites and 19 ground remote stations, Kinéis locates and connects objects through terminals, wherever they may be on the planet. Combining NewSpace's technological innovation with IoT ensures narrowband, low consumption, and simple global connectivity. With their very low power consumption, the terminals can be autonomous for several years, sending messages only when necessary.

**Forest fire control depends on early detection**

## Softbank targets two million with 1NCE flat rate IoT connectivity

**SoftBank** has announced an expansion of its global Internet of Things (IoT) business in the Asia Pacific (APAC) region, spanning 19 countries and regions, including Japan. SoftBank's primary emphasis in this initiative will be directed towards marketing IoT services, with a key focus on promoting the **1NCE** IoT Flat Rate connectivity offering. SoftBank aims to acquire a total of two million 1NCE IoT Flat Rate connections in APAC and other regions within its 2025 fiscal year.

SoftBank took an equity stake in 1NCE in April 2022 and agreed to exclusively market 1NCE IoT Flat Rate in 19 APAC markets. 1NCE IoT Flat Rate is available and at no additional cost, customers can also roam on 1NCE's global network of more than 160 countries and regions.

SoftBank's global expansion efforts will begin with a focus on its IoT business, primarily within the APAC region. "We're extremely pleased to be able to fully expand our IoT business in the APAC region," said Daichi Nozaki, senior vice president of SoftBank. "While we've been providing IoT services primarily in Japan and contributing to the digital experience (DX) of various industries there, we'll collaborate with strong business partners like 1NCE and use our expertise gained in Japan to fully establish ourselves in APAC. Doing this, we'll work to contribute to the digitalisation of the entire region and solve social issues."

## Drifter World and Tele2 IoT simplify the race for a parking space

**Tele2 IoT** and **Drifter World**, a company that uses AI to optimise the use of parking spaces and electric vehicle charging stations, are collaborating to connect drivers with spaces and charging points. Tele2 is providing a cellular IoT connectivity solution that maximises uptime and gives the company full control over its fleet of devices. Drifter's system enables the entire parking flow to be automated and the need for parking attendants, parking discs and payment machines disappears completely. When a vehicle arrives, the system automatically detects it using smart cameras and initiates a paid session, which ends when the vehicle leaves. Sensors seamlessly capture real-time data on occupancy and traffic flows, making parking not only efficient but also intelligent.

Together with Drifter, Tele2 IoT ensures that functionality and maximum uptime of the devices are achieved. While enabling the business to have full control over its fleet of devices, where they can understand how each device communicates and what its status is. At the same time, the connection can be restarted remotely, so that it does not have to be handled on site.

Collected data on driving and parking patterns can be shared with cities to better understand traffic flows. It can also help parking companies to optimise the use of parking lots.

"It's purposeful and fun to work on this venture together with Drifter World," said Cyril Deschanel, the managing director of Tele2 IoT. "With this solution, you can reduce driving time in cities and get smarter traffic flows. We are happy to be part of that development." said Cyril Deschanel, the managing director at Tele2 IoT.

Fredrik Durling, the chief executive and founder of Drifter World, added: "Tele2 IoT's solutions give us fantastic coverage, reach and speed. They help us enable smarter urban experiences, improve traffic and create a more efficient and sustainable urban ecosystem."

**Cyril Deschanel**, Tele2 IoT

## WaterSignal enhances water monitoring with Telit Cinterion's IoT solutions

**Telit Cinterion** is working with **WaterSignal** to ensure always-on connectivity for real-time water monitoring and leak detection systems. As water scarcity continues to increase worldwide, baseline water benchmarking and evaluation have become critical, requiring operation teams for domestic meters, irrigation systems and cooling towers to have reliable access to on-demand data. Through WaterSignal's remote water monitoring capabilities, supported by cellular low power wide area (LPWA) modules and IoT connectivity, teams gain deeper insights into their towers and system efficiency. This helps eliminate the need to perform repetitive, manual day-to-day meter readings.

Telit Cinterion's cellular LPWA modules support various devices, from point-of-sale terminals and smart meters to industrial sensors and asset management. Its modules include power saving mode (PSM) and extended discontinuous reception (eDRX) capabilities which can help to improve IoT application power saving and battery life.

"Telit Cinterion is a leading IoT provider and was selected because of its excellent reputation for quality modules, which later expanded to its IoT connectivity network services," said Mike Drake, the vice president of engineering at WaterSignal. "WaterSignal can ensure connectivity for customers via cellular data rather than Wi-Fi. It does not require a connection to power. This capability provides a more stable connection. It allows the WaterSignal device to communicate, even in deep vaults or locations far away from buildings with Wi-Fi."

Neset Yalcinkaya, the senior vice president of sales for Americas at Telit Cinterion, added: "When monitoring critical resources, like water, a reliable connection is pivotal to maintaining visibility and extracting actionable insights. WaterSignal's technology is invaluable for operation teams, and we are pleased that Telit Cinterion's cellular LPWA modules and IoT connectivity solutions are central to providing that essential connection, particularly the ability to use cellular instead of Wi-Fi to transfer water data independently of a power source during an outage."

## News in Brief

### AdriNet partners with Actility

**AdriNet** has announced a new partnership with **Actility** to enhance the deployment of IoT across the Adriatic region using Actility's network platform. Founded in 2015, AdriNet specialises in distributing wireless communication solutions to several countries, including Albania, Bosnia and Herzegovina, Montenegro, Croatia, Kosovo, Romania, Northern Macedonia, Slovenia and Serbia.

The company focuses on various sectors such as smart metering, smart cities, smart industry, smart energy and utilities, smart transport and logistics, and smart buildings. It also delivers communication solutions sourced from various manufacturers specialising in network solutions, antennas, RF equipment and related products. Actility's ThingPark LoRaWAN IoT connectivity management platform enables the management of LoRaWAN devices, subscribers and gateways. It facilitates smooth monitoring of network operations and data flow control, thereby expediting the implementation of large-scale IoT projects.

**Remi de Fouchier**
Thales' Digital Identity and Security Business



# IoT demands greater simplification, more orchestration and the right level of security for each use case

Robin Duke-Woolley, the chief executive of Beecham Research, recently had a video interview with Remi de Fouchier, the vice president of strategy, marketing and innovation at Thales' Digital Identity and Security Business, which can be viewed here. In the interview, de Fouchier shared his response to the latest trends in IoT and highlighted how Thales can help organisations maximise their opportunities and address the challenges the market faces

**Robin Duke-Woolley: There have been many projections about how the IoT market is growing. These include Ericsson's projection of over five billion cellular IoT connections by 2028 and Omdia's report that 83% of enterprises are deploying multiple IoT projects. Both of these point towards much larger and more varied IoT deployments over the next few years. Given this growth and context, what does Thales see as key trends that need greater support over the next few years?**

**Remi de Fouchier:** Firstly, we share your enthusiasm and analyst view of the developing market. This is our view as well – this is a promising market. But more importantly than the volumes, what we think is that this is an addition of many different segments, verticals and use cases and that they will have specific requirements in terms of energy consumption, security, interoperability and scalability. Some of these key urgent items are already addressed by standardisation.

One of the important market evolutions that we see is that traditional OEMs are shifting from selling just a device to more of a service model and they want to enrich their hardware business with digital services. We can think of predictive maintenance, consumption, monitoring or data analysis and of course they also want to reduce as much as possible their carbon footprint, which is also a very strong objective for Thales. ▶

**SPONSORED INTERVIEW**

Last but not least, by increasing the number of connected devices and the data they generate, the attack surface increases and security increases as well for security sensitive or privacy sensitive material. This is an important element that must be taken into account from the design of the device to the overall lifecycle of the data generation produced. We sometimes hear that security is considered to be expensive. Instead, it should be seen as an insurance that is protecting brands from potential heavy reputational and legal damages.

**RD-W: What would you see as the key challenges for enterprises when deploying IoT services?**

**RdF:** We have the privilege of already collaborating with hundreds of OEMs and IoT service providers and we can group these challenges into three categories that we summarise around:

Build, Run, Protect

Build covers design. Run means production, deployment and maintenance. Protect encompasses continuous virtuous cybersecurity. And without a proper approach, each of those different steps presents challenges.

For Build, OEMs and IoT service providers need to stay in the driving seat in terms of connectivity choices and number of stock-keeping units (SKUs) – a horrible name for the number of variants of devices.

For Run, OEMs have complex logistics to serve different geographies, different markets during installation, during deployment, with onsite labour and with truck rolls for initial setup or to fix issues during the device lifecycle. In terms of deployment and coverage, cellular connectivity has many real benefits. That also explains the enthusiasm for this technology and the growth of the market.

For Protect, there is the cyber protection journey of connected devices from the production line to long lasting operations. It is not protect once, it is protect all along the full lifecycle of the device.

**RD-W: What is your approach to address these challenges?**

**RdF:** We want to be absolutely solid in our product and service range to answer these challenges. First, on Build when designing your devices, we are proposing a range of industry grade, standardised future-proof hardware to securely connect these devices. It starts with MIM, which is a ruggedised SIM, and it evolves towards embedded and integrated SIM (eSIM and iSIM) which allow more flexibility to manage connectivity in the field.

For Run, our connectivity suite enables a secure, resilient and cost-effective connectivity from production through operations and this is what matters. With our solutions we want to help OEMs and IoT service providers to manage the initial connectivity with a fully automated, out-of-the-box experience and then all across the device or service lifetime. To do this, we need to take account of certain situations where you will need to adapt your connectivity plan for best coverage, for best clarity, for flexibility and for sustainability. Lastly on Protect, we have our cyber protection suite to protect IoT device identity and data generated from the factory to the field and from the edge to the cloud.

**RD-W: From a Thales perspective, what are the opportunities arising in the new IoT specifications?**

**RdF:** First let me start by saying that we have a clear view of the current pain points and unmet needs when deploying IoT projects which is due to our long experience working with customers from these issues and also being involved in the cellular and telecoms industry for a number of decades. Today IoT players that we meet, including IoT service providers, are keen to get simpler and more fluid solutions while protecting their devices and the data they generate and exchange through the lifetime of these devices.

The market requires more simplification, more orchestration and the right level of security for their needs. Thales is leading the progressive convergence towards what we call the consumer infrastructure approach, and it will make the ecosystem more fluid and simpler with pre-certified, pre-integrated components as well as reference designs. Our solutions can be plugged into the existing manufacturing process to provision the connectivity and security keys directly on the production line. Finally, the rule of the game will be to reach the best compromise between the optimised total cost of ownership (TCO) security and application of cyber protection to the requirements of each market segment.

**RD-W: How do you intend to position Thales in the IoT ecosystem? In other words, is there anything new that Thales is bringing?**

**RdF:** Firstly, we have a long history with our customers, notably in the telecoms industry where we have 450 MNOs as our customers around the world. We are present in more than 68 countries, and we have hundreds of OEMs as customers who are already well equipped with our products. Secondly, the cybersecurity expertise that we have, that we've been building, is very strong. We are suppliers to the Top 5 public cloud service providers, and you've probably heard that we've recently announced the acquisition of **Imperva** in the US and this will position us in terms of cybersecurity as a Tier 1 supplier of security and cybersecurity globally. Regarding 5G expertise as well, we have been leading the effort there. In a nutshell, we are simply your partner of choice to simplify your IoT deployments allowing you to remain in the driving seat at each step of your project and ensuring your devices are well-connected and well-protected.

***The market requires more simplification, more orchestration and the right level of security for their needs***

**www.thalesgroup.com**

# Success at scale in IoT relies on optimised connectivity, security, lifecycle and compliance

Following on from the interview with Remi de Fouchier, featured on pages 8-9 of this issue of IoT Now, Robin Duke-Woolley, the chief executive of Beecham Research, also interviewed Eva Rudin, the vice president of Mobile Connectivity Solutions at Thales' Digital Identity and Security Business, to find out more about Thales' plans for the IoT market

**Robin Duke-Woolley**
Beecham Research

**Robin Duke-Woolley: With the rapid growth in prospect for IoT and the increasing interest among traditional OEMs to move towards a service model, what sort of feedback are you seeing from the market on the challenges OEMs and IoT service providers are facing in implementing large IoT deployments?**

**Eva Rudin:** Firstly, let me clarify that when we talk about IoT, this covers many different sectors and applications as well as the connectivity itself. Thales positions itself in cellular connectivity, so this is the focus for this discussion.

With OEMs shifting from selling just devices to more of a service model, many see value in cellular connectivity but also may lack experience and expertise in cellular connectivity, especially if it's a new area of focus for the company. Understanding the cellular technology, the network options and best practices can be a significant hurdle and Thales is here to support them.

It's the same with security for IoT. Understanding the issues in security for IoT is challenging, yet it is also becoming much more important to get right. As IoT continues to become more central to business and service operations, the potential reputational damage to a brand in the market due to a security breach is escalating quickly, as are the potential legal and liability costs and the cost of downtime in operations. The costs could be huge and security for IoT is really an insurance against this risk.

Cellular can be complex to integrate into IoT hardware. That includes integrating cellular modules, antennas and power management systems into the devices.

IoT devices may also be deployed in challenging environments, such as extreme temperatures or harsh conditions. Ensuring device durability and reliability in these environments is a concern and these need specific hardware and software. Regarding scalability too, as the number of IoT devices grows, ensuring that the IoT solution being used can scale to accommodate all of them is essential.

Then there is connectivity management. This is all about ensuring the best connectivity – in terms of coverage, price and usage – depending on where any particular device is deployed.

Cellular can be complex to deploy as well, with multiple stock keeping units (SKUs) for multiple connectivity providers. IoT service providers today are looking for agile solutions, in terms of choice of connectivity, time to market and breadth of use cases. For example, low power options are now available with specific constraints.

Then there are security and privacy issues. IoT devices can be vulnerable to cybersecurity threats. Ensuring security of data and devices is a critical concern. IoT security threats are rapidly evolving, yet security can be complex and costly to implement and deploy. Having access to skilled security resources is difficult and diverts attention from the core business.

**RD-W: Can you describe the key industry requirements as Thales sees them?**

**ER:** Let's think about ten key considerations. These vary in importance depending on the use case.

First and foremost, **security** always tops the list of priorities in industry surveys. This is the ability of a solution to ensure secure communications and data transfer with the device while also protecting it against cyber-attacks. Not only does this relate to the reputational risk and potential legal risk that ▶

I mentioned just now. This is also of fundamental importance because security engenders trust. Trust in the connection and trust in the data transferred – that the data has not been corrupted in any way. Just a reminder that data collection and analysis is the basis of IoT for making decisions and actions. Without trust, there is no prospect of remote monitoring or control and the IoT cannot function.

**Cost** is also always a key requirement. The annual total cost of ownership (TCO) may need to be as low as less than US$10 in verticals such as smart metering that have very low data rates, while in others such as cellular routers it may need to be considerably higher to cater for very high data rates.

Related to TCO is **ease of installation**. Installation and maintenance/repair/operations (MRO) costs can amount to 10-20% of annual TCO so can be a key consideration.

Also related to cost is **bandwidth**. This is the ability of the solution to satisfy all bandwidth needs, including data intensive applications such as high-resolution video.

**Quality of coverage** is always important. This is the ability of the solution to provide consistent connection and fluid handover between connectivity providers within its coverage. For example, for a well-functioning supply chain across multiple levels and geographies, data must be collected, integrated and analysed to provide a single view of the supply chain at any time or location. This requires very high quality of coverage of the IoT solution end-to-end.

**Device lifetime** is often critical, especially when it is embedded in larger and more complex systems where MRO activities could be complex. Closely related to this is the power requirement, particularly where the device is reliant on batteries that must last for up to ten years in some cases. ▶

**Eva Rudin**
Thales' Digital Identity and Security Business

***For smart metering, the most important requirements tend to be: security; cost; quality of coverage; device lifetime and of course regulatory compliance***

Related to device lifetime is the **contractual model**. Contract duration can be an important consideration depending on user sensitivity to the need for flexibility and fear of stickiness to one MNO. For long life devices, such as smart meters, there may be a need to consider changing the MNO during the lifetime of the device in the field.

**Environmental resilience** is critical in many applications. This is the ability to operate in harsh environments, such as with vibrations, severe temperature variations and in locations with high levels of dust. For example, physical SIM cards and connectors must be reinforced to withstand harsh transport conditions that can induce movement and friction, causing long-term damage to connectors.

**Interoperability** is adaptability to interact with a wide range of types of connectivity provider, platform provider or application technology.

Finally, **regulatory compliance** is the ability to comply with use case specific and local regulatory constraints, such as temperature monitoring regulations. Safety and security are also often of concern, particularly in healthcare and also critical infrastructure monitoring.

**RD-W: You say these vary in importance depending on the use case. Can you give examples of this?**

**ER:** Let's consider four very different use case examples – smart metering, connected health, security – as in physical alarms and surveillance – and then track and trace.

For smart metering, the most important requirements tend to be: security; cost; quality of coverage; device lifetime and of course regulatory compliance. This use case is particularly demanding, with applications that have the highest importance requirements.

On the other hand, for connected health, the most important tend to be: security; quality of coverage and, again, regulatory compliance. Security in this case is heavily weighted towards safety and risk to life. Regulatory compliance is heavily weighted towards data protection.

Then for security, the most important tend to be: security; bandwidth and quality of coverage. Without bandwidth and quality of coverage, surveillance for example cannot operate and is particularly weighted towards safety.

While for track and trace, the most important tend to be: ease of installation; environmental resilience; interoperability and regulatory compliance. This gives an idea of how requirements vary between use cases. It means that different support strategies are needed for each of these cases.

**RD-W: Taking smart metering as an example, how does Thales utilise its Build, Run, Protect approach for this?**

**ER:** We can take smart metering as an example, but just to point out that Thales addresses other key segments such as the ones already mentioned – connected health, security and track and trace – as well as automotive and many more.

To define and deploy an IoT connected device there are different stages. Thales provides solutions at each of these stages and helps the OEM to select the best technical solution to meet the specific objectives and use cases for its IoT devices.

Thales identifies three main steps during the life of an IoT device: Build, Run and a transversal one we call Protect:

**Build** covers the device design and engineering.

**Run** encompass the device production and the deployment in the field from first activation through to decommission.

**Protect** for cyber protection is transversal across the full device and application lifecycle.

The Thales product and solution portfolio has been designed to help IoT stakeholders in their challenges across each of these three steps. Let's illustrate this with a specific industry/field of applications – smart metering.

Smart metering, or more globally smart utilities, covers energy with electricity and gas, and water. This is a highly important area right now due to the increasing need to manage scarce resources and respond to climate change issues. These have raised the need for real time monitoring and analysis of consumption and leakages.

With this in mind there are several challenges where Thales solutions can help lifecycle management of the device:

- **Design:** simplification of the device 'build' with a soldered eSIM – avoiding complex sourcing
- **Production:** a single stock-keeping unit (SKU) ready to be deployed all over the world versus many regional SKUs, complicating logistics and manufacturing processes ▶

- **Installation:** Out-of-the-box first installation, with automatic connection to the best network versus trying multiple SIMs from different MNOs

- **Operation:** many events can impact the connectivity in the field (network quality) with consequences for disruption of the data flow. Five, ten or 15 years is a long period of time and there may be a need to adapt the connectivity plan for business reasons. To avoid a costly truck roll, being able to remotely change temporarily or permanently the connectivity provider.

Across all these steps cyber protection is of the utmost importance: avoid data hacking and device identity theft; protect and guarantee service delivery and continuity.

Thales focuses mainly on data and device identity protection. We do this through a process of: Generate, Manage and Revoke smart meter credentials, and by storing secret keys and certificates to protect data exchanged from edge to cloud.

With the high importance industry requirements for smart metering noted earlier in mind, Thales products and services that support these are as follows:

For **Regulatory compliance**, we have embedded and integrated SIM (eSIM/iSIM) plus Thales Adaptive Connect (TAC) for connectivity and the need to be able to change provider. We also have IoT SAFE - the SIM Applet For Secure End-to-End Communication – plus Trusted Key Manager (TKM) for security, to align with sector regulations.

For **Cost**, we have iSIM plus TAC as suitable for narrowband IoT (NB-IoT) deployments both from technical and cost perspectives. This is increasingly important for smart water meters that are ramping up quickly using NB-IoT.

For **Security**, again we have IoT SAFE plus TKM to facilitate deployment and life cycle management of credentials, which is key. As threats are evolving, so are security protection solutions.

For **Quality of coverage**, TAC enables the ability to monitor coverage issues and to change the connectivity provider on a per device basis.

Then for **Device lifetime**, eSIM/iSIM have a very long lifespan that matches the requirements of utilities companies. Thales lifecycle management capabilities complement this to adapt fleets of devices to changing conditions over their lifetime of up to 20 years.

**RD-W: Are there case studies to illustrate these?**

**ER:** Yes, we have three case studies to share, (see page 14) covering:
- the connection of aircraft in airports for downloading safety-relate and maintenance data.
- monitoring the location and condition of containers as they are shipped in any country.
- the deployment of smart water meters in multiple countries that are in place for more than 15 years.

