IoT Now: ISSN 2397-2793

Q3 2022 • VOLUME 12 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

TALKING HEADS

Tele2 IoT's Cyril Deschanel explains why cellular IoT is entering a new era of sustainability, security and mass scale

INSIDE: THE IoT NOW GUIDE TO MWC LAS VEGAS 2022

tmforum dtw DIGITAL TRANSFORMATION WORLD | COPENHAGEN

DIGITAL TRANSFORMATION WORLD 2022 PREVIEW

SMART HOMES
New efficiency for living, working and playing.
See our Analyst Report at **www.iot-now.com**

HEALTHCARE
Why IoT is improving patient outcomes
See our Analyst Report at **www.iot-now.com**

UTILITIES
How IoT is enabling electricity industry transformation
Read the IoT Now Report at **www.iot-now.com**

CONNECTIVITY
Why the future is integrated
Read our iSIM report Inside this issue

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

PLUS: 7-page IoT in Manufacturing Report reveals how OEMs are driving new efficiencies • Analysts say IoT is exceeding enterprise expectations • Consolidation comes to IoT with Telit and Thales plus Semtech and Sierra Wireless deals • EV infrastructure charges ahead • European IoT market sees sustained investment • Why iSIM is the answer for micro-mobility and smart tracking • Fibocom on finding the right wireless connectivity to deliver the perfect experience • KORE goes beyond the tip of the IoT iceberg • Ikotek CEO explains the need for a US-headquartered IoT-dedicated ODM • Keeping track of tools with Nanolink • Exclusive IoT Now IoT Security Report reveals how IoT organisations will achieve security by design • News, features and interviews online at www.iot-now.com

THE FUTURE IS INTEGRATED

Be there first.

The integrated SIM (iSIM) reduces design footprint and simplifies the bill of materials, making it ideal for the next generation of connected things.

- *More compact devices*
- *Reduced Total Cost of Ownership*
- *Chip-to-cloud security for trusted data*
- *Choice of production-ready hardware*

Kigen invites you to write the next chapter of iSIM together.

Start today: kigen.com/isim

Kigen

#FutureofSIM

CONTENTS

IN THIS ISSUE

IoT hasn't become too big to fail, it's too useful for that

The deal struck by **Telit** with Thales to create **Telit Cinterion** as a new modules-to-connectivity provider, and the funds heading to Thales as a consequence, plus the US$1.2bn **Semtech** is spending to acquire **Sierra Wireless**, demonstrate that IoT is no longer a speculative punt, a market fuelled by pilot projects, most of which fail. The famous **Beecham Research** statistic of a few years ago that 75% of all IoT projects fail now needs updating as a growing proportion of IoT projects succeed

George Malim,
managing editor

Failure of course still happens but IoT is viewed much more positively today. Analyst firm **Omdia** reports that in a recent survey, 90% of enterprise respondents said that their IoT projects have met or exceeded their expectations (see full story on p.7). That's a phenomenal about turn for IoT in a period that has seen the pandemic, heightened geopolitical tension and the supply chain crisis. Perhaps these have provided IoT with a shop window through which it can display how it helps address new challenges rather than innovation in IoT being stifled because of them.

For any technology to meet or exceed expectations of 90% of its market is remarkable but for this to happen in an industry that only a few years ago was an unregulated lab environment in which players were attempting far-fetched business creation based on a technology looking for an application is exceptional. This is partly because established enterprises and industries now see IoT as their future. Car-makers evidently recognise the reliance their future business places on IoT for managing the EV charging burden in a way that makes EVs work but also provides a decent experience to their customers.

Healthcare enabled by IoT is here to stay as pandemic-led unwillingness to hang around medical facilities becomes permanent. Healthcare authorities now see how IoT saves money, adds efficiency and is developed enough to handle the risks of keeping patient data secure.

It is these steps towards maturity coupled with greater familiarity with what IoT can do, and what it shouldn't, that are creating mainstream IoT. Of course, projects will still fail and these failures should be applauded too, provided lessons are learnt and new approaches result from them.

With the consolidation activity we have recently seen and the heavyweight deployments multiple industries are engaged in, it's clear that IoT has not become too big to fail, it has become too useful to fail.

Enjoy the magazine!

George Malim

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

EDITORIAL DIRECTOR & PUBLISHER
Jeremy Cowan
Tel: +44 (0) 1420 588638
j.cowan@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

Telit to buy Thales' cellular IoT products and create Telit Cinterion

Paolo Dal Pino, **Telit**

Telit and **Thales** have agreed that Telit is to acquire Thales' cellular IoT products division. The intended transaction includes Thales' portfolio of cellular wireless communication modules, gateways and data cards, ranging from 4G LTE to low power wide area networks (LPWAN) and 5G products.

The intended transaction establishes California-based **Telit Cinterion**, as a US provider of IoT solutions, expanding the company's presence in growing industrial IoT segments and end markets including payment systems, energy, e-health and security. It also enhances the company's ability to respond more expertly to growing demand for cybersecure IoT solutions in modules and cellular connectivity, thanks to technologies from Thales.

"This transaction with Thales is arguably the most impactful one for Telit's competitiveness," said Paolo Dal Pino, the chief executive of Telit. "While it will boost our ability to address customer needs more precisely from a richer portfolio, it will also enable us to deliver all new offerings derived from the experience, expertise and the DNA of two companies that have made security and quality part of their brand promise from the very beginning."

Philippe Vallée, Thales's executive vice president of digital identity and security, added: "The Thales and Telit combination brings together complementary strengths. The business will provide a unique value proposition in a highly competitive global IoT market and will allow Thales to focus its investments on its three core activities in aerospace, defence and security and digital identity and security."

Thales' cellular IoT module business, with approximately 550 employees across 23 countries, services many of the world's top brands. It generated sales of more than €300 million in 2021. With the transaction expected to close in Q4 2022, Thales will become a shareholder in Telit Cinterion, controlled by asset manager **DBAY Advisors** and led by Dal Pino.

Separately, Telit has acquired a group of assets from custom IoT start-up **Mobilogix**. Under the deal, Mobilogix personnel will relocate to Telit's headquarters as the company becomes Telit Cinterion.