These illustrate that each individual case has its own requirements. The challenge that Thales is addressing is how to cater for all of these individual requirements in a straightforward, flexible and cost-effective way. ■

***Thales focuses mainly on data and device identity protection***

**www.thalesgroup.com**

IoT now supports mission critical use cases that ensure user safety, minimised environmental impact and efficient, profitable operations. The following case studies illustrate how Thales is helping customers in multiple industries across the globe

# Transportation - aircraft maintenance

### Context

Safety of an aircraft is always the highest priority for an airline or operator. Monitoring of the aircraft safety data – including data for preventive maintenance – can be a tedious, costly and labour-intensive process, which needs constant monitoring, analysis and expertise.

A manual download option is available. To do this, dedicated personnel must regularly go to the aircraft to manually remove the recording media or access the data ports. If connecting to a port, a cable is attached to download the required data and then brought to a specific computer to transfer the data in the files for further data analysis.

As an alternative, a wireless option is very simple, secure and useful for transferring the data to the servers within minutes after landing the aircraft. Wireless delivery enables automated data transfer to and from the aircraft through existing cellular or Wi-Fi networks.

# Tracking and tracing - containers

### Context

To export goods, shipping containers travel extensively and pass through the responsibility of many different partners. Tracking them is therefore essential to ensure successful delivery to the required destination. At the same time, companies are often charged for demurrage and detention costs if their container stays too long in a port, or an empty container return has been unexpectedly delayed.

In addition to this, the condition of the container also requires monitoring. Typically, this includes whether it has been opened or not. In addition, refrigerated units with perishable content need close monitoring and a recorded audit trail to ensure temperatures have not exceeded required limits.

This tracking and tracing activity is needed however long a container remains in any particular country.

# Utilities - smart water

### Context

With the increasing need to conserve water and with the effects of climate change, there is an increasing need for smart water meter deployments for water utilities. These have a long life of more than 15 years in the field with no external power and, for a particular utility, may be deployed in multiple countries.

The cellular technology used for the connectivity is low data rate and low power NB-IoT. This must operate effectively for a minimum period of ten years on a single battery charge.

**SPONSORED CASE STUDIES**

### Problem
As aircraft land in many different locations and countries, it is essential that the cellular solution can utilise the most appropriate local cellular network wherever it lands. A large amount of aircraft safety data is transferred at each landing, so it would not be cost effective for the data connection to be subject to a roaming tariff structure and being locked in to one particular network operator worldwide. Instead, when the aircraft lands, it should automatically connect to the most appropriate local cellular network so the safety data can be sent as soon as possible.

### Solution with Thales Adaptive Connect (TAC)
The TAC smart agent running in the embedded SIM (eSIM) of the cellular device in the aircraft will detect if it needs a new network profile to connect to the local network. If so, it connects to a remote server to provision an activation code and relevant details of the MNO that will supply the profile required. It then pulls the required profile from the MNO's server and activates it without manual intervention. This establishes the correct cellular connection to the local network and onwards to the flight safety server to set up the data link for automatic transfer of the aircraft safety data.

This solution significantly reduces the time to connect to the flight safety server and ensures the fastest download of this important data.

### Problem
On land, wireless coverage is required at all times. As containers move, this coverage varies and a solution is required to cater for that. In addition, permanent roaming is becoming an increasingly important issue. This refers to a device that stays out of its home network for a longer time, typically over 3-4 months. In some countries, permanent roaming is prohibited, while others effectively ban it by requiring the connectivity to be provided by a locally registered network operator. The rules about permanent roaming vary dramatically between countries and are continually evolving.

### Solution with Thales Adaptive Connect (TAC)
The TAC smart agent running in the eSIM of the cellular device in the container will detect if it needs a new network profile to connect to the local network. If so, it connects to a remote server to provision an activation code and relevant details of the local MNO that will supply the profile required. It then pulls the required profile from the MNO's server and activates it without manual intervention.

TAC also provides for automatic fallback to a previous profile or to the bootstrap profile in case of coverage issues. The bootstrap profile can be used to initiate the download of a new network profile if that is needed. In this way, TAC works to ensure optimum coverage at all times.

### Problem
There is a gap between the normal contract period for cellular connectivity and the field life of a smart meter. As a result, there may be a need to change network profiles in the field. On the other hand, downloading the first profile remotely uses battery power that many utilities would like to avoid.

### Solution with Thales Adaptive Connect (TAC)
To avoid downloading the first profile remotely, TAC allows for provisioning it in the device at the factory – termed In Factory Profile Provisioning (IFPP). This enables the manufacture of a single SKU which can then be personalised at the very last stage with the initial network operator profile that is the right one for the site where the meter will be deployed. When installed, the smart meters are activated and use the network profile already installed. If a subsequent change of profile is required as a result of a new connectivity contract negotiation, this can be managed remotely through TAC.

**www.thalesgroup.com**

**Improving the success rate of IoT projects is crucial to business operations.**

beecham research

Shaping the IoT future

In 2020 our first report in the series '**Why IoT Projects Fail**' identified that, at that time, only 12% of IoT projects were viewed as fully successful.

Since then, we have published a series of 10, 100+ page reports, bringing fresh insights to the market on a wide range of IoT related topics in collaboration with many IoT partners.


Succeed with IoT Report Series

**A few of our recent sponsors who have shared their experiences and insights...**

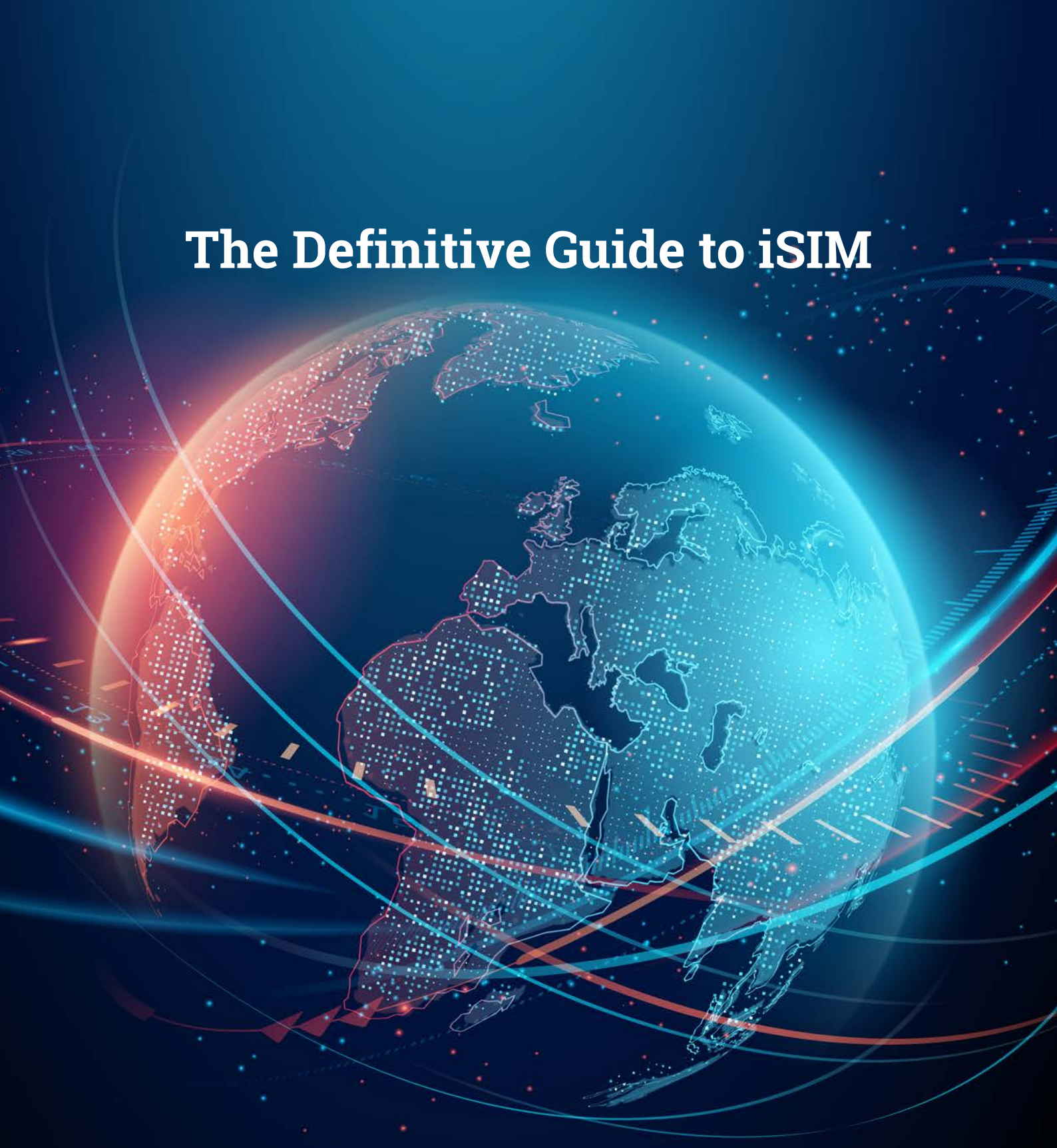
Airgain · AVSYSTEM · DIGI · ERICSSON · EUROTECH Imagine. Build. Succeed.

everynet · Giesecke+Devrient · Kigen · KORE · MULTITECH

SIERRA WIRELESS · SEMTECH · software AG · Telit Cinterion · THALES Building a future we can all trust


For upcoming sponsor opportunities please contact: hello@beechamresearch.com

# The Definitive Guide to iSIM



beecham research

Report sponsor:

Giesecke+Devrient

# IoT moves to large deployments

The IoT market is set for continued robust growth up to 2030, writes Robin Duke-Woolley, the chief executive of Beecham Research. According to Statista, almost 30 billion IoT devices are expected to be connected by 2030, up from nearly ten billion in 2020 – a CAGR of nearly 12% over the decade. This includes both long range and short range devices. According to Ericsson's mobility report of June 2023, cellular represents around 20% of this, growing slightly faster at over 12% per annum

Not only that – the size of individual IoT deployments is growing much faster. Recent research indicates the growing expectation among IoT users of individual deployments growing rapidly over the next few years. An example of this is a recent survey of IoT users by Beecham Research, some of the findings of which are illustrated in **Figure 1**.

As Figure 1 shows, more than a quarter (26%) of respondents already had deployments of over 10,000 connected devices, and a majority (52%) with deployments of more than 500 connected devices. In addition, there is an expectation of high growth of existing deployments in the near future, with as many as 22% of respondents expecting over 40% growth in the next 24 months. This is not an unusual finding – it confirms that substantial growth of individual deployments already in the field is under way.

Within that, the largest proportion of these IoT connections are expected to be low-cost devices that are small in size, have limited processing power and storage, are battery driven and may be expected to run for ten or more years. These resource-constrained devices must remain connected to deliver sensor data and act upon commands from remote locations, and they must do this securely. Secure identities are required to identify these devices and their data, as well as protect them from misuse by remote attacks. The sort of use cases this covers are sensors, trackers, wearables – including health related – and other low-cost devices that will increasingly form the backbone of IoT. These form a myriad of data sources providing up to date information on our world and how we live.

The growth rate of these devices is expected to be faster than the overall IoT market growth figures, primarily because of the rapidly growing need for connected data sources to support commercial operations.

SPONSORED REPORT

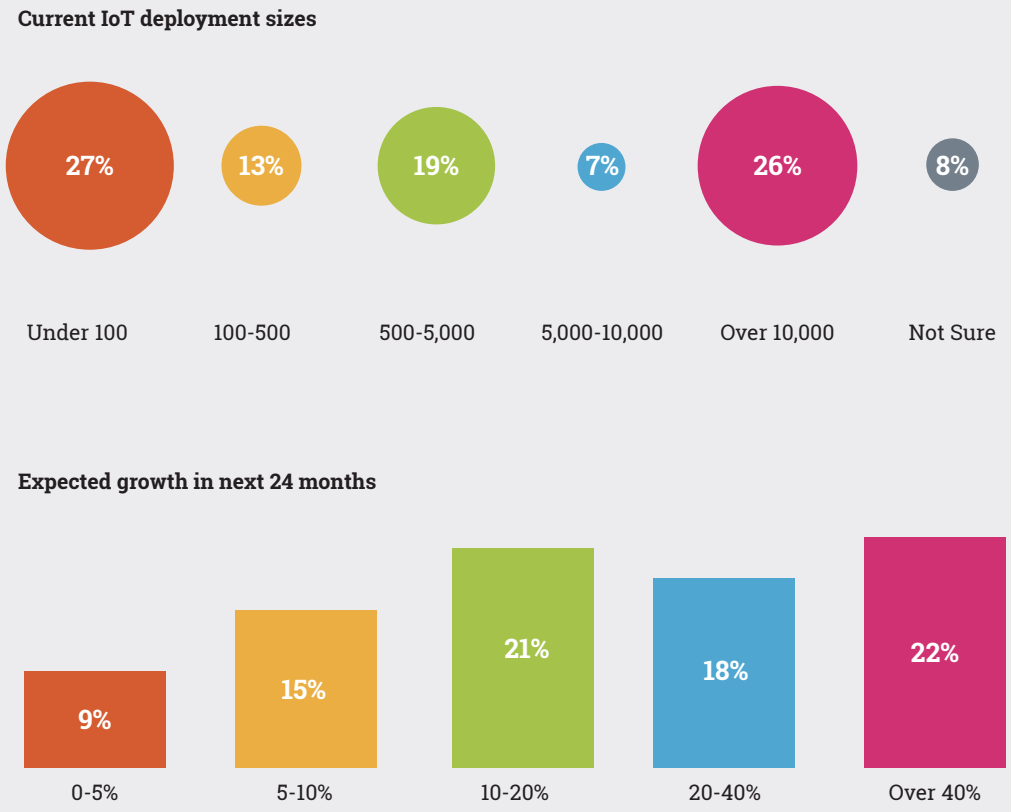



**Figure 1: Survey of IoT users: size of IoT deployments expected to grow rapidly**

This raises some vital questions, such as:

- How will these all be connected?
- How will they be powered?
- How will they be managed and updated?
- How do you ensure the data from them is sufficiently secure to trust it?
- Most of all, how do you make this easy for users to implement in the very large numbers envisaged anywhere in the world?

Taking this last point, for such large numbers of devices, connecting them securely must be a completely smooth operation where the user does not need to understand the technology – just switch on and go.

There is a growing consensus that standards-based embedded SIM (eSIM) technology and its integrated form factor (iSIM) provide a particularly appropriate basis for responding to these questions.

## From removable SIM to standards-based eSIM and iSIM

The physical SIM card has been part of cellular connectivity since 1991, when it was first brought to the market by Munich smart-card maker **Giesecke+Devrient** (G+D), who sold the first 300 SIM cards to the Finnish wireless network operator **Radiolinja**. It plays a leading role in many consumer mobile devices and IoT deployments and there have been several developments to reduce the size – from mini, to micro and nano. However, the SIM market is evolving rapidly, and newer options eliminate the need for a removable SIM.

First brought to market in 2012, the eSIM is soldered to a device's printed circuit board and introduced a way to send SIM profiles to devices over the air (OTA) using remote SIM provisioning (RSP). ▶

**Figure 2: How SIMs compare**

| | Mini SIM | Micro SIM | Nano SIM | eSIM | iSIM |
|---|---|---|---|---|---|
| **Introduced** | 1996 | 2003 | 2012 | 2016 | 2021 |
| **Physical form** | Plastic card | Plastic card | Plastic card | Soldered chip | Integrated in SoC |
| **Size** | 25 x 15mm | 15 x 12mm | 12.3 x 8.8mm | 6.0 x 5.0mm | Fraction of $mm^2$ |

The newest iteration is the integrated SIM, first brought to the market in 2021. This streamlines the eSIM's functionality by porting it into a system-on-a-chip (SoC) architecture, which means the SIM does not require dedicated hardware while also enabling remote SIM provisioning over the air.

**The classic or removable SIM** is a removable card that comes in various sizes. First developed for the consumer mobile phone market and inherited by the M2M industry, it has evolved into new form factors to fit smaller devices. They are straightforward and convenient for consumer applications and some IoT use cases. However, they present significant logistical and reliability issues for large-scale IoT device deployments as well as physical security concerns including theft.

For example, installing removable SIMs in manufactured products such as in the automotive sector used to be logistically difficult and expensive. They could not be installed in the factory – they had to be installed where each car was sold and used, to ensure each one was connected to the right mobile network. That introduced often substantial logistical issues to ensure that the right SIM reached the right car in the right country at the right time. The switch to eSIM helped to resolve these issues and, as a result, has led to a considerable expansion of the connected car market.

In addition to this, when an organisation switches mobile network and needs to change device profiles, removable SIMs are convenient in some use cases — users can simply remove the old SIM and plug in the new one. However, removing and replacing SIM cards on thousands of devices in large-scale IoT deployments can be costly or even impossible. If these devices are themselves low cost, then the physical replacement of individual SIMs may be considerably more costly than the devices themselves.

Although removable SIMs are easy to access, they are also subject to theft or tampering. Such SIMs must be continuously monitored to ensure they have not been removed and placed in other devices.

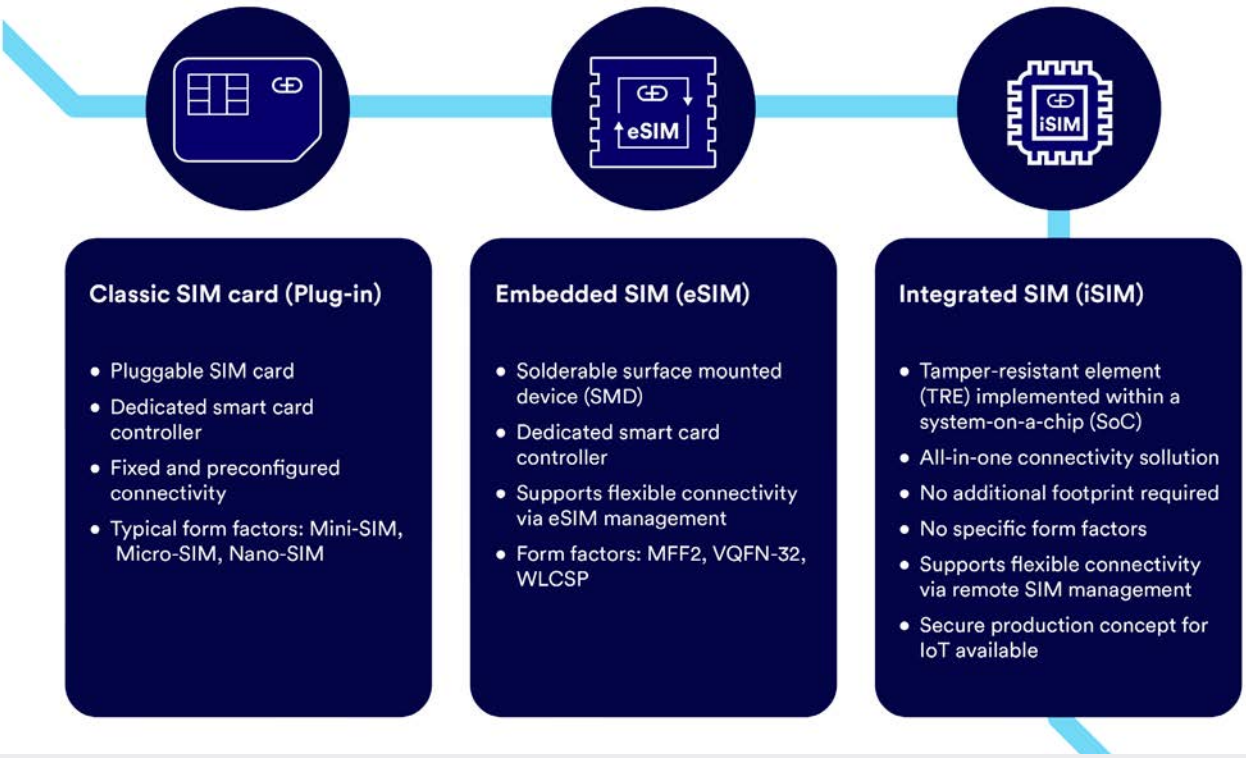
**The eSIM** was developed in response to the shortcomings of removable SIM cards for IoT. In particular, the connected car industry pushed eSIM forward. Automotive OEMs were motivated to create a tamper-proof SIM with more robust security that could be remotely provisioned with the right network profile. Such a SIM would serve their connectivity needs and protect against extreme environmental conditions, including dust, moisture, temperature and vibration.

Today, the automotive industry has adopted the technology widely, and all connected cars use a soldered eSIM as a single stock keeping unit (SKU). The embedded universal integrated circuit card (eUICC) standard makes the eSIM versatile. It allows remote provisioning of the hardware with network profiles. The standard allows mobile network operators (MNOs) to send their SIM profiles to eSIM devices remotely. By eliminating the need for physical access, the eUICC enhances connectivity management for secure IoT deployments at scale.

The eUICC standard also enables multiple profiles to be loaded. Devices can be manufactured for use in multiple geographies. Then they can be switched to the appropriate regional connectivity provider profile when the device is deployed or moved.

**The iSIM** has been developed to cater for cost-optimised devices that are efficient in terms of data and energy consumption and bill of material (BOM) costs. These use cellular IoT low power wide area network (LPWAN) options, such as NB-IoT and LTE-M, to address this IoT market need. iSIM technology incorporates the SIM ▶

**Figure 3: The evolution of SIM Technology**




operating system (SIM OS) into the cellular module hardware.

Unlike removable SIM cards, which are set into plastic housings, or eSIMs, which are soldered into the device, an iSIM (or iUICC – integrated UICC) is a tamper-resistant element (TRE) within a system-on-a-chip (SoC). It is an isolated hardware component combined with a baseband chipset to create a single connectivity module. The iSIM also saves space in hardware design. Every square millimetre makes a difference for size-constrained applications – particularly wearables. Since it does not require physical space for an eSIM chip or removable SIM card, the iSIM can also substantially reduce the device footprint.

With iSIM functionality built into the base cellular module hardware, the result is savings from eliminating components including SIM trays, SIM cards and eSIM chips. As a result, it is physically over 90% smaller than an eSIM chip. At the same time, it is particularly power efficient as the SoC itself powers the iSIM, which only uses power when it is actually being used for authentication. In addition, because the iSIM resides within the SoC and is directly connected to the SoC bus rather than through an interface to that bus, the performance is increased.

**Security is also enhanced** through the operation of the hardware TRE itself. The combination of hardware and software elements is very important. A secure software element on its own can always be hacked. If that structure can be changed, it can be cloned, impersonated or interfered with in many different ways. Secure hardware, on the other hand, is much more difficult. This is because hardware security involves burning secure identifiers/credentials into the hardware, which cannot then be physically tampered with or extracted. This is called a secure Root of Trust and considerably more secure than anything else. As such, it provides a secure basis on which to build a variety of value-added services that require very high security – see section on IoT SAFE later.

## What's special about iSIM

In this way, and in order specifically to cater for low cost, low power, constrained IoT devices, the iSIM has been designed to be the most cost-efficient SIM connectivity solution over the device lifetime.

The iSIM is now standardised along with the eSIM and together they have been catered for in three main Remote SIM Provisioning specifications – see section on RSP specifications for devices later.

Key points to note from this:

- The iSIM, the integration of the SIM into the baseband chipset, has paved the way for the next generation of secure IoT connectivity – in constrained devices
- The iSIM continues the success of SIM and eSIM in authenticating mobile networks without reducing security
- The iSIM ensures secure data processing while providing interoperability within the eSIM ecosystem
- For the foreseeable future, SIM, eSIM, and iSIM will coexist because they provide similar but also differing characteristics targeting varying areas of the IoT market
- The iSIM can be easily integrated into IoT solutions and enables secure device management during the entire lifecycle
- Since 2021 the iSIM is commercially available and has been proven in the field ▶

**Figure 4: Key iSIM benefits**


The iSIM has several features that help make it a more robust, secure phase of SIM card technology. These features have been designed by industry experts to meet agreed-upon, approved specifications, standards, and processes. As the latest phase of the SIM evolution, the iSIM offers several advantages and opportunities:

- **Reduced footprint:** embedded into the device's hardware, it allows for smaller, lighter devices that are less expensive to produce
- **Power optimisation:** lower power requirements means that batteries will last longer and IoT devices will benefit from greater efficiency
- **More efficient production:** integrating the iSIM as part of the baseband module can streamline production and operation processes
- **Security:** The isolated, tamper-resistant hardware element (TRE) is highly secure both physically and electronically
- **Reduced cost and time to market:** a generic and easy-to-integrate solution for all IoT verticals, as well as a significantly smaller chip that saves space, time and materials
- **Sustainability:** no extra housing or plastic, reduced power consumption and a much smaller size makes this the greenest SIM solution

## RSP specifications for cellular devices

As noted earlier, there are three main RSP specifications for cellular devices. These are:

- M2M (SGP.01/02)
- Consumer (SGP.21/22)
- Constrained IoT (SGP.31/32)

There are two standardised eSIM remote provisioning specifications currently in use designed by the GSMA: the Machine-to-Machine (M2M) eSIM Spec and the Consumer eSIM Spec. The M2M Spec is designed for IoT devices such as sensors that may operate without a user and have no user interface – so-called headless devices. It is implemented via SGP.02. However, this standard is based on SMS text message communication and is therefore neither efficient nor future-proof, since MNOs are now switching off SMS-based messaging.

In contrast, the Consumer Spec is designed for user devices such as smartphones and tablets, where there is a user interface. This makes managing profiles simple, only requiring user consent to add a new profile or switch between profiles. It is implemented via SGP.22 that relies instead on IP-based communication.

As a result of this, a new RSP SGP.32 standard for constrained IoT devices has been designed. This is similar to the successful SGP.22 for consumer devices but specifically caters for IoT devices with no interface – headless devices. As a result, iSIM with RSP functionality follows this standard. ▶

Standardisation of the RSP specifications belonging to the SGP.32 family have now been finalised but it will take until 2024 for iSIM products with full RSP support to reach the market.

## RSP and SIM profiles

In addition to the SIM OS, one or more SIM profiles are usually loaded onto an RSP-enabled SIM (mainly eSIM or iSIM, but in some cases a removable SIM) so that it can use them to authenticate itself to the respective network operator. Managing profiles goes within a few seconds when using a broadband connection. In the case of narrowband IoT, this can take longer. The administration is done in the background via an end-to-end secured connection to the RSP server.

As noted earlier, one of the great advantages of RSP is the single SKU. All devices can be produced identically, which significantly simplifies logistics as well as the production process and leads to cost savings. The decision as to which profile is to be used or loaded is only made when the device is commissioned for the first time. In practice, there are different use cases for which the use of the RSP technology is beneficial:

a) Switching between previously loaded profiles to adapt the IoT device to the best connectivity at the device's location (national or international), for example. This can also be used to keep roaming costs as low as possible. The SIM memory typically limits the number of pre-loaded profiles. If the change does not work, the device is switched to the original profile or to an alternatively available profile.

b) During the lifetime of an IoT device, it may be necessary to exchange a previously loaded profile. This may make sense for cost reasons, for example, or because the device is to be operated in a country not previously considered, or because a network operator has discontinued its service. In these cases, before changing a profile, assuming there is enough free memory on the SIM, the new profile must be loaded via the mobile network. Profiles that have already been loaded but are not active can also be deleted via RSP to free up memory. After the new profile has been successfully loaded, the change can be completed. Here, too, the system switches back if the activation of the new profile is not successful.

c) While previously loaded profiles with an international mobile subscriber identity (IMSI) incur costs even when not in use, using a so-called bootstrap profile offers a cost-effective alternative. Bootstrap profiles are designed by default to allow download of a permanent profile. They enable devices to connect to any available mobile network – whenever a device is turned on for the first time and wherever they are operated in the world. This enables a device to 'auto-configure' itself the first time it is switched on in the destination market.

   G+D's technology maximises efficiency by using this bootstrap profile in order to enable massive deployment of devices at low cost and allow downloads of additional operational profiles as needed. Permanently connecting to a bootstrap profile ▶

to transfer device data is not possible – it connects only to the RSP server, but not to any other network operator. During the lifetime of the IoT device, it is also possible to switch back to the bootstrap profile to load another profile in the event of a fault or for other reasons.

## IoT SAFE

The eSIM and iSIM have introduced tamper resistant elements (TRE) that enhance the security aspects of the SIM to a higher level, both physically and electronically.

The standardised eSIM specification was developed by the GSMA as a response to the problems of using the traditional removable SIM cards in IoT devices. A further GSMA initiative is the IoT SIM Applet for Secure End-to-End Communication (IoT SAFE). This recommends that the industry should use the SIM as a hardware TRE or root of trust to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted technically that the SIM is particularly well-suited for this purpose: it is one of the hardest of all identifiers to spoof, with advanced security and cryptographic features, is fully standardised, and has been deployed in huge numbers of devices for the past 30 years. Key characteristics of IoT SAFE include:

- Use of the SIM/eSIM as a mini 'crypto-safe' inside the device to securely establish a TLS session with a corresponding application cloud/server
- Compatible with all SIM form factors such as eSIM and iSIM. eSIM/iSIM are particularly suitable for IoT SAFE since they are certified
- Provides a common application programme interface (API) for the highly secure SIM to be used as a hardware root of trust by IoT devices
- Helps solve the challenge of provisioning millions of IoT devices

The IoT SAFE applet runs on Java virtual machine, which in turn runs on the SIM OS.

## Choosing the right SIM for your deployment

When selecting a SIM type and form factor for your IoT deployment, start by considering cost structure because it reflects the business model behind the device. For example, in the automotive sector, the cost of the final product might motivate you to invest in expensive chips. Embracing a less expensive platform would mean compromising on resiliency and security.

If your product is a low-tier device such as a pet tracker, spending an extra dollar or two on hardware per device could eliminate your profit margin. In that case, seeking a low-cost iSIM solution makes sense.

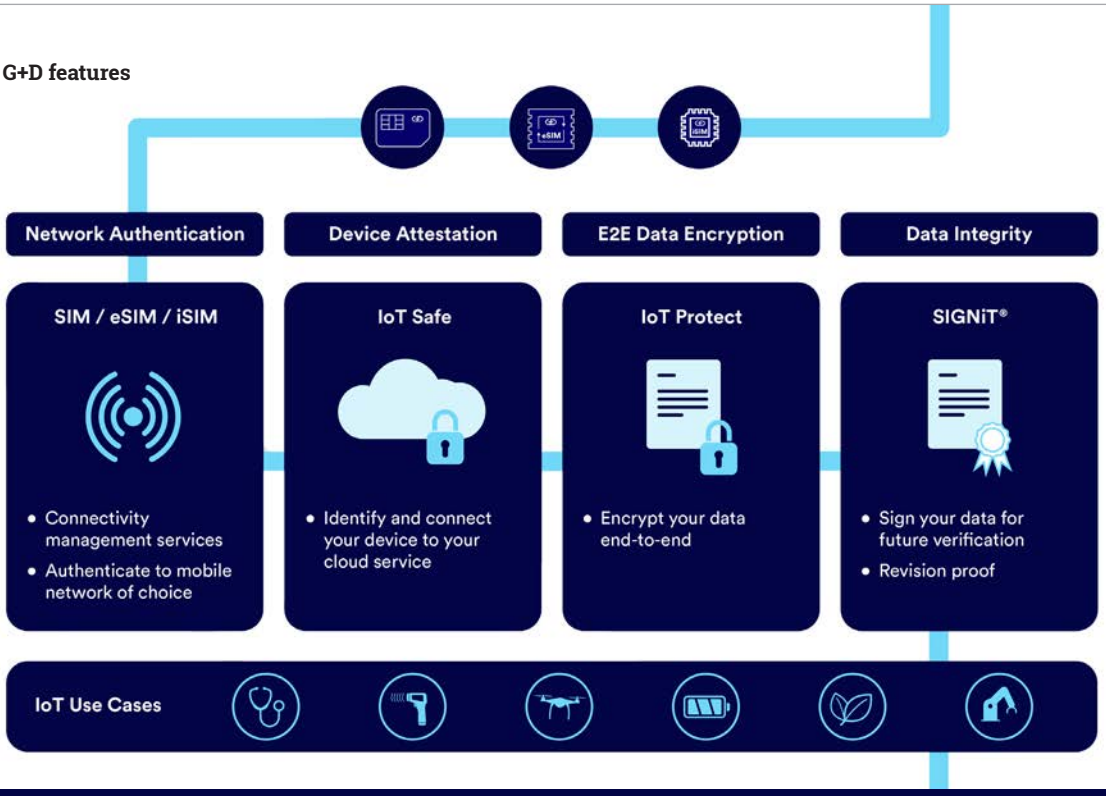
Also, consider whether the use case will require remote provisioning. While eSIMs are best known for this feature, all form factors are candidates for eUICC software that enables OTA profile updates. GSMA has designed a large-scale provisioning scheme for the IoT space, allowing MNOs to provision devices in large volumes simultaneously.

## The future of SIM technology

In spite of the huge growth of eSIM and iSIM, traditional SIM cards continue to exist in the IoT market — at least for now. In many countries, prepaid service remains the predominant way to connect, making traditional SIM cards the most practical choice.

For high-end IoT use cases with an inherently higher cost structure that require a high degree of MNO acceptance from the first day, eSIMs are an ideal solution. iSIMs will come into play for low-tier IoT connections where device size and energy efficiency are necessary strengths. There is a lot to consider when choosing between SIM, eSIM and iSIM. Depending on the use case, there is room for every form factor and SIM type for the foreseeable future. ▶

**Figure 5: G+D features**




## How G+D helps

The G+D IoT Security Suite protects data generated from IoT devices. The suite supports cellular and non-cellular devices. Its core services are IoT Safe, IoT Protect and SIGNiT. The platform covers both the backend and SIM software. It enables mobile operators to offer a consolidated toolbox to OEMs and enterprises. They, in turn, are able to manage SIMs and other devices over the entire lifecycle – from manufacturing and activation, to managing subscriptions and policies, all the way to deactivation.

### 1. IoT Safe

Companies build IoT solutions for the marketplace, and these devices connect to cloud platforms. The credentials, however, are mostly stored within the application processor memory. This makes them an easy target for attacks. The G+D IoT Safe protects against threats and provides cybersecurity by adding a secure element (a SIM card) to the IoT device. It is equipped with an applet that assists with the authentication to the cloud provider. In addition, this offering includes a credential manager that controls and replaces factory credentials. We also offer a device toolkit that provides documentation, which includes the sample code that is used to assist the IoT device developer in securing the communication between the IoT device app and the SIM applet.

### 2. IoT Protect

The overall functionality of IoT Protect is to provide an end-to-end encryption/decryption mechanism for IoT applications. Information is transmitted securely between the IoT device and the backend, independent of the communication channel (broadband, NB-IoT, Wi-Fi, etc.). Common applications for IoT Protect are those in which data transfer is low, which is typical for low-end and battery-powered IoT devices.

### 3. SIGNiT

SIGNiT is the solution that provides data integrity for multi-party IoT ecosystems. It helps sign every packet of IoT data generated so that they can be verified in the future – starting directly at the source: the IoT sensor. Digital signatures for its data are provided by either the SIM or eSIM.

SIGNiT combines secure and proven SIM environments with blockchain technology. It allows enterprises to easily digitalise and secure processes in a decentralised ecosystem while providing IoT users with comprehensive and robust security for data generated by IoT devices. The solution has already been successfully implemented in commercial environments, and has potential in sectors like logistics, agriculture, energy and the automotive industry.

**A recent example:** SIGNiT enables **Lufthansa Industry Solutions** to ensure that IoT data is 100% trustworthy – featuring G+D's awarded security technology and an innovative blockchain by Cologne-based start-up **Ubirch**. Ubirch has developed a trust protocol, which ensures that data from IoT sensors cannot be falsified after they are generated. The data packets of these sensors are sealed with strong cryptography in a way that it becomes technically impossible to manipulate them once stored in a blockchain. This combination of offering blockchain on a SIM is unique and the first of its kind.

### 4. Connectivity

G+D also offers 'out-of-the-box' connectivity, optimised specifically for IoT applications. This covers over 600 mobile networks in 185 countries. Furthermore, even 3GPP-based satellite network connectivity can be offered in remote areas, meaning truly global coverage is achieved.

### 5. Connectivity and lifecycle management with IoT Suite

G+D's IoT Suite is an innovative connectivity management platform that offers a new level of IoT management. This platform seamlessly integrates with SGP.32, ensuring maximum compatibility for IoT devices. Devices and accounts can be visualized and monitored from a single dashboard, which effortlessly integrates with existing systems, thanks to its open API and agnostic technology. ■

**www.gi-de.com**

# Security for the future of AI

Matt Hatton, founding partner at Transforma Insights, interviewed Vincent Korstanje, the chief executive of Kigen, about why security is the most critical consideration at the intersection of generative AI, IoT cybersecurity and blockchain, the implications of global supply chain fragmentation, and why one Eddie Murphy movie is very relevant to the new IoT world

**Matt Hatton: The interview is for the CES edition of IoT Now. Kigen will be heading over there. What are you expecting to talk about?**

**Vincent Korstanje:** In **Kigen**, we're thinking a lot about artificial intelligence now and its implications for our customers and society at large. It'll hardly come as a surprise as practically every industry sees a new paradigm of innovation with AI. The consumer tech domain is set to see the strongest increase with US$10.8bn of revenue growth by 2028 from Gen AI. As customers begin to implement it rapidly, it's encouraging that we are guiding the direction on security for AI. There are a couple of angles to this.

AI is mostly used to assist in performing tasks passively, but it's much more interesting when it makes decisions for you. Autonomous driving is one particular example where AI is starting to act, and those decisions have the potential to be life-critical and mission-critical. To act, AI needs to compute critical vehicle, passenger and surrounding data and to get it into engines. If the AI is acting, and there's no human filter, you had better make sure that the whole process, from sensing to acting, is highly secure. In an AI-powered world, security isn't a feature; it is a necessity.

So, where do you start? The answer is: Device security. A secure OS is the best way to secure a device. And our way to market is to help connectivity providers secure their credentials on the device. For device makers directly, we enable them to get their chosen connectivity with carrier-grade security. That element on the device is an expensive and secure asset, which allows you to use it for other value-added use cases and services that need data to be signed. Both parties can use the Open IoT SAFE app, providing the highest level of security for getting data off the device. And, more than that, sign the data coming off the device so there is proof of where you got that data from. This becomes essential if you're trying to secure the whole system to then use it with AI innovation.

Of course, Gen AI models are not perfect yet, and won't be until and unless we act with urgency on security built into AI-everywhere.

**MH: Can you give me an example of secure data proof driving revenue for OEMs?**

**VK:** Sure, we have a great implementation with a customer, **Energy Web**, which is a leader in decentralised energy trading – via data monitoring units to smart meters, solar panels, EV charging stations, wind turbines and so on across the world's largest zero-carbon ecosystem. The data from those devices is put in a blockchain, and the information is sold to energy providers to derive additional benefits, for instance, on where energy stores are available and when they can be used. Blockchain is great, but if the data is tampered with, then it makes it all invalid. You need to sign, tag and track the data all through the supply chain.

Our collaboration with Energy Web and **KORE** focuses on doing just that, allowing data trading to increase energy efficiency. What's really unique here is having end-to-end security that empowers unique capabilities of services built on exchanges, be it trading or transacting. For OEMs today, ▶

***In an AI-powered world, security isn't a feature, it is a necessity***

thinking of what experience and service model they want customers to engage with is essential, and a simple investment in IoT SAFE with readily available software and stack components unlocks new revenue streams.

Security of IoT data, networks and devices remains a challenge for OEMs. The issue of lack of ownership of security is a hindrance and here's a standards-based, future-proof solution that addresses this. This is where Kigen comes in.

What we enable in IoT with the benefit of eSIM also allows for doing more with data being delivered into AI. Data, in general, is important. You need to protect it and understand it: Who has collected it? What has been done with it? Making sure that the data can't be changed. All of that is going to be very important to talk about at **CES**.

**MH: What are your perspectives on the impact of IoT on some of the geopolitical challenges happening now?**

**VK:** Our customers have been faced with overcoming the pandemic and component shortages, followed by some disruptions through global political conflict and a high inflationary economic climate. As a result, we see a heightened focus from countries to bring more manufacturing, IP and supply chains locally. This can present challenges, but it also has spurred business model innovation.

Kigen has a horizontal play, making security simple and accessible. We horizontally disaggregate the supply chain: we just provide the SIM software and enable other companies to provide the hardware (to the names OEMs would be familiar with as module and chipset vendors), and work with all across the supply chain. We focus on what we're good at and let others build on that for differentiation. This has a strong benefit for end customers, especially where there is a need for local ecosystem collaboration. ▶

**Vincent Korstanje**
**Kigen**

***The main consideration in the creation of data silos is interoperability***

For instance, take Kigen's recent collaboration with **Protahub** and **floLIVE** in Turkey, which is targeted at opening markets with strict requirements about manufacturing in-country. Turkey has some of the strictest data sovereignty and localisation regulations, and permanent roaming is prohibited. So the connections must be managed locally. We work with Protahub, the entity authorised in Turkey to comply with all types of connectivity regulations, from maintaining IP traffic inside the country to remote, full localisation, with a single stock-keeping unit (SKU) SIM and connectivity. 71% of countries have data privacy laws and another 9% have legislation pending, which can pose issues for cross-border connectivity and data requests, so the same approach applies beyond one country.