Semtech to acquire Sierra Wireless for US$1.2bn

Phil Brace, **Sierra Wireless**

A definitive agreement has been announced under which **Semtech** will acquire all outstanding shares of **Sierra Wireless** in an all-cash transaction representing a total enterprise value of approximately US$1.2bn. The acquisition will significantly expand Semtech's addressable market and is expected to approximately double Semtech's annual revenue and create a strong and diverse portfolio of connectivity solutions for the growing IoT market, making it easier for customers to find innovative end to end solutions for any segment.

This acquisition brings together two important technologies for the future of IoT – LoRa and cellular – to enable the digitisation of the industrial world with a comprehensive chip-to-cloud platform. Semtech expects the combination of Sierra Wireless' cellular capabilities across its modules, gateways and managed connectivity together with Semtech's LoRa-enabled end nodes to create a differentiated IoT portfolio which will enable a plethora of new IoT use cases to be conceived.

"Our vision is to build a simple, horizontal platform with the goal of accelerating this transformation and to bring about a smarter and more sustainable planet," said Mohan Maheswaran, the president and chief executive officer of Semtech. "Together, with the world-class Sierra Wireless engineering team, we will be positioned to advance the market with multi-radio solutions that bring new chip-to-cloud services to support customers and grow our business."

Phil Brace, president and chief executive officer of Sierra Wireless, added: "Sierra Wireless is a high growth business with some of the best, most advanced IoT technology in the industry, and we are pleased to deliver immediate and compelling value to our shareholders through this transaction. Joining Semtech will also allow us to bring cellular and LoRa technology together to create innovative solutions that exceed the expectations of our customers around the world while delivering exciting career opportunities to our talented employees as part of the combined company."

News in Brief

Emerson Ventures invests in Spearix

Emerson has made an investment through Emerson Ventures, its corporate venture capital arm, in **Spearix Technologies**. The company's adaptive, multi-core radio processor provides a system-level solution for Industrial Internet of Things (IIoT) wireless communication.

Based in Cedar Park, Texas, Spearix's primary product offering is a multi-core radio processor and associated software that adapts to optimise performance and power based on measured environmental conditions. The technology has been shown to improve the connection reliability of industrial protocols while operating under heavy interference induced by high-power, high-bandwidth pervasive Wi-Fi operation.

Aramco's Wa'ed Ventures and Phaistos back OQ Technology

OQ Technology, a global 5G IoT satellite operator, has closed a US$21.5m Series A funding round led by **Wa'ed Ventures**, the venture capital arm of **Aramco**, and **Phaistos Investment Fund**, managed by 5G Ventures in Greece.

OQ Technology will use the funds to further develop its own technology solutions, acquire more spectrum licences and grow its 5G IoT satellite constellation. The constellation provides fast and real-time data processing for IoT and machine-to-machine (M2M) applications in remote and rural areas.

News in Brief

Bridgestone and AWS focus on platform development

Bridgestone is using **Amazon Web Services** as its strategic cloud provider in support of the company's sustainable mobility solutions. Using AWS Internet of Things (IoT), machine learning, and analytics and business intelligence services, Bridgestone is to accelerate the creation of digital platforms to launch new solutions for its customers, improve data analysis and streamline IT operations. This relationship is an important milestone in the Bridgestone 3.0 journey towards enhanced corporate value that merges business strategies with sustainability initiatives.

As part of the relationship, Bridgestone will work with AWS's ProServe and AWS Marketplace teams to enhance its existing fleet solutions and bring concepts like a Bridgestone marketplace to life. The Bridgestone fleet solutions and service-centric marketplace concept will provide a comprehensive selection of services and solutions to fleet managers to proactively assess fleet needs and reduce vehicle downtime.

Kubota and Accenture establish joint venture for more sustainable society

Kubota Corporation and **Accenture** have formed a new joint venture company, Kubota Data Ground to accelerate the digital transformation (DX) of the Kubota group's business model and operating infrastructure. Kubota Data Ground will be a subsidiary with strategic capabilities in DX that it will use to further contribute to solutions for food, water and environmental sustainability. In addition, the company will develop digital human resources and a cloud-based digital platform that will strengthen and upgrade existing businesses by connecting internal and external services and data.

TomTom to power Hyundai Motor Group with maps and traffic info

TomTom has been chosen by **Hyundai Motor Group (HMG)** to support its entire vehicle line-up in Europe. Over the coming years, millions of HMG vehicles will come equipped with this technology as standard. As was already the case for **Genesis** drivers, all Hyundai and **Kia** customers in Europe will now enjoy TomTom's maps supporting their vehicles' in-dash navigation and level-two automated driving features. Genesis, HMG's premium brand, launched its model range in Europe during the summer of last year, equipped with TomTom's maps and real-time traffic technology.

TomTom's maps help carmakers push the boundaries of automation by enabling advanced driver assistance systems (ADAS) to better anticipate the road ahead. The TomTom ADAS Map provides these systems with higher-quality road information, including gradient, lanes, curvature, and speed limits, improving safety, comfort, and eco-performance. HMG's innovative Highway Driving Assist (HDA) relies on this data to independently change speed if the posted limit changes, and automatically slow down and navigate freeway transition ramps and curves in a safer way. TomTom map data provides highly accurate, verified content for all speed limit types across Europe, helping with intelligent speed assistance (ISA) regulation compliance, which came into force as of July 2022.

Hyundais will use TomTom ADAS map capability

"We are thrilled that all Hyundai and Kia drivers in Europe will benefit from the comfort and safety provided by TomTom's geolocation technology," said Haeyoung Kwon, the vice president and head of the infotainment development group at HMG. "TomTom is a partner we trust to deliver highly accurate map data that enhances our Highway Driving Assist technology, and real-time traffic information that helps us optimise navigation guidance and ETAs."

Antoine Saucier, the managing director of TomTom Automotive, added: "Hyundai Motor Group is one of the most innovative and forward-thinking players in the automotive industry, and we look forward to collaborating over the coming decade, creating pioneering solutions that provide freedom of movement in a safe, enjoyable and clean way."