Similarly, in India, we work with SIM makers to support operators that have standardised on Kigen. We're opening a world-leading data centre in India, which will be the leading facility with **GSMA** SAS-UP certification by the time of CES. We're enabling local production in the country as India intensifies local efforts as a manufacturing hub and the world's fastest-growing digital economy. We've also just empowered manufacturers for eSIMs to be produced locally in Brazil with our software, of course, with our own quality control to ensure compatibility.

Further, there is the dynamic of the two largest powerhouses: China and the US, and the need for there to be two different supply chains independent of each other. We're agile and committed to flexibility. This allows us to enable supply chains for different players to be more localised but with the same functionality and compatibility across all vendors. It's an ethos we have retained from being founded within **Arm**, which allows different companies to make chips in their own markets.

Thinking about China and the US, We, and everyone else, have to work with the FCC, enabling the compliant solutions to coexist. We need to work with those other economies but be mindful of security implications. The new EU Data Act is also symptomatic of the wider phenomenon.

**MH: Interesting you should mention the EU Data Act, as we're seeing an increasing amount of regulation around IoT. How do you see that, and other regulations, having an impact?**

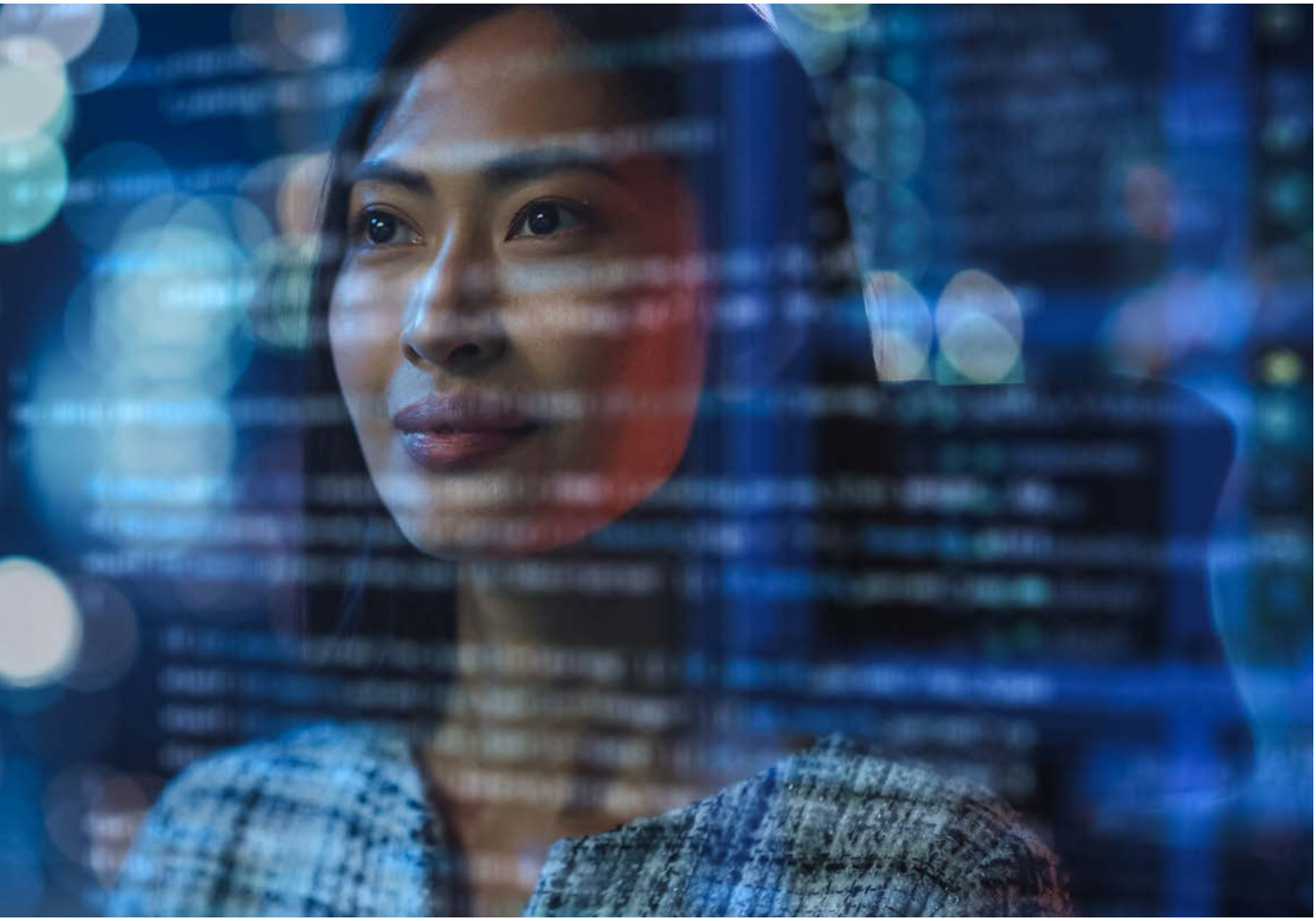
**VK:** From a business view it's quite interesting. For years, data has been identified as the new oil, which shows the importance of data and by extension, data trading. Data trading is the

data which can be aggregated and bundled up for weather predictions; many organisations could benefit from access to that data. Much of the new EU rules are aimed at helping make data interoperable.

The main consideration in the creation of data silos is interoperability. With this, what you can do is create environments where you can trade data, for instance data from all the all the leading brands of thermostats. What we need to do is find more ways of data trading to solve problems.

Kigen's fundamental approach to this issue is that you can't trade data if you don't know its heritage. Consider smartphone photos: each has a geolocation and time stamp, but you can change those, so it can't be used as proof of anything. If you cryptographically sign a file, you can't change it again, meaning it could be used as proof and it becomes valuable. Moving to IoT, consider the moisture sensor again. It will become a hygiene factor to make sure no one has messed with the data. The more you make automated decisions, the more it's critical that it can't be tampered with. Every IoT device will need to provide information on when its data was produced, where, who has access to it, and so on.

**MH: At Transforma Insights, we've looked closely at the topic of security risks and there aren't many IoT applications where there's no risk of intervention from a bad actor. Is that how you see it?** ▶



**VK:** Yes, indeed. Think about commercial espionage and providing bad data about commodities. If you've seen the movie Trading Places, a lot of that revolved around providing false weather data which was very relevant to the prices of a commodity market, frozen orange juice.

**MH: Great to get a reference to an Eddie Murphy movie into an interview, but sadly we can't dwell on it too long. I want to delve into how some of the technologies you're involved with are transforming the experience of consumer products?**

**VK:** "How to transform experiences for customers?" I listen keenly from our customers, OEMs and device makers around this and feel we are at a great intersection of the tools available to them: Generative AI, cybersecurity, future of digital payments and more! Our job at Kigen is to make them successful in rolling these devices out of the market with the best chance of doing this now and lasting for the longest time for consumers to benefit. So three things:

Firstly, security that just works. End-to-end security, designed with a secure element that's resilient to hacks and built on standards such as GSMA and **Global Platform** so that consumers trust their IoT applications. Biometers, payments and deeper integration into the services that people rely on – are all enabled through these. We're bringing that into IoT devices as default.

Secondly, it's about using connectivity to deliver a product with a service. A product that is always connected is always able to deliver that benefit. And this extends to lots of use cases. Wi-Fi has been an easy route to connectivity, but it has its limitations in both resilient and consistent experience. Consumers expect unhindered always-on connectivity with a unique device experience, on the move: a connected watch or wearable on the run used to need a smartphone, now we see customers moving to narrowband-IoT (NB-IoT) enabled cellular products that can offer personal trainer and coach service, social encouragement, all independently.

Third, we have launched our eSIM consumer OS that is garnering interest particularly driving enriched mobility and travelling experiences, smart streaming wearables, voice and music streaming speakers and even laptops. Last year, our eSIM-enabled **Motorola** Satellite Link was unveiled with **Skylo**'s profile at CES, and went on to high praise as the 'Product of MWC22' for the simple experience delivering peace of mind in even the most remote situations. Similarly, we are looking ahead to supporting the next tranche of eSIM experiences that contain the ultimate blend of Gen AI applied with strong security and out-of-the-box connectivity.

***We are looking ahead to supporting the next tranche of eSIM experiences that contain the ultimate blend of Gen AI***

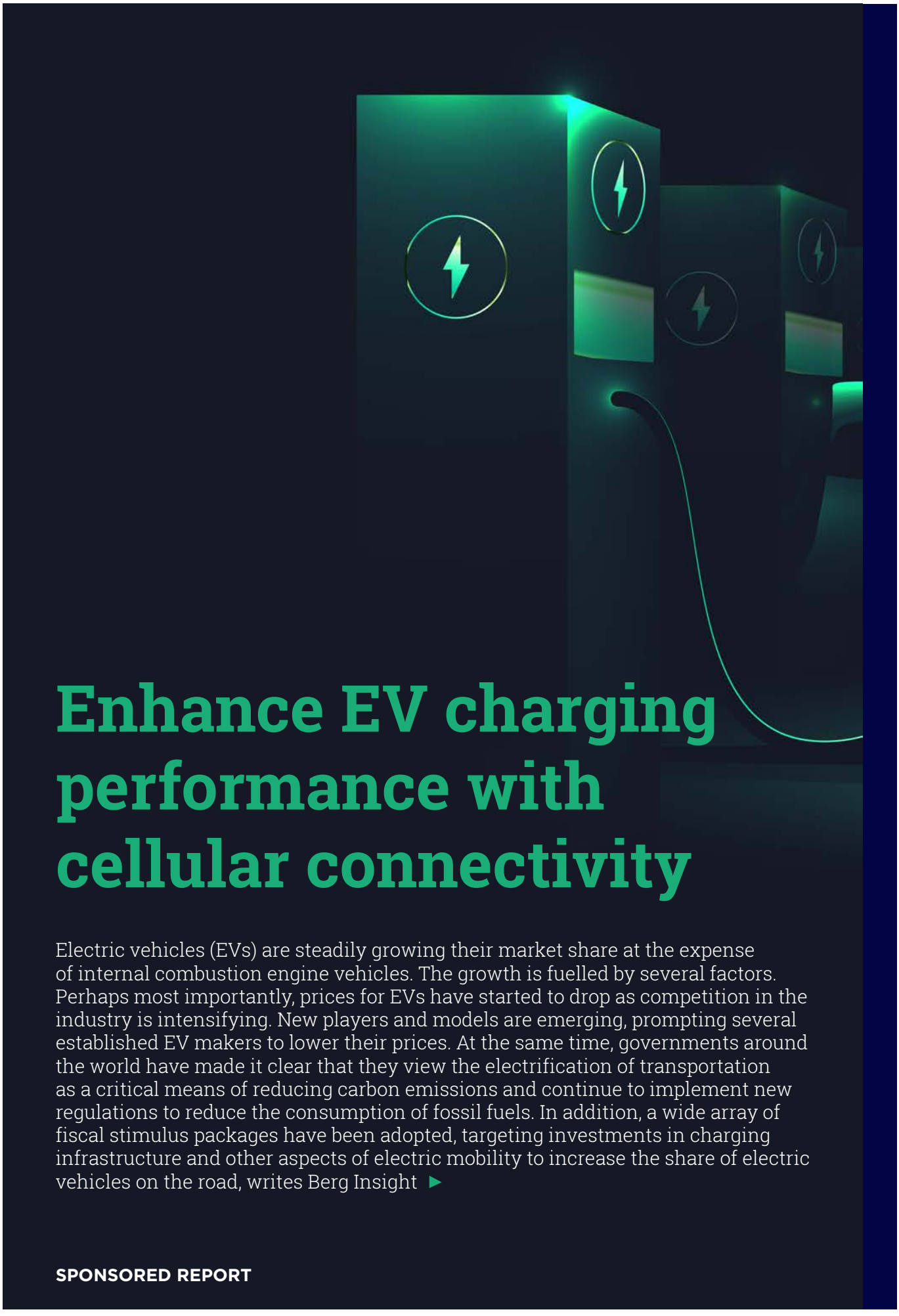
**www.kigen.com**

# Why cellular connectivity will enhance EV charging performance

Berg Insight™

Report sponsor:

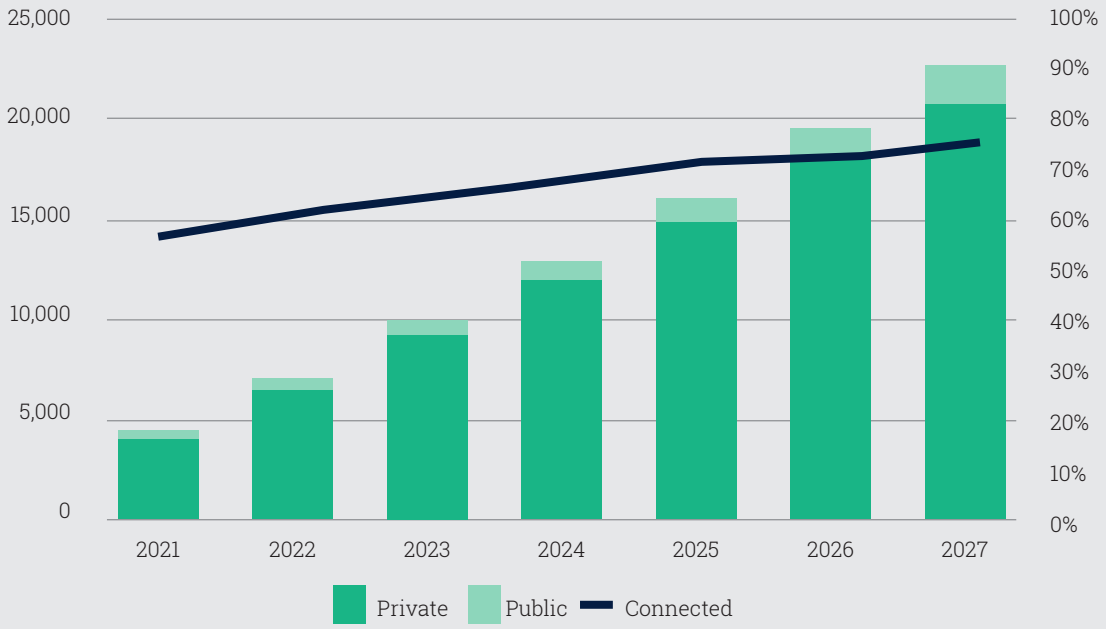
pelion



# Enhance EV charging performance with cellular connectivity

Electric vehicles (EVs) are steadily growing their market share at the expense of internal combustion engine vehicles. The growth is fuelled by several factors. Perhaps most importantly, prices for EVs have started to drop as competition in the industry is intensifying. New players and models are emerging, prompting several established EV makers to lower their prices. At the same time, governments around the world have made it clear that they view the electrification of transportation as a critical means of reducing carbon emissions and continue to implement new regulations to reduce the consumption of fossil fuels. In addition, a wide array of fiscal stimulus packages have been adopted, targeting investments in charging infrastructure and other aspects of electric mobility to increase the share of electric vehicles on the road, writes Berg Insight ►

**SPONSORED REPORT**

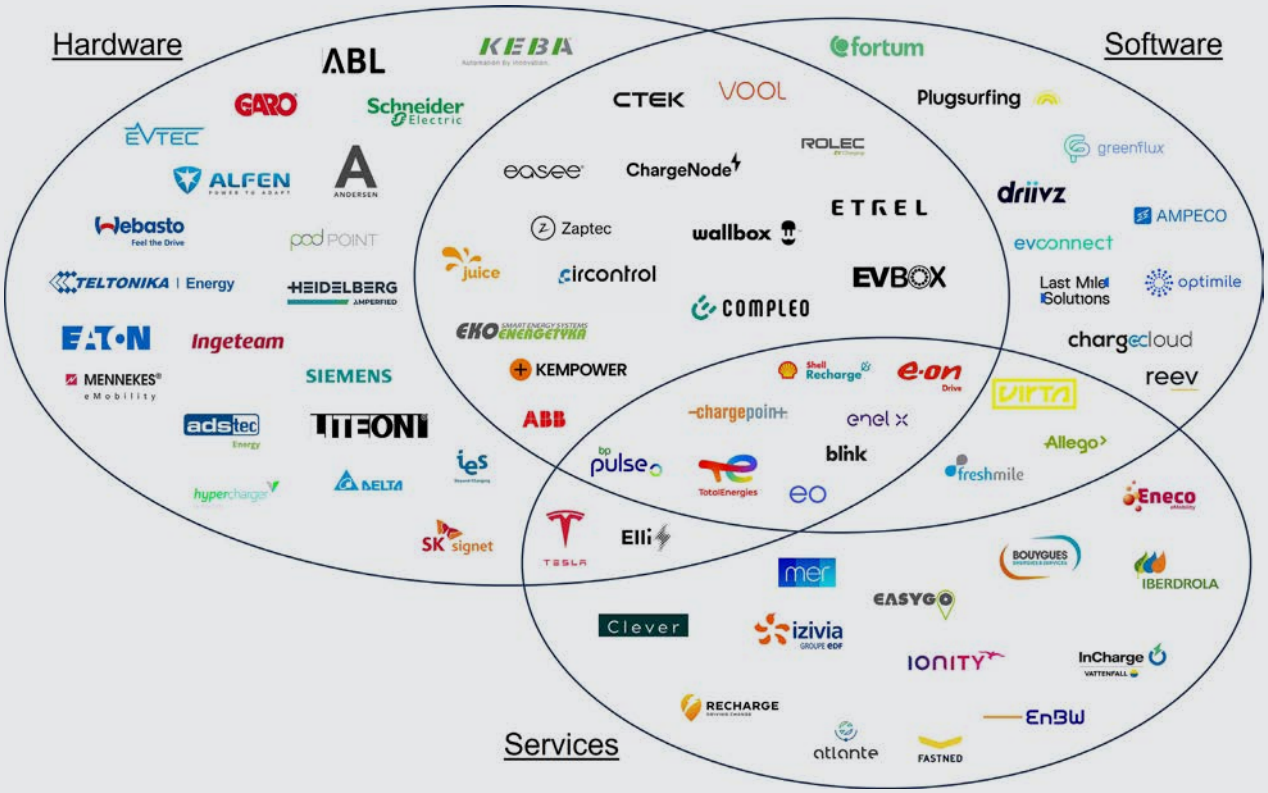



**Installed base of EV charging points in Europe (2021-2027)**

The EV charging market has grown significantly over the last few years, despite recent economic headwinds and supply chain-related challenges. The total installed base of charging points in Europe amounted to about 7.1 million in 2022, including around 0.5 million public charging points and 6.6 million private charging points. Private charging points include all dedicated charging points, excluding the public chargers defined as by the European Alternative Fuels Observatory (EAFO). Private charging points can be home charging points, workplace charging points and other charging points unavailable or partly available to the public according to EAFO's definition.