Aeris launches IoT readiness calculator to instantly determine readiness to launch IoT projects

Aeris has announced its IoT Readiness Calculator, a free online tool to help determine enterprises' level of preparedness for deploying IoT solutions. The IoT Readiness Calculator provides organisations planning IoT projects with a scorecard that details the readiness of your IoT project from a business and technical perspective and how it compares to others in the same vertical market or geography. It will also help to identify potential issues in an IoT launch plan, so users can remediate them before they become costly.

The average cost of a cybersecurity data breach in the US is estimated at more than US$4 million. However, with the right IoT security strategy in place, it's possible to mitigate those risks. Security is just one element that the Aeris IoT Readiness Calculator takes into consideration. It also examines variables such as latency, integration and scalability.

Syed Hosain, **Aeris**

Syed Hosain, the chief technology officer at Aeris, said: "According to **Microsoft**, 30% of IoT projects never get past the proof-of-concept phase. The Aeris IoT Readiness Calculator and our IoT experts can help identify the gaps in your current IoT plan and can ensure that your IoT deployment launches successfully."

Omdia research finds enterprises are turning to 5G for their IoT needs

Enterprises are not only increasing their IoT spending and their deployment of devices but are doing so because IoT projects are meeting or exceeding return on investment (ROI) expectations according to the latest **Omdia** Internet of Things (IoT) Enterprise Survey. Omdia surveyed approximately 500 enterprises across countries that are deploying or are in the process of rolling out IoT solutions and found that over 90% of enterprises said their IoT projects have met or exceeded expectations.

"Both IoT and 5G have been derided as overpromising and underdelivering," said John Canali, the IoT principal analyst at Omdia, "yet the IoT market is still developing and 5G technology is still evolving. While sometimes outrageous proofs of concept are touted for headlines, our survey results are clear: enterprises are embracing IoT and 5G is emerging as the preferred type of connectivity."

Omdia's survey results are positive for players across the IoT value chain. Communications service providers will likely see growth in high-bandwidth, high-value connections as 66% of enterprises are using or plan to use 5G connections while 53% of enterprises are using or plan on deploying new connections using LTE. The responses were similarly encouraging for growth in low-bandwidth connectivity such as NB-IoT and LoRaWAN.

John Canali, **Omdia**

Worldwide wearable shipments to reach 344m by the end of 2022, says ABI Research

Demand for wearables and accessories slowed during 2021 due to economic and geopolitical factors impacting consumer's priorities. Yet, despite this decline, global technology intelligence firm **ABI Research** expects continuous growth from now until 2027.

More than 300 million wearables devices were shipped by the end of 2021 and the total will reach around 344 million by the end of this year. Additionally, more than 650 million of these devices are expected to be shipped worldwide by 2027, a CAGR of 13.2% between 2022 and 2027.

Up to the end of the current year, the growth in the wearables market is foreseen to be driven mainly by two segments, namely sport, fitness and wellness trackers and smart home-enabled smartwatches. "The reason behind the rise of these two segments is the continuing direct consequence of the pandemic on consumer's habits," said David McQueen, the consumer technologies research director at ABI Research. "This year, smartwatches will continue to dominate the wearables market due to the strength of the **Apple** smartwatch and the growing number of companies offering smartwatches with impressive functionalities." says David McQueen, consumer technologies research director at ABI Research.

The increasing demand for activity trackers is predicted to drive the wearables market. Activity trackers will reach shipments of about 91.5 million by the end of 2022 and are forecast to reach 105 million by 2027, a CAGR of 2.9%. "There is rapid growth in the use of wearables, notably smartwatches and activity trackers, among cyclists, runners, gym-goers, swimmers and athletes, to track calories burned, hourly activity, stationary time and activity time," added McQueen. "The growth in health and fitness use cases is expected to propel wearable shipments. However, standalone cellular connectivity will be confined to smartwatches for the time being as sport, fitness and wellness trackers market will not ship with a cellular connection before 2026."

In comparison, smart home-enabled smartwatches - smartwatches with the ability to interact with smart home devices - represented about four million devices in 2021 and is expected to expand to 32 million in 2027, a CAGR of 35.8% between 2022 and 2027. This category will mainly be shipped with a 4G connection, producing a spectacular CAGR of about 60% from 2022 to the end of 2027. ABI Research forecasts 5G smart home-enabled smartwatches to be in the market by 2024.

Berg Insight says global cellular IoT connections grew 22% to reach 2.1bn in 2021

Berg Insight says that the global number of cellular IoT subscribers increased by 22% during 2021 to reach 2.1 billion. The major regional markets China, Western Europe and North America grew similarly during the year as the world recovered from the COVID 19 pandemic. By 2026, Berg Insight now projects that there will be 4.3 billion IoT devices connected to cellular networks worldwide.

The top ten mobile operators reported a combined active base of 1.8 billion cellular IoT connections at the end of 2021, accounting for 86% of total connections. China Mobile is provider of cellular IoT connectivity services with an estimated 801 million cellular IoT connections. **China Unicom** and **China Telecom** ranked second and third with 300 million and 297 million connections respectively.

We're at the beginning of a new era in cellular IoT. The momentum with technologies like LTE-M, narrowband IoT (NB-IoT) and 5G is only just starting in terms of hardware availability, coverage and so on, and demand is ramping up

How cellular IoT is turning a corner after COVID 19 with the emergence of massive IoT capabilities, sustainability and security

The recent pandemic has transformed many companies' attitudes towards IoT and cellular technology is at the forefront of future growth expectations. Addressing that demand is not a simple process given the complexity of the ecosystem, how cellular networks and suitable coverage are rolled out, and how end-to-end security of networks and devices is achieved. Cyril Deschanel, the managing director of Tele2 IoT, tells Steffen Sorrell, the chief of Research at Kaleido Intelligence, how the industry is working to achieve cellular IoT's inflection point

Steffen Sorrell: What has been happening with the IoT market over the last 18-24 months or so? How have you seen the market developing given the impact of COVID 19?