## EV's role in future mobility solutions

Today's market mainly comprises three types of EVs – battery electric vehicles (BEVs), plug-in hybrid electric vehicles (PHEVs) and hybrid electric vehicles (HEVs). The batteries in BEVs and PHEVs can be charged using external power sources like household outlets or designated EV charging stations, while HEV batteries are charged through operating the vehicle. Charging stations are crucial to support the rapidly expanding fleet of electric vehicles, making the respective markets highly interdependent. The adoption of both needs to keep pace to reduce range anxiety and ensure a smooth driver experience. ▶




**EV charging hardware and software vendor landscape**

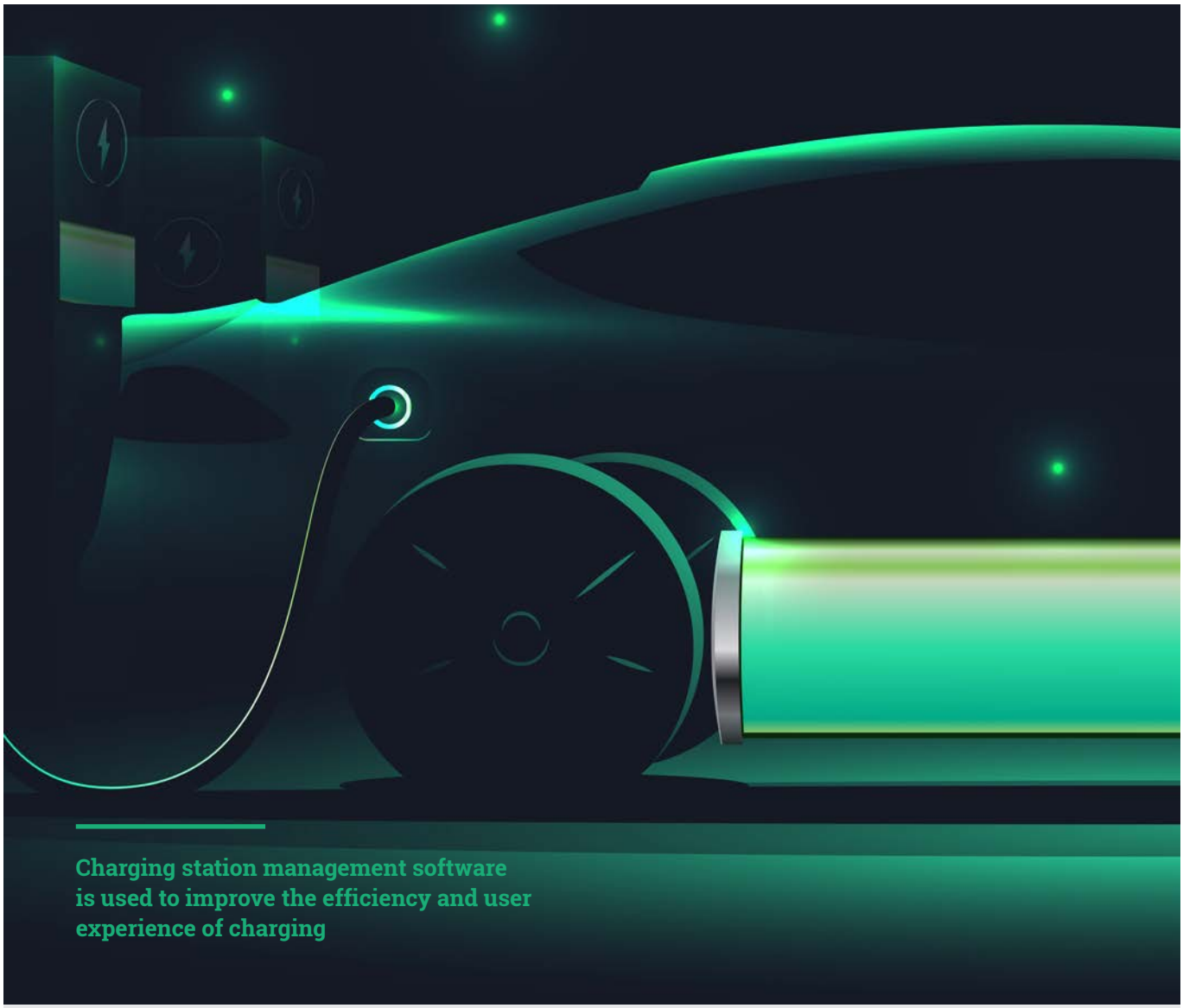
The sales of new EVs have grown rapidly in the European markets for several years. In 2022, new BEV registrations in the EU+EFTA+UK region grew by 30% to 1.6 million vehicles. On top of this, 920,000 new PHEVs were registered in 2022. The trend has continued throughout the first half of 2023 too, with the combined sales of BEVs and PHEVs growing 28% compared to H1 of 2022.

## The EV charging ecosystem

The EV charging market hosts a variety of different types of players. Several hardware providers are specialised EV charging station manufacturers focusing more or less exclusively on these products, with some even focusing solely on either AC or DC charging stations. In addition to manufacturers of EVs and EV chargers, the market includes players offering charging station management solutions, charging station operation and electric mobility services. The business scope varies, with some companies offering end-to-end solutions including hardware, software and services, while others specialise in a specific part of the value chain.

The two main service categories within the EV charging industry are charge point operators (CPOs) and e-mobility service providers (eMSPs). A charge point operator (CPO) manages one or several networks of charging stations. The operator does not necessarily own the charging stations but is responsible for maintenance, service and administration of the charging stations in the network. For example, a housing cooperative can install charging stations and contract a CPO to be responsible for keeping the chargers functional and to distribute the charging cost between the users of the charging stations.

E-mobility service providers (eMSPs) mainly operate in the public charging segment and offer EV drivers access to the charging stations in their connected networks. This is accomplished by providing means of authentication at charging stations like customer accounts, RFID cards or tags, and charging apps. In most cases, CPOs also act as eMSPs but there are examples of companies acting only as a CPO or an eMSP. ▶



**Charging station management software is used to improve the efficiency and user experience of charging**

## The basics of EV charging

The rate at which an electric vehicle is charged is measured in kilowatts (kW), and the EV battery's capacity to store energy is measured in kilowatt-hours (kWh). There are two main types of EV chargers – AC chargers and DC chargers – named according to the type of electric current they supply to the vehicle. In Europe, a charger able to charge more than one vehicle simultaneously is often said to have multiple charging points.

AC chargers are simpler and feed the EV with AC power from the grid without major transformations. An on-board charger in the vehicle then converts the AC power into DC power that can be stored in the battery. In this case, the on-board charger is usually the limiting factor when it comes to the rate at which the battery can be charged.

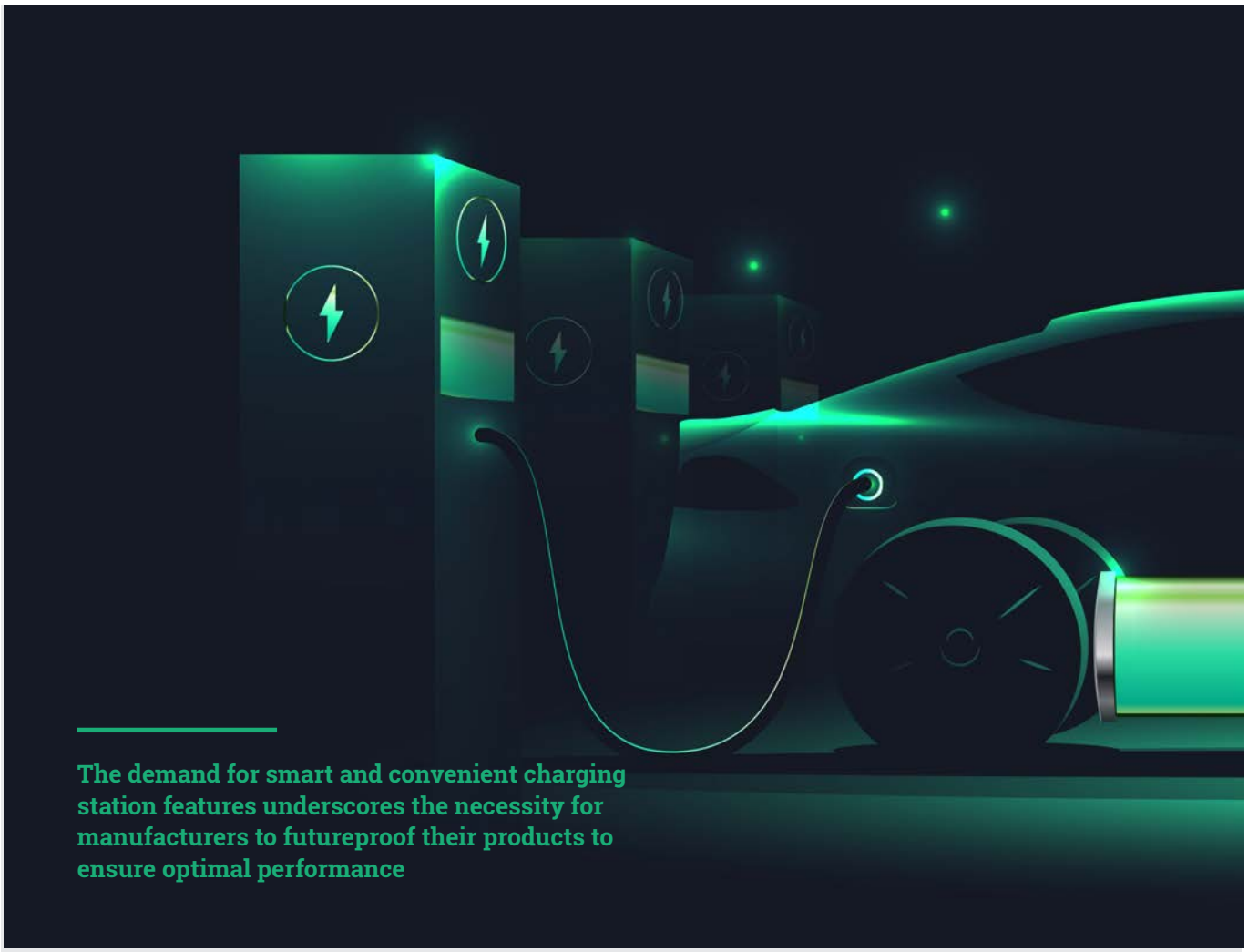
DC chargers are generally larger and more complex as they convert AC power from the grid into DC power directly, enabling the charging process to bypass the vehicle's on-board charger and feed electricity directly to the battery. In this case, it is either the battery's structure or the DC charger that limits the rate at which the battery can be charged.

## Energy optimisation

Charging station management software is used to improve the efficiency and user experience of charging. In private settings, management software enables drivers to plan charging sessions, log power consumption and keep track of costs. The solutions also provide alerts to warn in case of malfunctions as well as functionality to share the charging stations and to assign cost to the right user.

Another important aspect of charging station management is energy management. Energy management solutions allow for monitoring and management of the charger's electric consumption and adapt it to the limitations of the local grid connection. Load management features can distribute the charging load between charging points and the rest of the local grid to reduce the risk of overloading fuses and power outages.

Demand response solutions adjust the power consumption from the chargers to limit the strain of the power grid. For example, charging can be scheduled to occur on off-peak hours for the grid when prices are lower. Modern energy management tools can also consider the contributions from local power generation and energy ▶



**The demand for smart and convenient charging station features underscores the necessity for manufacturers to futureproof their products to ensure optimal performance**

storage solutions, like batteries or EVs capable of bi-directional charging. The case for smart charging and load balancing functions has become even stronger in view of the increasing energy costs.

## Secure firmware updates ensure optimal performance

The demand for smart and convenient charging station features underscores the necessity for manufacturers to futureproof their products to ensure optimal performance. A critical component of futureproofing efforts is the implementation of secure firmware updates. Firmware updates can ensure that the chargers are compatible with new EV models, as well increase the reliability of or the chargers by minimising downtime. Similar to any connected device, charging stations are susceptible to cybersecurity risks. Manufacturers can address vulnerabilities in the charging station's software through firmware updates and ensure that it remains secure against potential threats.

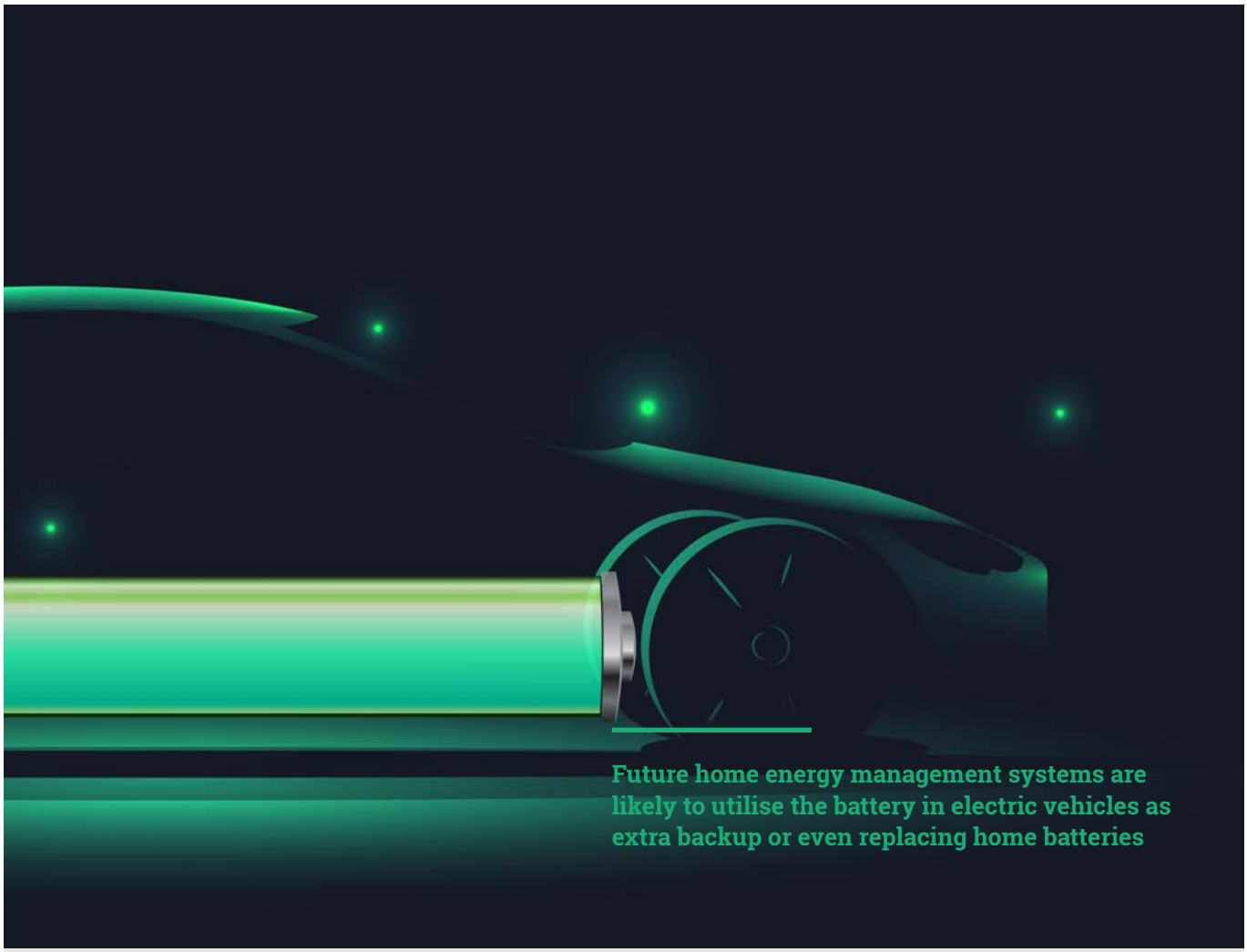
## Cellular connectivity offers flexibility and independence

EV chargers commonly feature some type of connectivity, such as cellular, Wi-Fi or fixed connectivity. In a private setting, cellular connectivity offers distinct benefits to other options. If a CPO is responsible for the charging station, connecting it with cellular connectivity removes potential limitations and uncertainties related to using a third-party network. Wi-Fi coverage may be limited or easily disrupted at the installation site and wired connections may incur additional costs. Customers may also not prioritise improving Wi-Fi coverage as few other devices need a connection where EV chargers are installed. Cellular connectivity enables the chargers to be installed where they are most useful to the driver and not where connectivity is available. Additionally, it offers a more reliable and independent connection to the charger, which helps improve the service level.

## EV charging will benefit from eSIM localisation

Cellular connectivity is an essential enabler for remote charging station management, which must be further optimised for coverage, performance and security to match the requirements for the deployment. Traditional roaming can meet the requirements for applications with low to medium data volumes but may lack support for connectivity across multiple networks in any given country. Local sourcing of SIMs from local mobile operators is always a possibility, but the model becomes increasingly complex when scaling to a growing number of countries.

eSIMs address the shortcomings of traditional cellular connectivity solutions by enabling over-the-air management of multiple operator profiles without having to replace the physical SIM itself. As the operator ▶



**Future home energy management systems are likely to utilise the battery in electric vehicles as extra backup or even replacing home batteries**

selection and personalisation is moved to the post-deployment stage, manufacturers can buy large batches of eSIMs and install them in their chargers without deciding which operators to use. With eSIM technology, the chargers can automatically scan networks and download the most suitable operator profile at the installation site when turned on. Thus, eSIM technology can both simplify manufacturing and installation processes, but also future proof the device against changes in network coverage.

Using a single cellular connectivity provider offers several benefits that streamline operations and reduce complexity. A unified platform for managing connectivity centralises control of devices and services, making it easier to monitor, manage and troubleshoot the network, and provides one point of integration. With one provider, it's also easier to ensure that all devices adhere to the same security protocols and regulatory requirements, reducing the risk of breaches that can occur due to inconsistent security measures.

## Interoperability strengthens the EV charging value chain

The fragmentation of the EV charging market creates significant challenges relating to interoperability between the various products and solutions. An important means of mitigating the problems arising in the diversified EV charging market is the open charge point protocol (OCPP), which gives hardware from different vendors a common language for communication with charging station management software. This allows companies to specialise in their segment of the value chain, like charging hardware, software or services. The OCPP also opens up the market for players like CPOs and enables them to use hardware that suits their different installation sites and management software that suits their operation. In addition, a standard communications protocol reduces technological lock-in and reduces the risk of choosing new, untested suppliers.

## The future of EV charging and home energy management systems

Future home energy management systems are likely to utilise the battery in electric vehicles as extra backup or even replacing home batteries. Vehicle-to-grid (V2G) or vehicle-to-home (V2H) are systems where the vehicle can send back power from the battery. This requires an EV charger that features bi-directional charging. It may also require an upgrade of the home's electric system to enable disconnection from the grid. Bi-directional charging functionality is starting to be introduced in new chargers. A typical EV has a battery with a capacity of about 67 kWh. High-end EV models may have batteries with a capacity of well over 100 kWh. In comparison, battery storage systems for residential applications typically have a capacity of 5–15 kWh. Due to the size, an EV battery could power a home for several days in case of a blackout, whereas a typical home battery would last only for a day.

# Why anomaly detection matters

Security measures are vital to defend and protect IoT devices and solutions, writes Pritam Shiravadekar, the product manager for value added services at Wireless Logic. It is natural to focus resource on prioritising breach prevention – everyone wants to avoid breaches – but companies mustn't neglect detection. If they do, significant damage could be done before a breach has even been discovered. Anomaly detection must form part of a 360-degree approach to IoT security, one that empowers companies to defend, detect and react in the face of cyberthreats

***Anomaly detection provides visibility into IoT devices and solutions and flags any activity that needs investigation***

According to an IBM Security/Ponemon Institute report it takes an astonishing 212 days on average to detect a data breach. All the time security compromises go undetected, damage could be done. If companies want to protect their revenue, relationships, and reputations, they cannot afford to be on the back foot when it comes to breach detection.

## What is anomaly detection?

IoT devices generally sit outside enterprises' perimeters, in unmanned environments where they can be significantly more vulnerable. Hackers could target them to take control of devices, or use them as entry points into enterprises' systems to steal data or launch ransomware attacks. They could even use compromised devices as launchpads for attacks on other connected targets. Constant vigilance is required - once a weakness has been exposed, it could be exploited further.

To mitigate the risk, IoT devices must be secured, but they must also be monitored. Anomaly detection identifies activity that wouldn't be considered normal. That could be more frequent, or higher levels of, data transmission. A temperature sensor, for example, might have something wrong if it suddenly starts sending data every hour instead of the expected twice a day. A device suddenly appearing to communicate from another country could be another indication of possible trouble.

Not all anomalies mean devices have been hacked, necessarily. A SIM may increase or cease communication for very genuine reasons and devices can simply malfunction. Either way, whether the reason is sinister or benign, companies still need to know about anomalies, and quickly. If there has been a breach, they will need to identify and isolate it to minimise any impact.

## How does anomaly detection work?

IoT security begins with defence, but it is incomplete without the ability to detect potential problems and take action should they occur.

If companies don't have visibility into their IoT devices and traffic, they won't know if they've been compromised. The solution is to know what 'normal' looks like and then monitor connected devices so anomalies can be identified.

Anomaly detection provides visibility into IoT devices and solutions and flags any activity that needs investigation. The engines are device-agnostic and work with artificial intelligence (AI) programmes to analyse data feeds and score any potential threats.

It begins with profiling IoT network baseline behaviour, setting business rules containing thresholds to instruct the AI programme so it can learn. The programme then monitors device, network traffic and application-level behaviour.

It can flag anything it detects in real-time, so that action can then be taken. That action could be automated or not, again according to the business ▶

**SPONSORED ARTICLE**


rules. It could include throttling bandwidth to stop a device communicating into the network or isolating the device within a restricted zone. Alternatively, the anomaly could be sent for review to determine probable cause and therefore what action to take.

The AI engine can also analyse anomalies to identify types of attack. These could be distributed denial-of-service (DDoS), man-in-the-middle (MiTM) attacks, or device takeovers.

## How to incorporate anomaly detection into IoT security

Too often, IoT security is thought about after solutions have been deployed. It is imperative to think about security, and anomaly detection, at the product or solution design phase. The best outcomes result from preparation, to prevent attacks ideally of course, but also to detect and react to them should they occur.

Fortunately, anomaly detection is service based, so it is fully scalable according to the size and scope of an IoT project's initial deployment and growth over time. It can work for a single device or fleet, system wide. By working with automation, anomaly detection helps companies cost-manage and react in a timely way because they are not constrained by over-dependence on labour-hungry manual tasks.

It is important to stress again that anomaly detection is only one part of the security puzzle. It must form part of a 360-degree security model, made up of technology capabilities, standards and best practice that work together to defend, detect and react to cyber threats.

The IoT security threat landscape evolves constantly so all companies, even those who have already adopted best practices, must maintain both defensive and active measures to mitigate risks across their IoT device fleets, communications networks, data and application layers.

There are many threats to counteract including ransomware, malware, device spoofing and MiTM attacks. Companies must protect themselves against the safety, operational, financial and reputational damage that can arise from security breaches.

For these reasons, IoT security must leave nothing to chance. Companies must manage their IoT solutions' attack surfaces to prevent unauthorised access to data, systems or devices and protect them from compromise. In this, defence is only part of the complete security picture. Detection is a second layer, whereby devices and network behaviour are monitored to spot anything out of the ordinary.

After detection, comes the capability to react, which includes quarantining and cleaning affected devices, reporting breaches and anomalies and applying corrective actions across systems. All aspects of defence, detection and reaction must be planned, understood, practised and maintained for companies to be fully equipped to face the risks that threaten their IoT solutions. ■

***Too often, IoT security is thought about after solutions have been deployed***

**www.wirelesslogic.com**

# TRANSFORMA INSIGHTS

## Global Advisors on IoT, AI and Digital Transformation

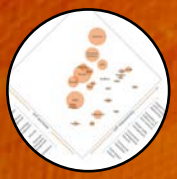
# Transforma Insights can increase your revenue, reduce your costs, and limit your exposure to risk

# 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.

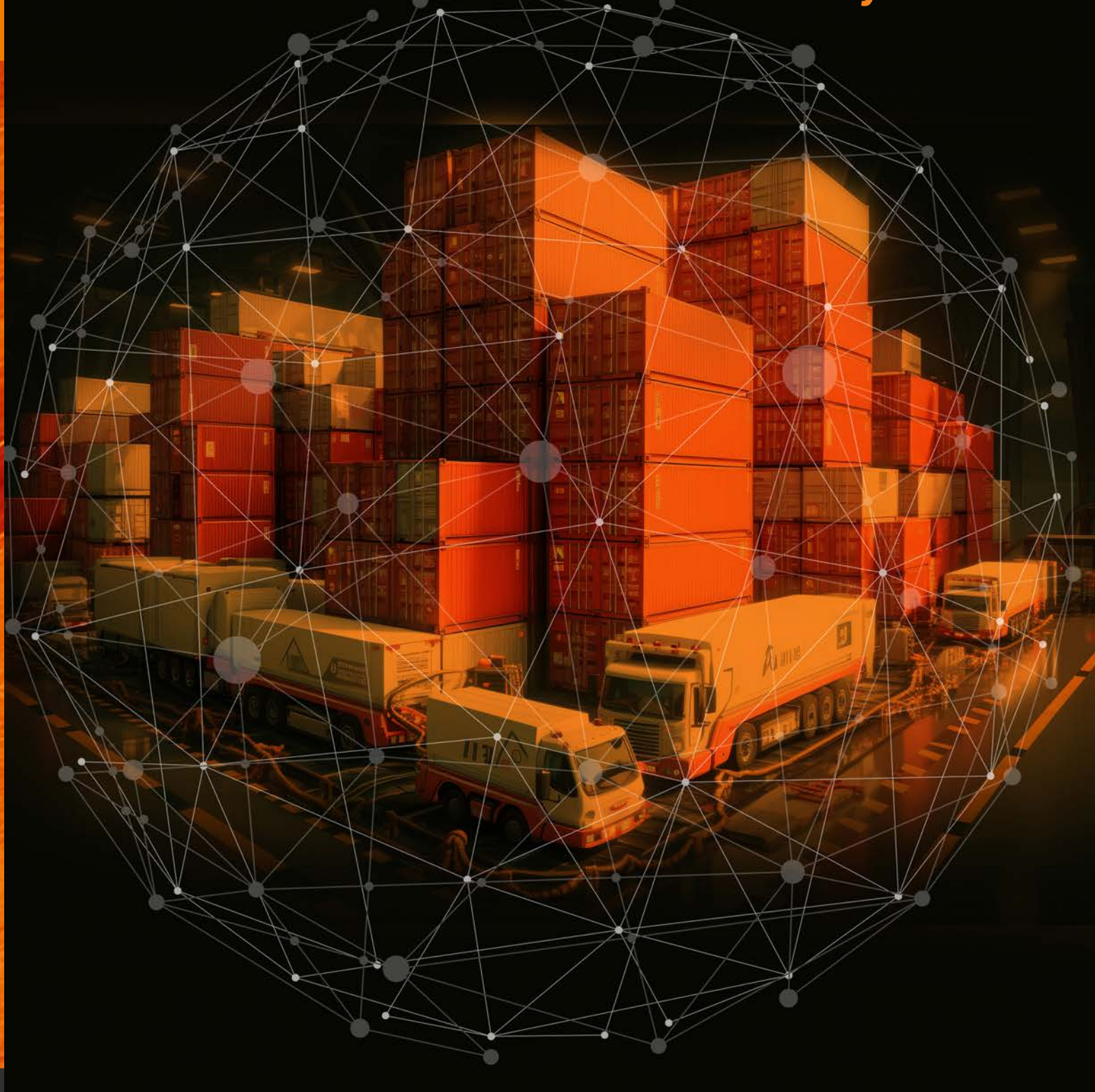
### Our tracking of the complexities of the rapidly evolving regulatory environment mean your risks are mitigated

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

# Increased transport and logistics complexity demands simpler, faster and easier cellular connectivity



Report sponsor:

KORE®

# Increased transport and logistics complexity demands simpler, faster and easier cellular connectivity

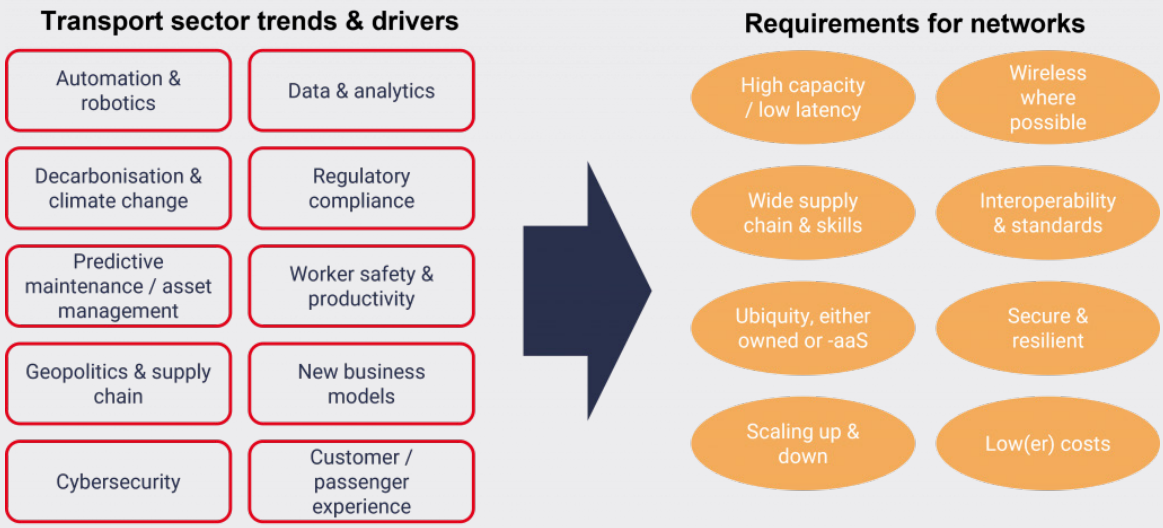
The near-ubiquitous availability of robust, secure, wireless connectivity still involves navigating substantial complexities for service providers. In the transportation and logistics sector, service providers are faced with the need to connect not only the vehicles in their fleets but also the loads being transported. Increasingly, these include the ability to connect the load and its contents including pallets, large objects, assets in transit and even parcels. Although connectivity options are available in both the low power wide area (LPWA) network arena and with global navigation satellite system (GNSS) connections, cellular connectivity provides an optimal solution for the transport and logistics sector, for most applications, most of the time.

This whitepaper therefore focuses on the applications of cellular connectivity in fleet vehicles and the items they transport. Cellular sits in the sweet spot between cost, coverage, security and reliability that transport service providers require from their connectivity. The challenge today is to achieve cellular connections with the minimum of friction, allowing automated provisioning, greater flexibility and maximised choice. Simultaneously, the switch to 4G and 5G, caused by the sunsetting of 2G and 3G networks, must be handled smoothly to avoid disruption and avoid unnecessary costs

The transport and logistics sector has been an early adopter of Internet of Things (IoT) technology to help increase efficiency and to serve customers better. The sector has seen the value of rolling-out management systems and augmented these with connectivity. Since the 1980s, large transport and logistics providers have used transport management systems (TMS) which help them to plan, execute and optimise how physical goods are moved. Adoption of these systems continues but the richness of data they now rely on has increased enormously as vehicles, packages and containers can communicate not only their locations but also information such as shock, temperature and moisture.

Analyst firm **Berg Insight** estimates that the value of the European TMS market reached around US$1.16 billion in 2022. Growing at a compound annual growth rate (CAGR) of 11.4%, the market value of transport management systems in Europe is forecast to reach US$1.89 billion in 2027. The North American TMS market is at the same time predicted to grow from US$1.47 billion in 2022 to reach almost US$2.42 billion in 2027, representing a CAGR of 10.6%. ▶

**Figure 1:** Trends driving transport sector performance improvements




Source: STL Partners

Specific sub-sections of the transport and logistics sector have been quick to adopt IoT technologies to support high value and sensitive cargo. **ABI Research** reports that the global pharmaceutical industry, for example, will surpass US$1.9 trillion in revenues by 2027 and online pharma revenues will surpass US$185 billion by 2027. With online healthcare, tailored medicines and regulatory stringency all increasing alongside an elevated focus on drug supply security following the Covid-19 pandemic, pharma supply chains have drawn considerable attention.

Digital transformations are being used to ensure not only resilient supply but also to enable competitive differentiation. As a consequence of this, the analyst firm predicts that cold chain track and trace revenue for refrigerated containers in the pharma industry is expected to reach US$2.9 billion globally by 2027 as companies look to tackle the US$35 billion worth of products lost to failures in temperature-controlled logistics within the industry each year.

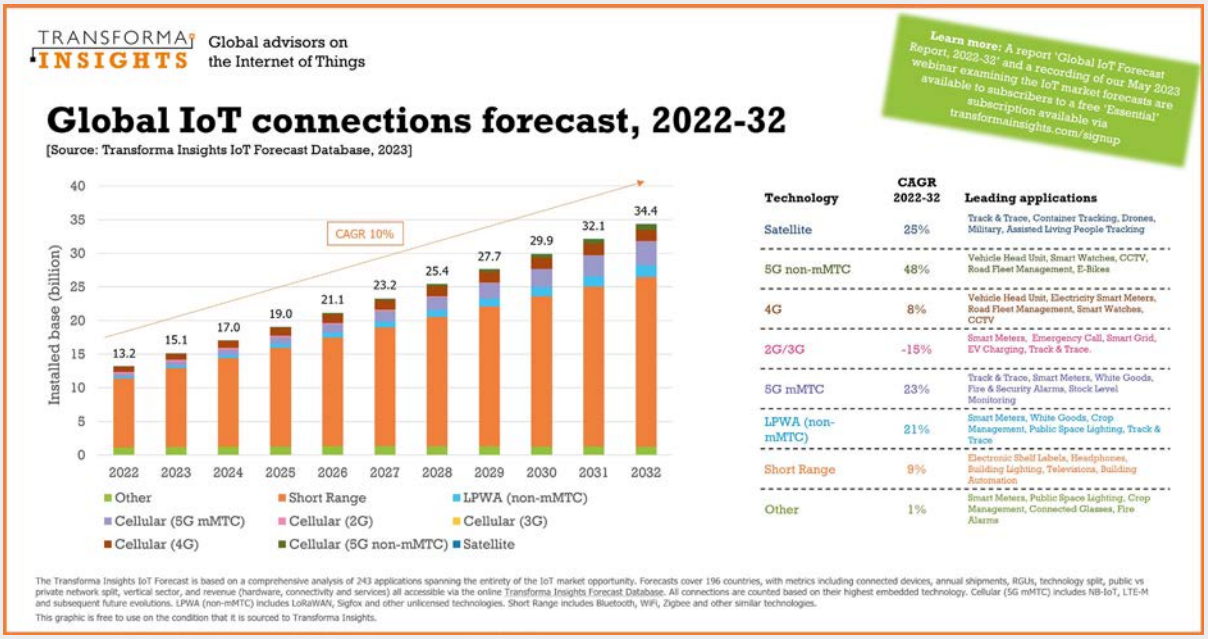
It's not only the pharmaceutical industry that is pioneering adoption of new technologies to streamline logistics performance. **STL Partners** has detailed some of the key trends enabling the next generation of transport and logistics in a recent report. The firm highlights automation and robotics which are being deployed in transport hubs and warehouses to enable greater efficiency. This extends further to port cranes, supply chain handling systems and the utilisation of automated guided vehicles.

Robots and automated systems are increasingly using video cameras for detecting packages and to enable remote control by operators. The firm says that transport and logistics companies are at the forefront of data-rich applications which range from digital twins of jet engines, wind turbines and rail locomotives, to optimised scheduling and packaging of goods in warehouses. Better-connectivity underpins progress and connected equipment, IoT sensors and video input can improve turnaround times, reduce shipment errors and lower energy consumption.

A key driver behind investment in connected systems is that transport service providers are in a capital-intensive sector. The cost of downtime for a vehicle or critical system in a warehouse or airport terminal can be huge. STL Partners therefore identifies a large opportunity for using networked information and sensors to enable predictive maintenance.

The advanced uptake of technologies enabled by connectivity in the transport and logistics sector will see transport service providers overshadowed as ▶

**Figure 2:** Connection forecasts for an IoT enabled world




Source: Transforma Insights

innovators as IoT applications are adopted at mass scale by consumers. Analyst firm **Transforma Insights** predicts that in 2032 the consumer sector will account for 61% of all connections. Of the enterprise segment in 2032, 30% of devices will be accounted for by cross-vertical use cases such as generic track-and-trace, office equipment and fleet vehicles, 26% by utilities, most prominently smart meters, 22% by retail and wholesale, 8% by government, 4% by transport and storage, and 2% each for agriculture, forestry and fishing, finance and insurance, and manufacturing.

While the market matures in this way, it's clear that cellular connections will be adopted for non-short range scenarios. Inevitably, as 2G and 3G networks continue to be sunset, 4G and 5G will step in to fill the gap, continuing to deliver ubiquitous, secure, wireless connectivity with more than adequate capacity and latency for transport and logistics use cases.

Later in this decade, the performance of newer-generation cellular connectivity is likely to have stronger relevance to transport and logistics applications as richer data is required and video is increasingly used to enable robots and support in-depth condition monitoring. The vehicles themselves will become ever-more connected according to **Kaleido Intelligence** which predicts that telematics connections will reach 573 million subscriptions by 2028.

The firm acknowledges that telematics applications won't use the same volume of data as infotainment systems but expects data rates to grow. It says the average data rate per connection is set to grow by 47% between 2023 and 2028, as the use of video telematics becomes more common in road haulage fleets. This will double telematics connectivity revenue over the same period.

The firm also notes that although direct tracking of cargo by cellular means is becoming more common, connections will grow at less than 9% CAGR throughout the forecast period. 2G and 3G shutdowns in several countries are a significant contributing factor to this relatively low growth rate. Logistics firms and suppliers will need to adopt LTE-based tracking, and the cost of replacement of older equipment will be prohibitive in many cases. As a result, Kaleido Intelligence expects less than 40 million cargo tracking cellular connections to be in place by 2028.

A key consideration for transport and logistics organisations today is how to future-proof their technology selects and ensure they have maximised flexibility to power through the sunsets and into the 5G era. 4G in the form of LTE and LTE-Advanced will be popular enabling technologies with operators intending to continue to offer 4G for the foreseeable future.

## What has changed?

Transport and logistics has surfed a wave of radically increased volumes of shipments and logistics and now encompasses several quite different activities. ▶

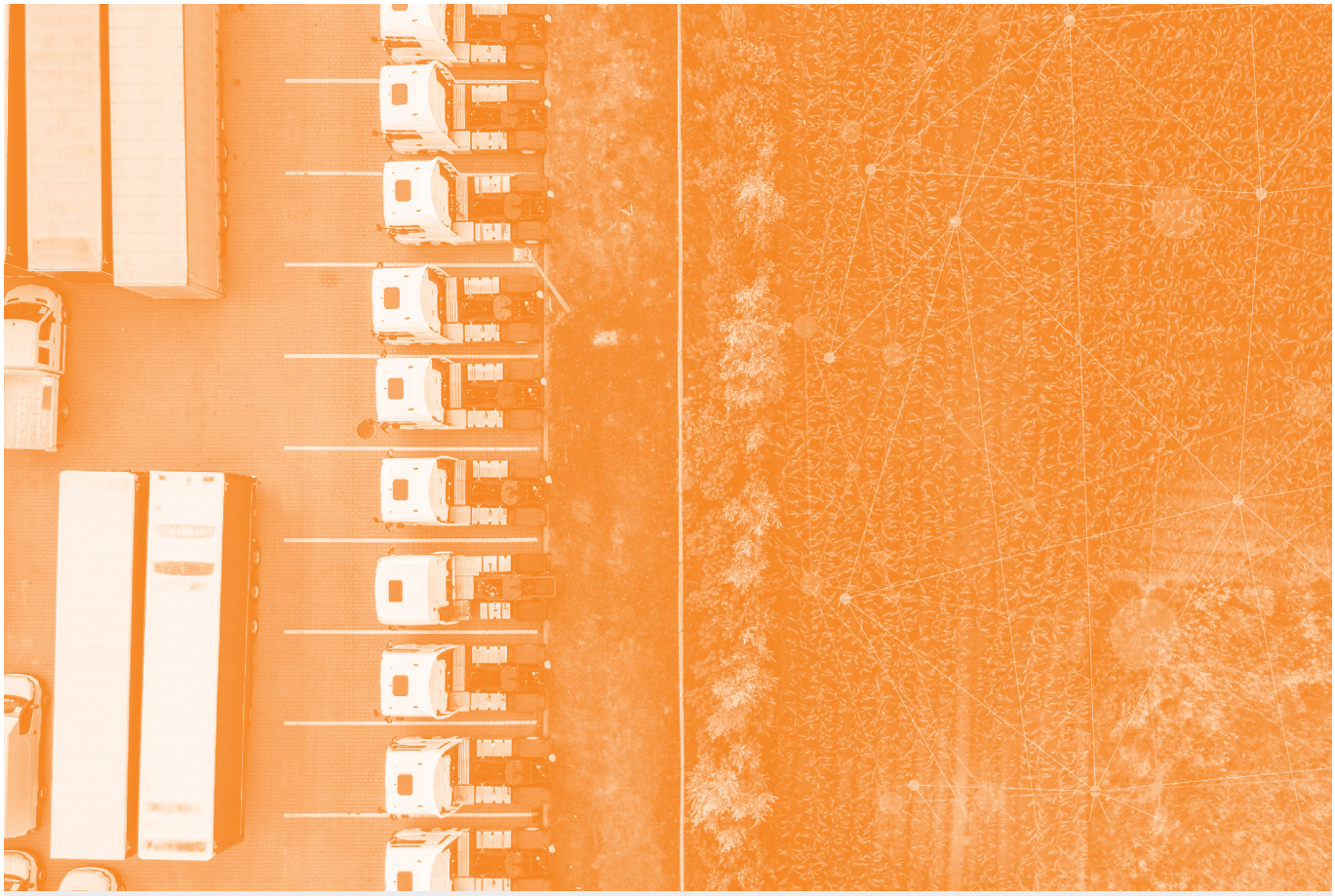
Last mile deliveries for example are very different from shipping twenty-foot equivalent (TFE) containers around the globe or ensuring foodstuffs don't spoil in refrigerated transport. To maintain customer satisfaction and be ready for greater demand, organisations are transforming their operations to take advantage of new opportunities and address customers' needs. There are three significant drivers transforming the sector:

**i. User expectation**
End users now expect to be able to track their shipments in transit and gain accurate information on demand. Service providers similarly need timely, accurate location data to support their services. Cold chain or pharmaceutical deliveries, for example, rely on the transport service provider being able to prove the products have been delivered within an acceptable temperature range and timescale. Users are familiar with tracking dongles in the consumer market and expect to have at least the same functionality available for their goods in transit. Users also have the expectation that their service providers will minimise their environmental impact, so being able to demonstrate minimised emissions through route optimisation and vehicle efficiency is now part of the business of transport and logistics.