Cyril Deschanel: IoT has been growing steadily in the last two years, with around 12% revenue growth in Europe. There hasn't been the expected fast uptake yet because COVID 19 has slowed down some application demand, such as in automotive. However, many new IoT applications are emerging, such as in the health sector, and this acceleration has persisted even as the restrictions implemented during COVID 19 have been lifted. Today, you have people videoconferencing with their doctors remotely from walk-in cabins, sending blood pressure and other readings, and with devices at home to measure things like sleep apnoea and so on. In other areas, we have a customer that's using artificial intelligence (AI) and IoT connectivity to identify potential workplace safety hazards to prevent accidents before they happen. That's important in environments like manufacturing, construction sites or ports.

We're at the beginning of a new era in cellular IoT. The momentum with technologies like LTE-M, narrowband IoT (NB-IoT) and 5G is only just starting in terms of hardware availability, coverage and so on, and demand is ramping up. If you look ahead 5-10 years from now, there'll be many more hundreds of millions of devices connected with these technologies, on top of other technologies like 4G.

There are also external drivers that are accelerating growth. Enterprises are making digitalisation a top priority for one thing, while sustainability is a key issue today. Companies want and need to deliver a better planet. I think it's fundamental for companies to contribute, but you also need to use IoT to realise cost savings in that effort. There's also a ramp-up in things like Industry 4.0, smart manufacturing and the relocation of manufacturing facilities to ▶

SPONSORED INTERVIEW

Cyril Deschanel:
Tele2 IoT

hedge against some of the supply chain challenges that came about during COVID 19.

There are many drivers on the demand side and new technologies on the supply side that will fuel growth.

SS: Talking about growth at Tele2 IoT, what would you say are the key factors behind that in terms of your own offering or your experiences with customers?

CD: Nearly a decade ago we started building our IoT operations from scratch with an ambition towards digital native operations, which has allowed us to move faster than others. I think one of the key things is that the organisation is dedicated to IoT, from sales to product and down to technical support through the IoT Network Operations Centre (iNOC), which is different to most operators, where if you call up their technical support, you don't immediately get someone specialised in IoT. That iNOC team is also proactive – we don't just monitor devices on our own network, but also those roaming on other networks, looking at devices' behaviour over the last six weeks to detect any changes at the access point name (APN) level ,which helps us develop ▶

We were the first to bring 5G to our IoT connectivity management platform, and we've seen the roll-out of 5G being the fastest out of all of the cellular technologies

proactive approaches to connectivity management. If you have a fleet of tens or hundreds of thousands of devices deployed in the field globally, this becomes really important for you.

Today we're very strong in Northern Europe and the Baltics and one of our main objectives over the next 18 months is to get closer to customers in Western, Southern and Central Europe, which is especially important for larger customers.

It's strange to think of IoT companies not being digitalised, but they actually have focused on digitalising their customers, rather than themselves. You need to use that digitalisation to really streamline the customer experience via a single tool – from SIM delivery and provisioning to SIM logistics, contract management, rate plans, on-boarding and many other processes. At **Tele2 IoT**, within around three years, we're aiming to become fully digital in our operations to remove any remaining manual processes to address customer needs.

Also, we don't just focus on connectivity – we are the IoT-friendly experts. We know the hardware side well, so can offer recommendations for modules or routers and point customers towards suppliers so they can establish direct relationships with those players. We position ourselves as friendly experts who help customers make the right choices. This is especially important for bearer services like LTE-M and NB-IoT, where customers often find the ecosystem confusing. We help demystify eSIM for customers and are one of the few operators that allow enterprises to use our virtual profile on SIM cards that are not issued by us so that customers can benefit from our footprint and connectivity agreements.

SS: Speaking of coverage footprint, we touched a little earlier on massive IoT and the potential explosion in IoT connectivity. How do you see the market for technologies such as 5G, LTE-M and NB-IoT developing, especially on the roaming side for the latter two?

CD: We offer a full suite of technology support all the way to 5G but roaming for LTE-M and NB-IoT is probably the biggest challenge for the market adoption right now. Even though the technology exists, you need time to roll it out due to the fact that each and every network operator needs to fulfil a set of test cases with every other operator that wants to be part of the roaming network of that respective technology. Nevertheless, we have been one of the fastest in rolling out LTE-M – we launched it around two years ago, and already have 25 markets covered. We're expecting support for another eight by the end of the year and ready to enable more as long as the roaming partners are as ready as we are. We're pretty flexible in terms of prioritising how those roaming agreements get rolled out – when we see a customer need for a particular market, we can prioritise addressing that roaming need.

NB-IoT is quite limited today in terms of roaming and coverage, so LTE-M offers a great compromise given that it can also address a broader set of use cases. That said, we're launching NB-IoT roaming this year and should have ten agreements by the end of the year. NB-IoT has mostly been used for national or local use cases, which is why many utilities are looking to utilise it. However, some constrained devices still need that roaming capability. There's a bit of a misconception around NB-IoT, with customers expecting lower costs on the connectivity side, and a misunderstanding about how it gets rolled out. Actually, the main savings come on the device side, as NB-IoT devices are cheaper than LTE-M. Mass adoption of NB-IoT is going to be helped tremendously by the roll-out of 5G roaming; NB-IoT has been absorbed into the 5G standard, and the way that 5G roaming agreements are set up will mean that they will both go hand-in-hand in future.

We were the first to bring 5G to our IoT connectivity management platform, and we've seen the roll-out of 5G being the fastest out of all of the cellular technologies. We have already launched in 60 markets, and by the end of the year we expect that number to increase to around 100, which is remarkable. The thing about 5G is that it not only brings the LTE-M and NB-IoT technologies into the standard, which guarantees longevity for those low power use cases, but it also brings higher speed and lower latency, so you can address near real-time application requirements. This brings new use cases to the market – cellular connected CCTV and security systems, vehicles and transport systems equipped with autonomous and connected safety features, robots and drones, enhanced remote operations for manufacturing, mining and healthcare, and so on. We see for example a need from large companies to reduce reliance on manufacturing in places like China or India, so plans are being made for new factories. It's always easier to build a connected factory than to retrofit an existing one, and private 5G networks can offer a tremendous benefit here.

SS: We can't really talk about IoT without mentioning security, and how important it is for customers to have solutions in place to guarantee the end-to-end security of devices. How is Tele2 IoT approaching this?

CD: There are less security standards around IoT than in the telecoms world in general. Part of our responsibility is to push for standardisation, but also to not wait for the industry. We need to lead in the security area. In that context, we have been pioneering helping increase the security of the communication between devices and the companies that manage these devices. Last year we launched our first secure dedicated IoT fibre for our customers through our **Equinix** partnership.

It's called Private Interconnect, and transports customer data through Tele2's backbone fibre network onto the customer's own fibre network. This takes the data away from the public internet and significantly reduces the chance that cybercriminals can access any data. We've complemented this service with Cloud Interconnect which uses Tele2 and Equinix infrastructure to offer a secure, pre-integrated connection to major cloud providers like **AWS**, **Azure**, **Google** and **Oracle**. Almost all of our customers are using some cloud service, but the ▶

type of security offering we've developed is not common on the market today. IoT is still a young industry, so the market regarding these types of offerings is not very mature. For example, you still see providers offering connectivity over public access point names (APNs) – this is really high risk.

The issue is that IoT devices can be used as a door to the rest of the network. Today, not a single industry doesn't use IoT for remote operations, and security is only ever as good as the weakest link in the chain. If you don't properly secure your devices, there will always be a door. Security doesn't have to be overbearing – if you look at the traditional way of doing things, you'd use a private APN and virtual private network (VPN) like an onion layer, but then devices need to be configured one-by-one, which is hard to set up and maintain. Perhaps this is one of the reasons why IoT hasn't adopted the security protocols that it should. Technologies like Cloud Interconnect are basically plug-and-play, as long as you're using a cloud service, because they are managed at the network level. This is likely to become the norm when we consider how IoT security is implemented.

SS: You mentioned sustainability as a big driver for IoT earlier in the interview. How do you see these interacting?

CD: First off, we would like to be sustainable at Tele2 Group as a whole, and so we've invested a lot in the sustainability area, and we've recently been named one of the first 40 companies in the world to get approved against the net-zero Science-Based Target Initiative. Now all our customers need to do the same, whether that is due to regulations or other factors, so we want to help them in their sustainability efforts, because there are different needs around that. As you're probably aware, the European Union is quite strong on that.

For some companies, it is clearly at the heart of their business model – take a classical traditional fleet management company. Their objective is to reduce the costs and the fuel consumption of their customers. And then you have an important change in the market where investors are now looking at the corporate profile of the enterprise and looking to see if they are investing in sustainability efforts. If you are not doing it today, I don't think you will be very attractive as a company from an investor and shareholder perspective. This wasn't the case some years ago.

Some people ask me, how many IoT applications are helping on the sustainability front? I would actually ask how many are not. For example, a couple of years ago that new factory would have been in China. But thanks to low latency technologies such as mobile private networks, production costs can be dramatically reduced, so you can benefit from local production, avoiding exploitative working environments and produce in your own market in a sustainable and eco-friendly way. We're now moving in the direction where essential products are made in local markets, and also recycled in local markets thanks to connected and automated technology.

In conclusion, what has been expected to happen in the IoT world is finally happening. All cellular technologies are becoming enabled, the device ecosystem is becoming mature, and more importantly, society is becoming more demanding when it comes to connected applications. This makes us at Tele2 IoT conscious of our role as an enabler at the heart of this new digital realisation.

Some people ask me, how many IoT applications are helping on the sustainability front? I would actually ask how many are not?

www.tele2iot.com

ChargeNode shows how large scale electric vehicle charging can be achieved

As electric vehicles (EVs) become mainstream, single outlet charging stations continue to be installed, but in many ways they no longer meet the demands and requirements of EV drivers. ChargeNode is at the forefront of this development, building large scale EV charging systems that serve hundreds or even thousands of EV customers in places like office parks, airports, shopping malls and municipal parking garages