**ii. eSIM and eUICC**
Embedded SIM (eSIM) and embedded universal integrated circuit cards (eUICC) enable SIM functionality to be installed into devices at the point of manufacture so a global SIM can then initiate its own connection – known as bootstrapping – at the point of deployment. This means vehicle manufacturers, and the retrofit market, can ship global products with a single stock-keeping unit (SKU) designation. For transport providers this means their devices can turn on and automatically connect to the best available operator regardless of their location. This decouples the connection from the local mobile operator so organisations aren't locked-in to contracts and have the ability to switch operators if coverage is poor or, with the 2G and 3G sunset, terminated. There's no need to replace a physical SIM so money is saved and flexibility and scalability enhanced.

**iii. Network performance**
With the arrival of 5G and various categories of 4G, cellular connections now offer high-speed throughput alongside resilience and security. For many basic tracking apps, this capability isn't needed or affordable but, for higher value shipments, the ability to continuously track and monitor is a monetizable business opportunity. At the lower end offerings such as narrowband-IoT and LTE Cat 1 bis, offer ample capacity to enable simpler transport and logistics functions.

These three dynamics have come together to enable a new degree of data transmission for the transport and logistics industry. This extends from connectivity in vehicles and also retrofitted equipment down to advances in sensor technology which can monitor temperature, shock and velocity while also tracking location down to the centimetre level, if required. ▶



## Future-proofing transport and logistics

The sheer volume of shipments demands greater management and connectivity simplification. Logistics providers can't manage hundreds of relationships with different network providers, they need to simplify and automate to handle the scale and deal with the potentially very short lifespans of connections, which may exist only for the life of a single shipment or an adhesive label on a parcel.

In support, solutions need to accommodate greater intelligence to process useful data and send only relevant information for consumption. This might involve the richer insights detailed earlier or confirmation that an EV has been used for a delivery.

## How KORE Wireless helps

**KORE** has been at the heart of delivering connectivity to IoT organisations of all types since the dawn of IoT. It currently covers more than 200 companies via relationships within excess of 500 carriers and sells its offerings to telematics equipment OEMs as well as transport and logistics service providers and their technology providers. The company offers a comprehensive range of connectivity and connectivity-as-a-service offerings which are augmented by its sector-specific offerings and its management platforms which include the KORE One Platform.

In the transport and logistics sector specifically, KORE has offerings that enable critical asset and cold chain monitoring, container tracking and reusable transport asset tracking. This portfolio encompasses managed services for visibility and traceability with actionable data that can help bring together the disparate elements of the fragmented global logistics sector.

The company's innovative capabilities have enabled it to harness the potential of new developments such as eSIM and eUICC. For example, when **AT&T** and **Verizon** in the US announced their plans to retire 3G, eSIM would have enabled organisations to switch to the remaining 3G networks in that area, potentially enabling 10 months or more of additional usage by a device. This flexibility is important and, while Verizon has committed to LTE until 2030, changes in coverage and capacity availability continuously impact IoT applications. The ability to be able to switch to the best available network to support a business case is fundamental to the business success of IoT.

As fleets shift and electrify, further complexity is added and systems will be needed to manage the charging demands of vehicles. It is, however, unlikely that large trucks will turn to electrical power exclusively in the short to medium term but customers will want to be assured that environmental impact associated with their shipments is being minimised and this will need to backed up with data collected by advanced systems. ▶

For transport and logistics organisations, KORE's ability to provide multi-carrier connectivity ensures optimised coverage without the headache of having a customer organisation manage multiple carrier relationships in all the markets it operates in. KORE's platforms automate and simplify management and operations vastly cutting the need for manual network tasks to be completed and freeing up resources for other activities. The diversity of KORE's network footprint means customers can manage their global deployments and scale up or down easily with KORE as their one network.

A further benefit is that KORE is technology agnostic and is able to provide narrowband-IoT, LTE-M and LoRaWAN, in addition to 4G and 5G networks, to support low-power IoT devices and to ensure maximised redundancy and failover options in the event of network outages. This is a significant contrast to services provided by a global carrier which, regardless of the size of the carrier, will be delivered using a patchwork of preferred partners who are often in a position to shift blame amongst themselves and create obstructions to efficient service management. Global carriers simply can't offer the optimum coverage and capacity for every application in every market in the world through their relationships.

KORE's aim is to abstract the complexity and fragmentation of global connectivity away from customers so they can focus on their core business of service delivery and customer satisfaction. KORE has designed its coverage, management and service offerings to achieve this and free up IoT companies in all industries to focus on their innovations, not the network connectivity.

## Conclusion

Tracking and monitoring in the transport and logistics sector is already experiencing massive growth as transport service providers aim to meet customers' expectations and, in some cases, exceed them. This is not simply a situation of straightforward growing pains, companies need to simultaneously connect to add greater richness to the customer experience, handle the transition to EVs and enable the secure and resilient flow of service-centric data.

With the increase in scale to mass-market size, all of this must be automated and simplified so old approaches can't be replicated. The market needs the flexible, global, secure connectivity that cellular provides and KORE is making that simple to access, deploy and utilise. ■

# Achieve operational excellence by using digital manufacturing

Manufacturing will be transforming faster than ever before in the next few years, writes Guy Denis, business development, Bosch Software and Digital Solutions. As the ninth largest manufacturing nation by the value of GDP, the UK still has global reach and impact. Manufacturers have a desire for change, to reap the benefits of digitalisation and Industry 4.0 and to evolve traditional manufacturing with adaptive, flexible manufacturing. This trend is supported by a recent research report, which found that 96% of companies are using at least one next-generation technology

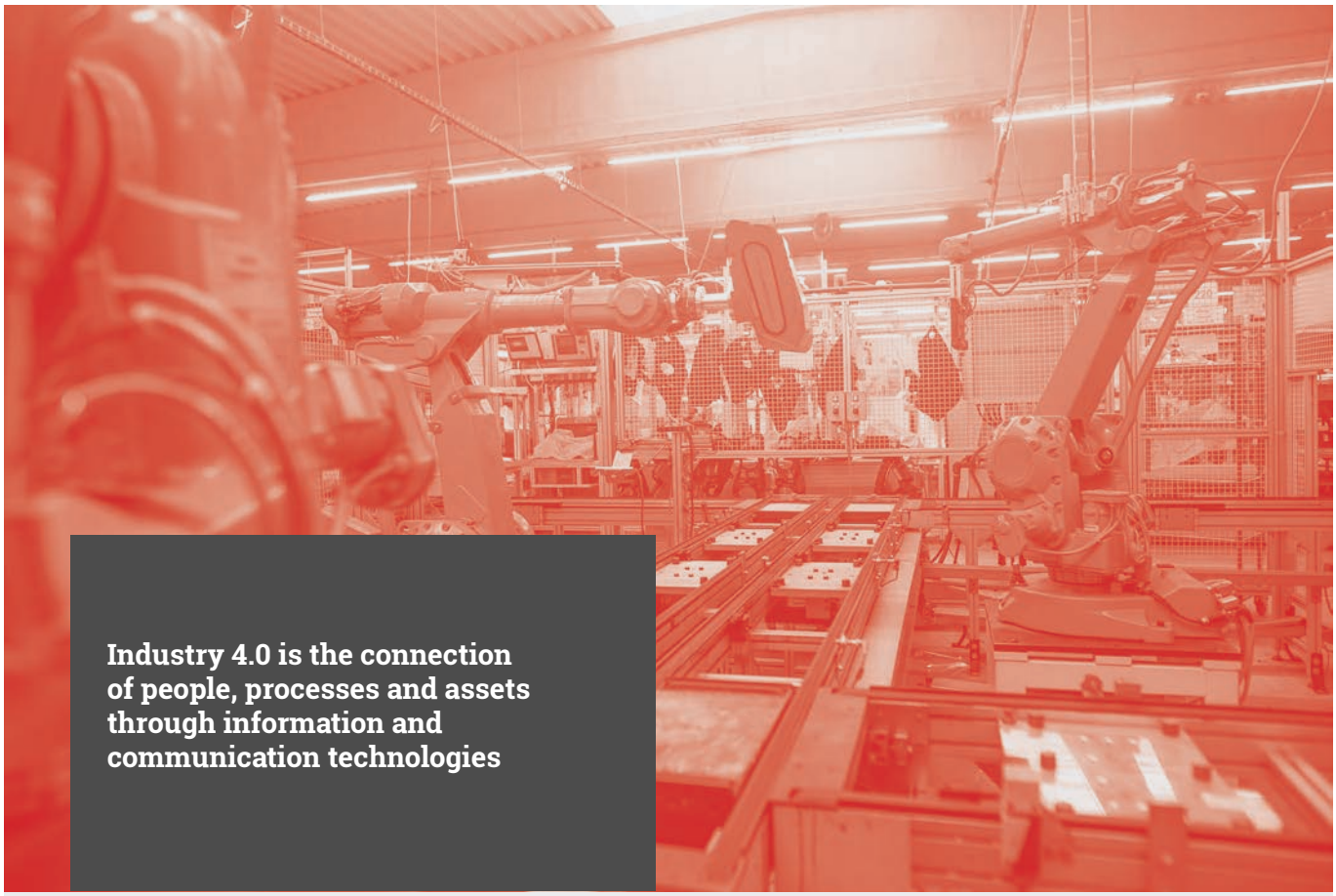
Multiple challenges face UK manufacturing and are driving necessary change. For example, with rising costs and depleting reserves, energy optimisation is a critical focus for manufacturers. An overdependency on non-UK sources is also a factor and many companies are rapidly adapting to use other localised power sources like renewables.

## Necessity is the mother of invention

Bosch is working closely with leading UK manufacturers to enable their adoption of this rapidly changing technology landscape in order to benefit from Industry 4.0 and IoT, as well as to offset some of the issues created by a global marketplace. Some of the key areas of involvement include:

- **Modernisation and investment** - Manufacturing has been slow to adopt technologies that would enable competitiveness, agility, flexibility, market leadership and future-proofing.
- **Workforce challenges** - A talent shortage combined with the loss of experienced workers (over 50s) has created a void. Younger Generation Z workforce skills in coding and gaming technology are not being made use of or sufficiently recognised as potential assets. For reference, the vacancy rate in the manufacturing sector is the highest ever since Office of National Statistics (ONS) records began, standing at 3.7% in October 2021 (vs an average of 1.8%). ▶

SPONSORED ARTICLE



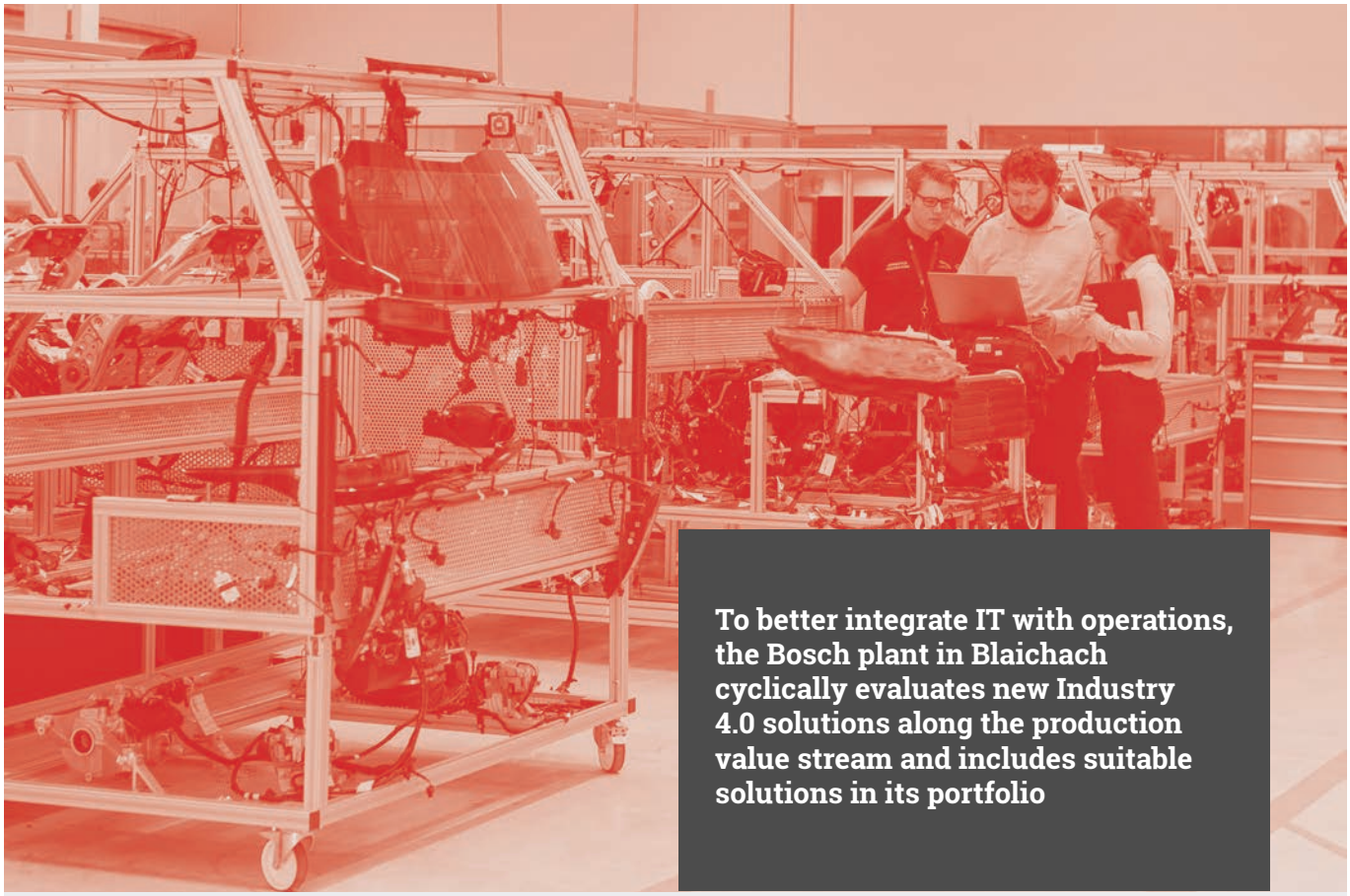
**Industry 4.0 is the connection of people, processes and assets through information and communication technologies**

- **Lack of integration between IT and operations** - This results in stranded assets, manual dependency, low productivity, poor quality and overcomplicated processes.
- **Overextended assets** - Machinery and equipment are being used beyond their planned operational lifecycle and the adoption of new automation, robots and drones has been slow.
- **Overdependency on offshore investment** - Depending on non-UK corporate HQs such as **Ford** from the US, **Nestle** in Switzerland and **Toyota** of Japan, leaves local manufacturers in a potentially vulnerable position.
- **Cost of manufacturing** - Manufacturing costs in the UK are comparatively higher than in other regions and nearshore alternatives like the Czech Republic.
- **Brexit impact** - The impact on supply chains, cost of raw materials, import duties, workforce access, export order book and investor confidence continues to present issues.
- **Covid impact** – Continues to present challenges in supply chains, R&D and production.
- **Changing PESTLE landscape** – The Ukraine war has created a rapidly changing environment, disrupting the movement and accessibility of raw materials and goods.
- **Evolving technologies** – The pace at which technologies are evolving is a challenge to keep up with, for example, the development of hydrogen engines.
- **Consumer-driven market dynamics** – Keeping current with new trends from consumers such as mass customisation, healthier eating and environmentally-friendly products.

## The role of digitalisation and Industry 4.0

Industry 4.0 is the connection of people, processes and assets through information and communication technologies. Implementing intelligent solutions in production and logistics enables optimisation within factories and ultimately improves competitiveness in manufacturing. By embedding advanced data-generating and processing software into production facilities, organisations can evolve into smart connected factories. This increases productivity, quality and energy efficiency while helping to develop value-added, outcome-based measurable results and creates new, profitable business models toward sustainable manufacturing.

Manufacturers are at different stages of digitalisation adoption and development. Some are yet to start and as a result, Industry 4.0 standardisation can be difficult to implement. For example, many UK manufacturers have multiple vendors for equipment, automation systems and software which inflicts a heavy burden on time, money, ▶



**To better integrate IT with operations, the Bosch plant in Blaichach cyclically evaluates new Industry 4.0 solutions along the production value stream and includes suitable solutions in its portfolio**

productivity and quality in supporting the operation of non-standardised systems.

There has been a long-term sector-wide lack of sharing best practices among manufacturing companies, despite there being much to learn from each other. With this in mind, Bosch has undergone a programme of connecting its own 270 factories and 700 warehouses worldwide first, with the aim of sharing proven practical experience with customers following successful validation. Some of the key areas where Bosch has demonstrable proof points include:

## Energy management

Sustainability is a common agenda and challenge within the sector with several manufacturers making the statement to be completely carbon neutral by 2030 globally despite huge legacy issues. Tracking and visualisation of energy usage within a factory including intelligent algorithms to lower energy costs is a way how the Bosch plant in Homburg has reduced energy costs by about €12 million with a total amortisation time of under 1.5 years.

## Human-robot collaboration

As an example, the UK adoption of automation, robot and drone technology has been relatively slow. Greater use of automation enables companies to increase productivity as well as speed up the production process, resulting in significant cost savings. This has been applied in Bosch's Nuremberg plant where collaborative robots have been implemented to combine human capabilities alongside the robot's strengths such as precision, power, speed and repeatability.

## Production improvement

To better integrate IT with operations, the Bosch plant in Blaichach cyclically evaluates new Industry 4.0 solutions along the production value stream and includes suitable solutions in its portfolio. The application supplements existing solutions with respect to the visualisation and evaluation of real-time data. This results in full transparency, increased efficiency and cost savings.

## The future of manufacturing

Example operational benefits like 90% lower expenditure over manual data collection and a 15% increase in productivity, make it clear that Industry 4.0 brings measurable success and solutions to manufacturing sector challenges. Industry 4.0 is here, is real, and if organisations come together to define and apply Industry 4.0 concepts processes and standards it will be to the advantage of all.

Bosch benefits from its own experience in numerous use cases and will be happy to share. ▶

**Bosch acquired Protec Fire & Security. The company's innovative product portfolio and services are used in numerous sectors**

## Globally, the UK is Bosch's fourth largest market and is its second largest within Europe, after Germany

**Recent investments in the UK and Ireland include:**

August 2021: Bosch opened its Automotive Research & Development Centre in Limerick, Ireland. The focus of the activities in Limerick will be on state-of-the-art automotive electronics, for example the centre will develop Advanced Driver Assistance Systems (ADAS) such as Automatic Emergency Braking, as well as the radar sensors and semiconductors that are needed to bring this technology to new cars around the world.

September 2021: Bosch subsidiary **ETAS** opened its Centre of Excellence for Embedded Software in York. This is an extension of the existing ETAS facility and represents a £1.6 million (€1.8 million) investment. The expanded centre will develop the middleware that will power future generations of advanced autonomous and highly automated vehicles. It will contribute to the realisation of Bosch and ETAS's vision of accident-free driving around the world.

November 2021: Bosch acquired **Protec Fire & Security**. The company's innovative product portfolio and services are used in numerous sectors, for example in industry, airports and railway stations, and will strengthen the European business for fire detection in Bosch Building Technologies Sector. Protec employs around 1,100 people and had a turnover of around £125 million (€142 million) in 2021.

April 2022: Bosch announced it will acquire **Five**, the start-up that specialises in autonomous driving. Five's technology will complement Bosch's existing automated driving expertise and the two companies share a common vision of automated driving and of safe automated driving systems. The acquisition of Five is subject to regulatory approval.

April 2022: Bosch UK announced its acquisition of a new office building within Broadwater Park in Denham. Bosch UK's headquarters have been based at Broadwater Park since 1984 and it has now acquired the whole site. Bosch will move multiple divisions into the new office once it has been refitted to include the latest Bosch technology, which will ensure it has high levels of energy efficiency and is wholly sustainable. Bosch's 400 locations all around the world, including in the UK, have been net zero since 2020.

**www.bosch-softwaretechnologies.com**


# The IoT Tech Expo Global 2023: Shaping the future of connectivity

The world of technology is evolving at a remarkable pace, with the Internet of Things (IoT) standing at the forefront of this rapid transformation. IoT, the interconnection of physical devices through the internet, is an ever-expanding realm of innovation that promises to revolutionise industries, improve efficiency and enhance our daily lives. One of the most anticipated events in the IoT domain, the IoT Tech Expo Global, is set to take place on 30 November – 1 December 2023 at the iconic Olympia London, UK. This two-day event is not just a gathering of tech enthusiasts; it's a celebration of how IoT technology is advancing and changing the world

Following the record-breaking Amsterdam edition of the event that took place in September, the organisers are eagerly anticipating another bustling and successful gathering. The overwhelming success of the previous event, which attracted a record number of attendees and featured groundbreaking insights and innovations, has set a high standard to maintain. With the continued growth and dynamism of the tech industry, there is every reason to believe that the upcoming event will once again be a hive of activity, bringing together thought leaders, innovators and enthusiasts keen to explore the latest trends and developments in the world of technology. The anticipation is high, and the organisers are fully committed to delivering yet another event that not only meets but exceeds the expectations of the tech community.