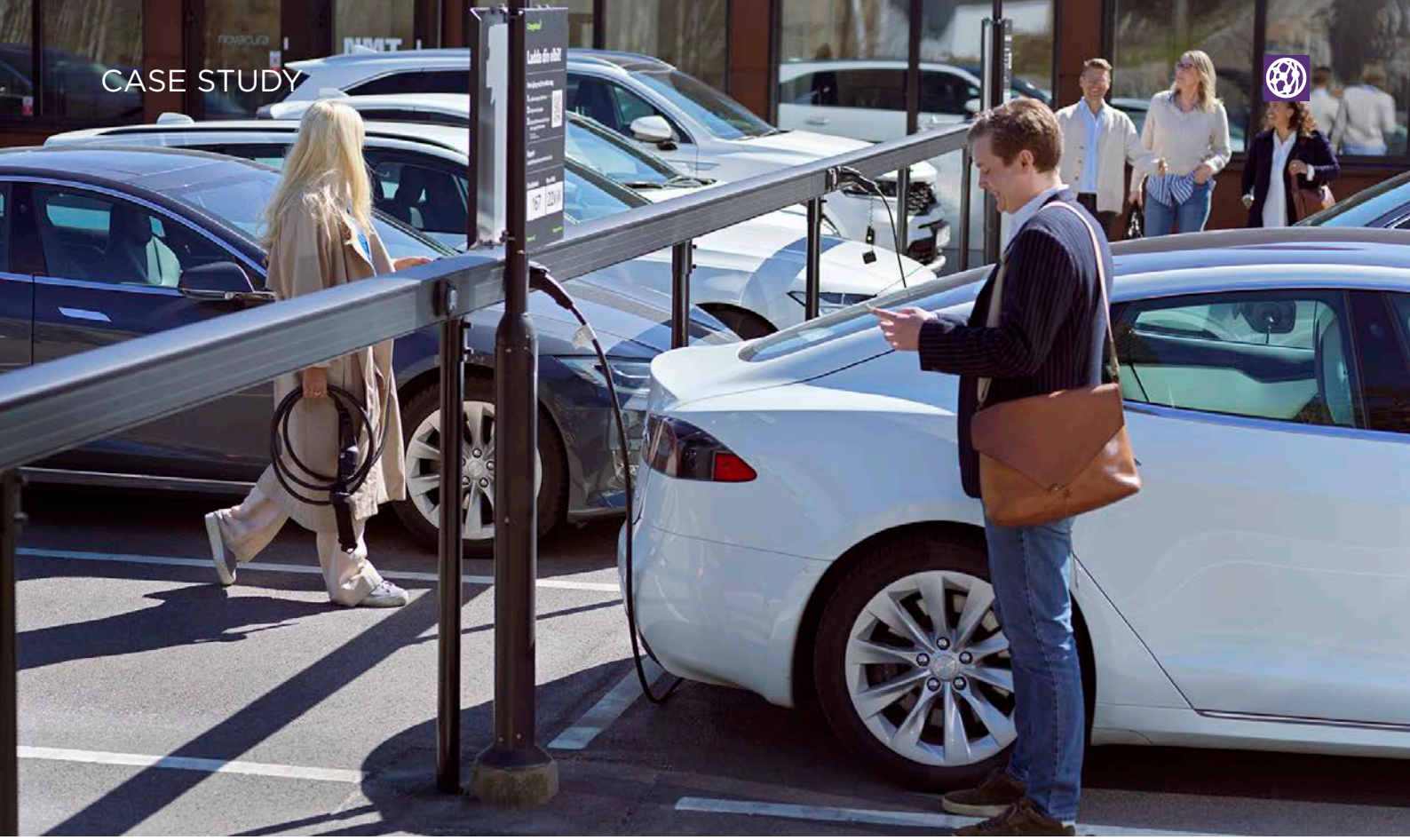
Kristian Sandahl
ChargeNode

To put it another way, when we're talking about individual charging stations, it's pretty much a first come, first served situation – and the person who comes late might not be able to charge at all. This is where large scale installations are a game changer. They are a more effective use of resources because **ChargeNode** can see when people are at work and how long they will be there and then optimise the charging. In order to do this and connect each car, ChargeNode needs information, such as how much the customer wants to charge their vehicle and how long the car will be parked. This allows them to allocate energy across the charging system in order to meet the customers' needs.

"Because we work with really large facilities, we have to consider that hundreds of cars may need charging in the same location, because large scale charging requires a totally different way to charge cars," explains Kristian Sandahl, the chief executive and founder of ChargeNode. "So, we ask our customers two very basic questions: how much would you like to charge and when are you going to use the car? Having this information means that instead of charging hundreds of outlets at a minimum power rate all at the same time, we charge an optimal number of cars in sequence of how they will be used. If the person changes their leaving time or something else happens, we can accommodate that by making adjustments within the system."

It's IoT and connectivity that allows ChargeNode to make those adjustments and optimise energy and charging for its customers. By being connected 24/7 the ChargeNode solution allows it to see who is, for example, coming to work at what time and who needs to leave at what time. ChargeNode gets its information through its connected app, which asks customers how much they want to charge and how long the car will be parked, allowing ChargeNode to optimally allocate the energy as needed.

"In terms of IoT, it's very simple: we need to be online all the time to be able to have a dialogue with the car owner, not just the car," says Sandahl. "The car is an asset to put energy into, but in order to do that I need to rely on the owner so he or she can be informed if something occurs, such as a fourth car comes in and needs energy. If that happens we can contact the owners who have cars already charging and say, for example 'You asked for 20kWh, would you be fine with 15kWh? Or, if they have changed their time of departure ▶



and that would need to be fed into the system. If they're leaving earlier or later than they initially planned, we need that information in order to make sure they are served and that the change works across the system. That means we need to be connected in order to stay informed all the time. You could say that other charging stations need to be online every hour or so to send data, while we need to be online 24/7 to operate efficiently and effectively. That's why having reliable connectivity is so important. We chose **Tele2 IoT** after evaluating a number of vendors. Tele2 IoT was competitively priced and flexible in those discussions, and there was also the considering of the managed logistics with the SIM cards – basically it was a very smooth process for us."

Reliable connectivity not only keeps ChargeNode in touch with its customers, it also allows them to gather data in order to see patterns and how much they change.

"Even if the data is not useful today, it will be useful in the future, because we can see patterns over time, such as how much of an impact energy prices will have if you have a half-full battery or an almost empty battery, along with what's your comfort level in terms of how much of a charge you want before you worry about the price," says Sandahl. "All that data tells us a lot about customer behaviour, such as if you have 10% charging left, you are more reliant on paying more so that you feel comfortable with the charging level."

In terms of the future, Sandahl says that charging is all about convenience and people not worrying about how much charging 'juice' they've got in the tank. And as more and more people buy EVs who don't live in individual homes where they can charge off their home energy supply, large charging station installations are going to become increasingly important.

"Right now, some apartment complexes are a bit reluctant and slow to implement charging stations," says Sandahl. "But they are starting to realise that this is like having fibre internet in their buildings. Even if you don't worry about charging your car, the residents of your building probably want the possibility to do so, and the person they eventually sell their apartment to will likely also want that possibility, so this is an area where a lot of things can happen."

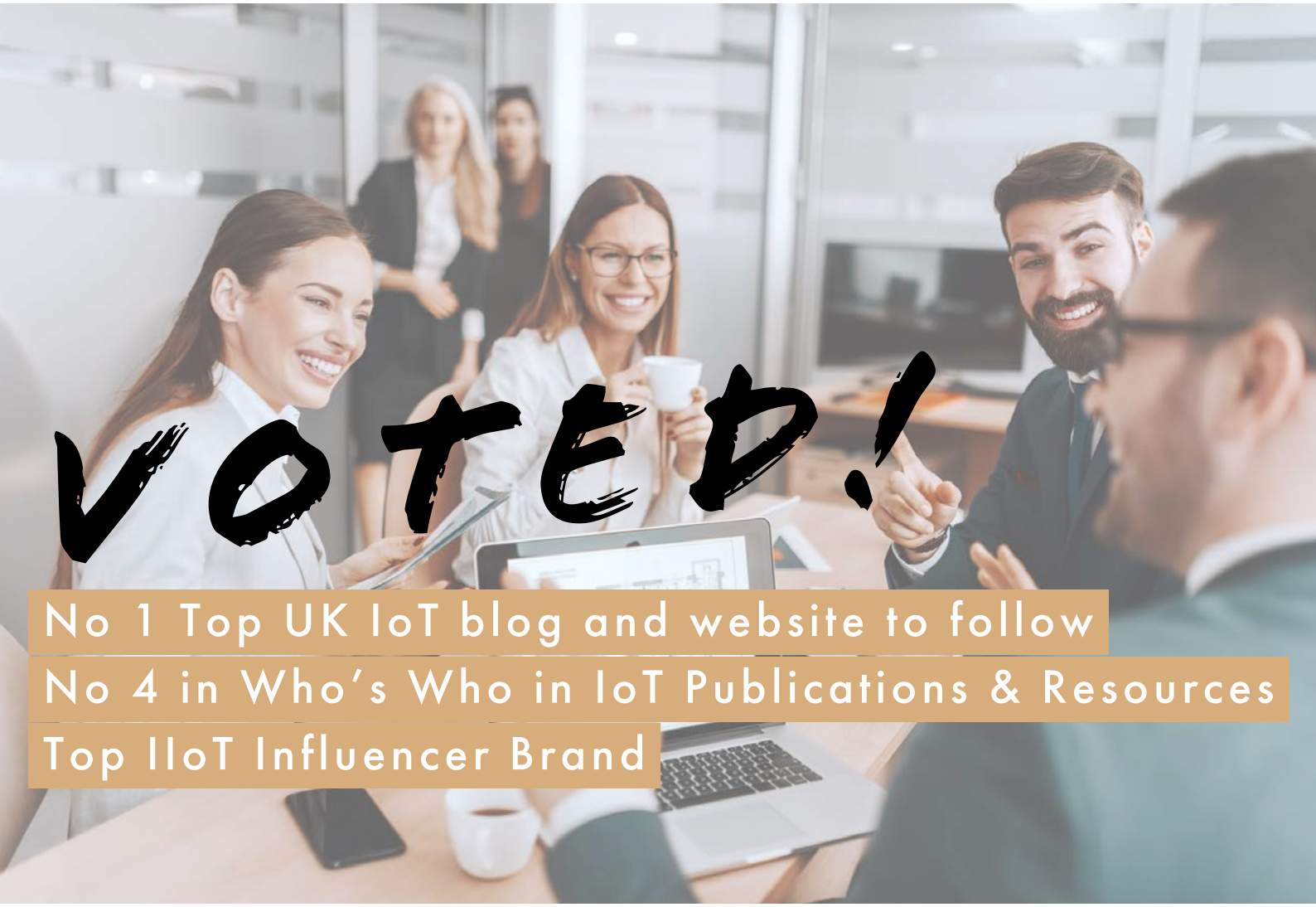
"EV sales are overtaking fossil fuel car sales, which means more and more charging stations will be needed going forward," he adds. "People need to think beyond next week or next year and think more long-term in order to be prepared. Installing large scale charging solutions now means not having to retrofit or spend more money later on – and it also means using our limited resources more wisely." ■

www.tele2iot.com

IoTNOW

HOW TO RUN AN IoT ENABLED BUSINESS

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

Europe's IoT industry doubles down to make the mass market a reality

Europe is an early adopter of IoT and sustained, planned investment by enterprises will ensure it keeps its position as the third largest IoT market behind China and North America as the decade continues, in spite of the challenges of war and disease, writes George Malim

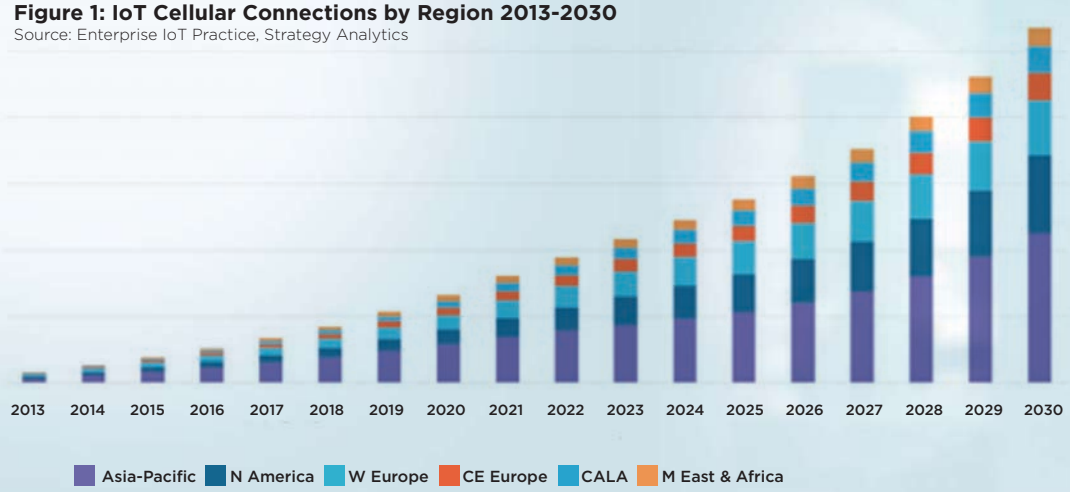
The **Next-Generation Internet of Things** (NGIoT) initiative of the European Union reports that 80% of processing and analysis of data currently takes place in data centres and centralised computing facilities, and 20% in smart connected objects but this is poised to flip. Within the next five years, 75% or more of the data processing and analytics will run at the edge of the network. Within this shift, the organisation says, Europe must take advantage of the decentralisation trend through new IoT and edge computing capabilities.

The continent has the opportunity to make use of its well-established communities in the physical, industrial world and in the digital world to bring the best of both to Europe's next generation of IoT and edge computing infrastructure. NGIoT believes that edge computing will have a radical impact on how sensing, evaluation and control of our environments are achieved. The organisation believes that edge capabilities will be central to the adoption of cloud, artificial intelligence (AI), energy aggregation, manufacturing, precision farming, autonomous vehicles and many other vertical activities that are part of a wave of innovation that will dramatically improve the lives of European populations.