## The speed of IoT advancement

IoT technology is developing at an unprecedented rate. Every day, new devices and systems are connected to the internet, generating vast amounts of data and enabling businesses and individuals to make informed decisions like never before. The rapid pace of innovation in this field is a testament to the boundless potential of IoT. At the IoT Tech Expo Global, attendees will have the opportunity to witness the latest breakthroughs, explore cutting-edge solutions, and gain insights into the future of IoT technology.

## London: The perfect host for IoT Tech Expo Global

London, a city steeped in history and renowned for its diverse culture, is a fitting host for an event of this magnitude. With a rich tech ecosystem and a global reputation as a hub for innovation, London is the ideal backdrop for an expo dedicated to IoT. The city's strategic location, well-connected transport systems, and vibrant tech community make it an inviting destination for both international and local attendees. The IoT Tech Expo Global in London is not just an event; it's an experience that combines the excitement of technology with the allure of a world-class city. ▶

## Distinguished speakers

The IoT Tech Expo Global presents an extraordinary assembly of speakers, each a recognised luminary in the dynamic realm of Internet of Things (IoT). These influential thought leaders have harnessed their extensive knowledge and hands-on expertise to illuminate the multifaceted landscape of IoT technology. By generously sharing their profound insights and invaluable experiences, they are poised to provide attendees with a comprehensive understanding of the ever-evolving present and the promising future awaiting the IoT industry. Speakers include:

**Jamie Stapleton**, vice president of Global Digital Strategy at Hitachi Energy

**Agata Grela**, digital strategy leader at RBS International

**Barbara Gunter**, transformation director at DHL

**Jesper Toubøl**, vice president of Operations at Lego

**Vaia Sdralia**, head of IoT Product Portfolio at Vodafone

**Anubhav Banerjee**, chief technology officer at Allianz

**Yatin Pahwa**, global head - IoT Product and Portfolio Management at Vodafone

**Anu Widyalankara**, director of Payments Strategy and Technology at EY

**George Floros**, head of GIS - Infrastructure at Skanska

**Emily Collier**, technology director at TUI

**Goldy Samra**, technology platform director - Digital at Lloyds Banking Group

**Ghulam Rasool**, transformation lead at Ford

**Marlon Wilson**, Transformation, Change, and Inclusion manager at BT Group

**Oleg Polovynko**, CIO at Kyiv City Council

**Hiliana Fienieg**, global director - Retail Brand Information Solutions at Avery Dennison

**Anna Brailsford**, CEO and co-founder of Code First Girls

**Matt Hatton**, founding partner at Transforma Insights

**Guy Denis**, industrial business development manager at Bosch Software and Digital Solutions

This diverse group of speakers represents various sectors and industries, providing a holistic view of how IoT is transforming businesses and improving our daily lives.

## Co-located events

The IoT Tech Expo Global isn't just a solo act; it's a tech forum that brings together a variety of significant tech events, making it a complete tech experience. Here are some of the co-located events:

**Cyber Security & Cloud Expo:** This one's all about keeping things secure in the digital realm. Learn how to protect your data and navigate the cloud computing landscape.

**AI & Big Data Expo:** Dive into the world of artificial intelligence and big data. See how these technologies are changing the game and impacting various industries.

**Digital Transformation Week:** Embrace the digital age and learn how organizations are evolving to keep up with the times.

**Blockchain Expo:** Explore the fascinating world of blockchain, its real-world applications, and its potential to disrupt different industries.

**Edge Computing:** Delve into the cutting-edge realm of edge computing, where data processing happens closer to the data source. Learn how this revolutionary technology is redefining data analysis and decision-making in real-time, particularly in industries where low latency and immediate responses are critical.

**Intelligent Automation Expo:** Get ahead of the curve in automation. Discover the latest in robotics, machine learning, and intelligent process automation.

With all these co-located events, the IoT Tech Expo Global isn't just a one-stop-shop for IoT; it's a tech bonanza that lets you explore a wide range of cutting-edge technologies. It's the perfect opportunity to expand your tech knowledge and see how various fields are shaping the future.

The Intelligent Automation Expo is a highlight of the 2023 edition of IoT Tech Expo Global, as it marks the first time this event is taking place as a co-located event. Intelligent Automation is a dynamic field that combines AI, machine learning, and robotic process automation to enhance business processes and productivity. It is an essential component in the era of digital transformation, and its inclusion in the IoT Tech Expo Global demonstrates the growing importance of automation in the IoT ecosystem. ▶

## Ticket Types

There are three ticket types available for the IoT Tech Expo Global:

**Free Ticket:** This ticket provides access to the expo floor and free presentations.

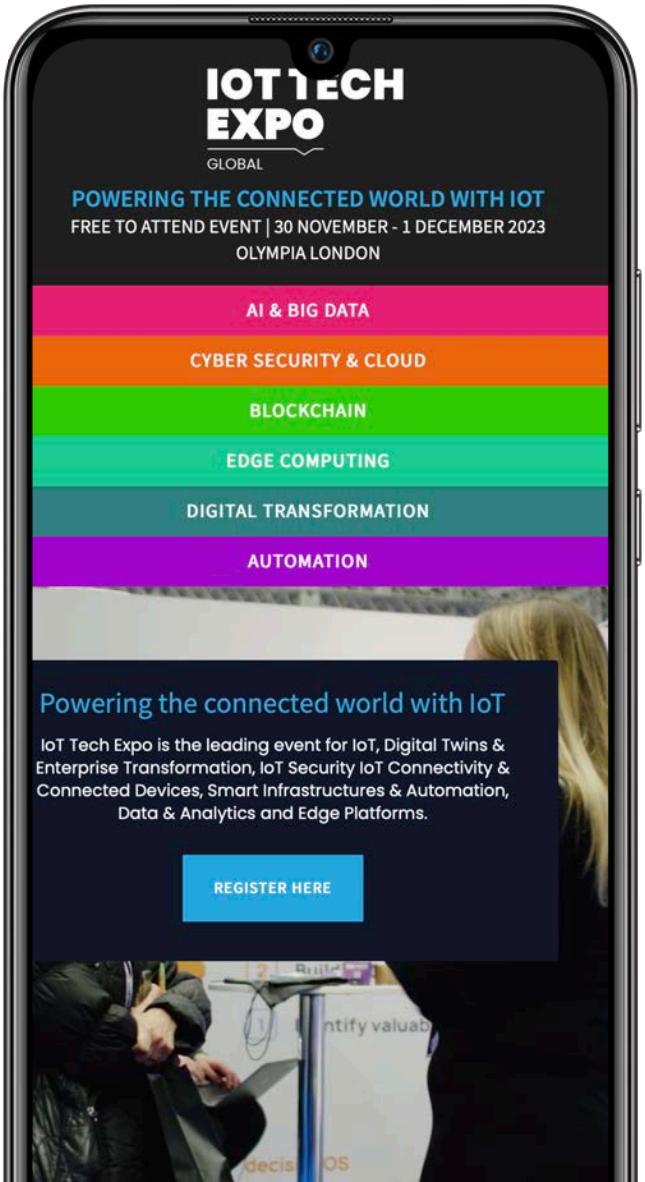
**Gold Ticket:** The Gold ticket offers access to everything included in the Free Ticket, along with access to paid IoT Tracks, VIP Networking Party and the Networking app.

**Ultimate Ticket:** The Ultimate Ticket provides access to everything included with the Gold Ticket, as well as all paid tracks from the co-located events.

## VIP Networking Party

At the IoT Tech Expo Global, don't miss the VIP Networking Party – it's a real highlight! This exclusive event is your chance to meet and connect with like-minded professionals, potential business partners, and industry leaders. It's all about networking, collaboration, and making valuable connections. The VIP Networking Party is open to Gold and Ultimate pass holders, exhibitors, speakers, and members of the press. Just make sure you have your badge ready for entry.

This fantastic event will be hosted at the Prince Pub, a cozy and friendly venue right in the heart of the city. The Prince Pub is known for its warm and inviting atmosphere, perfect for a night of networking and great conversations. With comfy seating, delicious refreshments, and a welcoming vibe, it's the ideal place to build connections and enjoy your evening.




## Networking app

At the IoT Tech Expo Global, an exciting addition to enhance the event experience comes in the form of a networking app. This app serves as a valuable tool for attendees, providing a comprehensive set of features designed to make the most of their event participation.

The app allows attendees to seamlessly navigate the in-person conference agenda and select sessions of particular interest, effectively curating their own personalised event schedule. Beyond simplifying schedule management, the app's primary utility lies in its networking capabilities. It enables attendees to not only view but also initiate connections and pre-plan meetings with a wide spectrum of individuals including fellow attendees, sponsors, speakers, and exhibitors.

The significance of this networking functionality is paramount. By initiating conversations and forming connections prior to the event, attendees can set the stage for meaningful in-person interactions. This, in turn, can lead to more productive discussions, more insightful knowledge sharing, and more effective business collaborations during the actual event.

In essence, the networking app offers a powerful means to enhance the value of an attendee's participation at the IoT Tech Expo Global. It serves as a bridge that facilitates the transition from virtual introductions to real-world interactions, ultimately contributing to a more productive and enjoyable event experience. ▶

## Agenda highlights

The IoT Tech Expo Global features a diverse and engaging agenda, covering a wide range of topics related to IoT technology. Some of the agenda items include:

- Staying on Track with Digital Twins
- Developing Operations with Digital Twins
- Enabling the shop floor to pave the way for productivity and sustainability
- Leveraging data for improved energy efficiency of electric motors
- Contextualized IoT data for enhanced operational excellence
- Taking Action on IoT Data Analytics
- Machine Learning for the Ultimate IIoT Infrastructure
- Digital Acceleration through the IoT
- IoT Data Handling
- Disruptive innovation at the heart of the "store of the future" at Ikea
- Transformation and Talent: Building a Tech Workforce for the Future of IoT
- Working on the Edge for Optimum Response
- The State of Edge in 2023
- The Economics of Edge – How to Ensure a Cost-Effective Transformation
- Edge Compute in Robotics and Computer Vision
- The Intersection of Edge Computing and Digital Twin
- Deep Dive Fire-Side Chat: Setting Realistic Goals and then Smashing Them
- Getting to grips with our automation objectives: Are we cost-saving, de-risking, innovating, or something else?
- Cross-industry learning: Fireside chat
- Leveraging the huge productivity potential of a successful augmented workforce
- Exploring emerging technologies and their impact on intelligent automation
- Data culture, gathering, and analytics: The essential building blocks for successful automation
- Maintaining an unbiased, fair, and ethical digital environment: Essential steps we must take as a sector on the cusp of massive change
- ŠKODA AUTOmation: From Zero to Hero
- Digital Twins as an Essential Baseline for Predictable, Scalable Automation
- Advancements and future trends in intelligent automation
- Kyiv Digital Connecting Communities in a Time of War
- Reaching Long Ranges with Satellite IoT
- Castrol Smart Monitor – IoT Innovation for Industrial and Marine Customers
- A Holistic Approach to the Connectivity Landscape
- Finding the needle in a haystack – the story of the World's smallest asset tracking IoT sensor
- Payments Technology Reshaping the World
- Examining the Current IoT Security Landscape
- Supply Chain and IoT Security Management
- Building a Robust Cyber Security Strategy, an IoT Perspective
- Data Volume & IoT Security
- The Ins and Outs of Device Security
- Keeping Patients Safe – The Role of Connected Medical Devices

As the IoT Tech Expo Global 2023 approaches, we can't help but be excited about the wealth of knowledge, innovation, and collaboration that awaits. This event is not just about technology; it's about the people who drive it, the possibilities it opens, and the connections it forges. Whether you're a seasoned professional in the IoT world or just dipping your toes into this ever-evolving landscape, this expo offers something for everyone. It's a unique opportunity to be a part of the future, to learn from the best, and to shape the path of IoT technology.

The IoT Tech Expo Global promises to be an experience like no other, a convergence of minds, and a celebration of innovation. Whether you're exploring the expo floor, attending illuminating presentations, or networking at the VIP party, this event is your gateway to the cutting edge of IoT technology.

In the digital age, where information flows at the speed of light and technology leaps forward with each passing day, the IoT Tech Expo Global stands as a beacon of progress. It's where ideas are born, partnerships are forged, and the future takes shape. Don't miss your chance to be a part of this transformative journey. Join us in London, and let's shape the future of connectivity together.

**https://www.iottechexpo.com/global/**


# Connect. Inspire. Evolve.

Enlit Europe 2023, to be held in Paris, France on 28-30 November 2023, is a constantly growing, inclusive and end-to-end forum that addresses every aspect of the energy agenda. A community that for 365-days a year collaborates and innovates to solve the most pressing issues in energy. Attend the event for the latest news, inspiring stories, insights, marketplace and virtual and live events

Enlit Europe 2023 is taking place in Paris on 28-30 November. Key features of the event include:

- 12,000 Attendees
- 700+ International Exhibitors
- 500+ Speakers
- Live Summit Sessions across 2 stages
- 9 sector-specific Hub Theatres
- 76+ EU-funded projects at The EU Projects Zone
- Innovation Festival
- Future Energy Leader Programme
- Multiple Networking and Meet & Greet opportunities

In addition, Enlit Europe 2023, will showcase the following:

**The Guide:**
Newsletter and annual print publication taking a deep dive into the people, projects and technologies shaping the energy transition.

**Enlit on the Road:**
The Enlit Team hits the road to champion innovation and connect extraordinary people across Europe.

**Energy Transitions:**
A podcast exploring the future landscape through the lenses of remarkable industry professionals.

**Industry Directory:**
Your resource for finding the best tech solutions and partners to move your business forward.

**The EU Projects Zone:**
Endorsed by the European Commission, Enlit supports the communication, dissemination, and exploitation of Europe's energy projects.

**The List:**
A monthly newsletter and podcast giving an insider's look into the world of energy projects.

**Membership:**
Make meaningful connections with people who share your passion for accelerating the energy transition.

**Get involved:**
**www.enlit.world**

Enlit Europe

# Feeling Enlit?
# Let's meet in Milan
## 22-24 October 2024

At Enlit we are on a journey to **#Connect** industries, **#Inspire** action and help Europe **#Evolve** into one decarbonised and digitalised energy system for the energy transition.

Along this journey, we have the privilege to meet extraordinary people.

People making their mark on the energy transition. **People like you!**

And although the road of the energy transition is a bumpy one, filled with challenges, uncertainties, hope, and opportunities, one thing is crystal clear:

Across borders and across sectors: our purpose - to deliver clean, affordable, and reliable energy for all - is what connects us.

The next stop on our journey is Milan on 12-14 November 2024. **In-person.** Because nothing beats meeting face-to-face.

**Join us**

**15.000 attendees**

**1000 exhibitors**

**500 speakers**

**Find out more at**
**www.enlit-europe.com**

## Our pick of IoT industry's upcoming events

Enlit Europe 2023
28-30 November 2023
Paris, France
**https://www.iot-now.com/event/enlite-europe-2023/**

London EV Show
28-30 November 2023
London, UK
**https://www.iot-now.com/event/london-ev-show/**

Smart Cities Connect
28-30 November 2023
Washington DC, USA
**https://www.iot-now.com/event/smart-cities-connect/**

IoT Talks 2023
29 November 2023
digital event
**https://www.iot-now.com/event/iot-talks-2023-through-the-iot-looking-glass/**

Cyber Security & Cloud Global
30 November – 1 December 2023
London, UK
**https://www.iot-now.com/event/cyber-security-cloud-global/**

AI & Big Data Expo
30 November – 1 December 2023
London, UK
**https://www.iot-now.com/event/ai-big-data-expo/**

Global OPEX and Business Transformation Summit
30 November – 1 December 2023
Berlin, Germany
**https://www.iot-now.com/event/global-opex-and-business-transformation-summit/**

Global Digital Transformation & Customer Experience Summit
30 November – 1 December 2023
Berlin, Germany
**https://www.iot-now.com/event/the-global-digital-transformation-customer-experience-summit/**

GIANT Health Event
4-5 December 2023
London, UK
**https://www.iot-now.com/event/giant-health-event/**

Chief Data & Analytics Officer, APEX West
5-6 December 2023
Scottsdale, Arizona, USA
**https://www.iot-now.com/event/chief-data-analytics-officer-apex-west/**

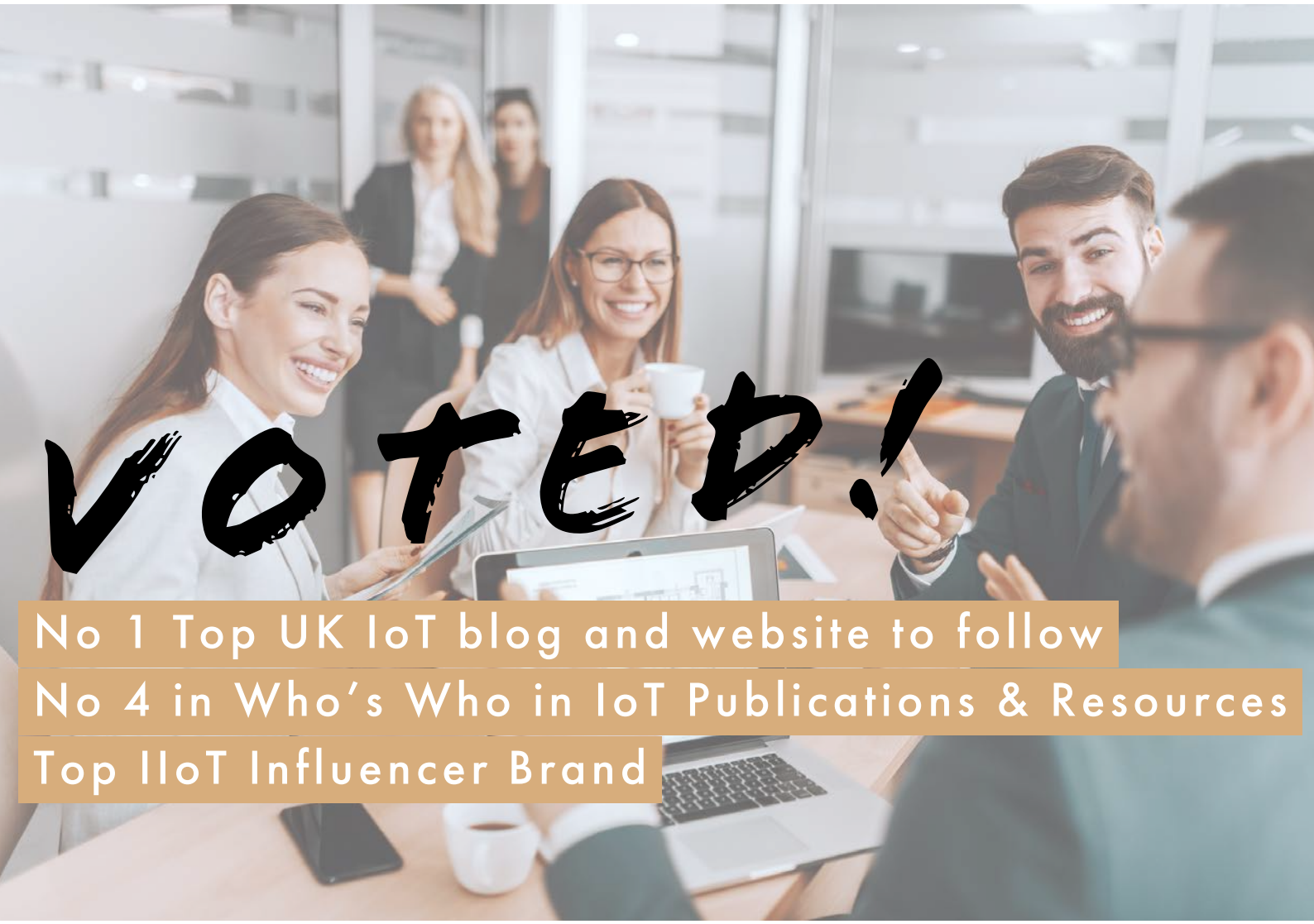
Consumer IoT Summit – CES 2024 Online Preview
6-7 December 2023
digital event
**https://www.iot-now.com/event/consumer-iot-summit-ces-2024-online-preview/**

Geo Week 2024
11-13 February 2024
Denver, Colorado, USA
**https://www.iot-now.com/event/geo-week-2024/**

London PropTech Show
27-28 February 2024
London, UK
**https://www.iot-now.com/event/london-proptech-show/**

Bosch Connected World 2024
28-29 February 2024
Berlin, Germany or online
**https://www.iot-now.com/event/bosch-connected-world-2024/**

# JOIN THE INNER CIRCLE




Launched in 2010, IoT Now is read in 100 countries by top level management, enterprise owners and decision-makers in IoT

## SUBSCRIBE NOW

www.IoT-Now.com

# Make massive IoT available to all

thalesgroup.com

THALES
Building a future we can all trust