That vision remains some way off with mass market IoT only now truly arriving in Europe which continues to be one of the leading regions in terms of adoption in the world. Europe's position ▶

Europe must take advantage of the decentralisation trend through new IoT and edge computing capabilities

Figure 1: IoT Cellular Connections by Region 2013-2030
Source: Enterprise IoT Practice, Strategy Analytics



A new report from IoT market research firm Berg Insight also sees active subscriptions increasing, reporting that the global number of cellular IoT subscribers increased by 22% during 2021 to reach 2.1 billion

as a leading IoT region will endure thanks to committed investment by enterprises which **IDC**'s 'Worldwide Semiannual Internet of Things Spending Guide' estimates will total US$208 billion in 2022 in Europe. This growth will continue at a double-digit rate until at least 2026 and comes in spite of the current challenges of the Russia-Ukraine War, the aftermath of the pandemic and the economic challenges affecting the continent. IDC says increased spending will continue in areas in which improving business performance is essential such as manufacturing, healthcare, retail and infrastructure.

"During the pandemic, many organisations refocused their technology investment plans, aiming for a technology stack to support innovation, efficiency and performance, even in challenging situations - such as the Russia-Ukraine War - with IoT and automation at the core," says Alexandra Rotaru, a research analyst for Data and Analytics, Europe, at IDC. "With organisations seeking to improve productivity, reduce costs, better orchestrate resources and assets, and enhance customer experience, IoT will remain on the agenda for many technology leaders in the years to come."

In fact, the firm says the largest share of spending in Europe will be in the manufacturing and resources sector, directed at predictive maintenance and production asset management in which IoT is used to enhance manufacturing organisations' tracking, monitoring and maintenance of industrial devices.

The fastest rate of adoption according to IDC will be in electric vehicle (EV) charging in Europe, driven by the expansion of commercial EV charging stations across the continent, with IoT enabling real-time availability and reservation scheduling, charge notifications, automated billing, and value-added services, as well as offering marketing opportunities.

Europe's position as an early adopter of IoT is borne out by **Transforma Insights**' 'Global IoT Forecast Report 2021-2030' which projects that Europe will account for 20% of the value of the IoT market in 2030, behind China and North America with 30% and 20% respectively. The report paints a picture of a maturing IoT industry with 11.3 billion active IoT devices at the end of 2021 which will grow to 29.4 billion in 2030.

A new report from IoT market research firm **Berg Insight** also sees active subscriptions increasing, reporting that the global number of cellular IoT subscribers increased by 22% during 2021 to reach 2.1 billion. The major regional markets China, Western Europe and North America, grew similarly during the year as the world recovered from the COVID 19 pandemic.

The top ten mobile operators reported a combined active base of 1.8 billion cellular IoT connections at the end of 2021, accounting for 86% of total connections. **China Mobile** is the world's largest provider of cellular IoT connectivity services with an estimated 801 million cellular IoT connections. **China Unicom** and **China Telecom** ranked second and third with 300 million and 297 million connections respectively.

Vodafone ranked first among the western operators and fourth overall with 142 million connections, followed by **AT&T** with 95 million in fifth place. **Deutsche Telekom** and **Verizon** had in the range of 45–55 million cellular IoT connections each, when counting **T-Mobile USA**'s customers as part of Deutsche Telekom's IoT subscriber base. **Telefónica**, **KDDI** and **Orange** were the last players in the top ten with about 31 million, 23 million and 20 million connections respectively.

These huge numbers don't mean massive revenues for operators and IoT connections still represent only a small share of their business. IoT connectivity services account for only around 1% of total revenues for most operator groups. Berg Insight's analysis of the IoT business KPIs released by mobile operators in different parts of the world suggests that global IoT connectivity revenues increased by around 15% during 2020, while the monthly average revenue per user (ARPU) dropped by 2% to €0.38. ▶

Europe's position behind China and North America is expected to continue to at least 2030, reports **Strategy Analytics** pointing out that while there will be regional differences between the cellular technologies adopted, substantial growth will be seen in all markets. 5G will start to gain traction, the firm says: while 4G will continue to dominate overall, driven by 2G replacements, especially in China, but also elsewhere. 3G will retire with most connections moving to 4G and the firm expects 5G to total 47% of connections by 2030, while 4G will remain the dominant technology at 49%.

"The adoption of 5G will likely happen in different stages, with extended mobile broadband (eMBB) reaching mass adoption first, ultra-reliable low latency communications (uRLLC) gaining traction soon afterward, and massive machine-type communication (mMTC) showing the longest tail," says Gina Luk, the director of Enterprise Research at Strategy Analytics. "Adoption will be determined by the availability of 5G chipsets, the speed and coverage of 5G networks, and as well as the evolution of regulations. The engine for driving 5G forward for fast growth and rapid adoption is its radio access technology, referred to as new radio (NR). One recent example is NR support for reduced capability (RedCap) devices which can facilitate the expansion of the NR device ecosystem to cater to use cases include wearables such as sensors and video surveillance, as these are not yet best served by the current NR specifications."

Projections can only go so far, especially when covering a large and diverse region such as Europe. What is clear is that Europe has recovered relatively quickly from the COVID 19 pandemic and increasing spending, although hampered by the supply chain crisis. **IoT Analytics** says that technology budgets differed widely from region to region going into 2022 and are still correlated to the pandemic's impact. North America and Europe have increased IoT technology spending while in APAC and the rest of the world there is heightened caution with regard to innovation and technology investments.

Security becomes essential spending

The growth in number of IoT connections is creating an expanded threat surface that exposes organisations to new vulnerabilities. IoT security spending is therefore becoming mandatory and regulations are being put in place to mandate minimum standards and protections for users' data.

Bloomberg has reported that the regulatory landscape for IoT is evolving rapidly as governments seek to mitigate risks. The governments of various countries have put in place regulations and these will drive investment in IoT security. Examples include:

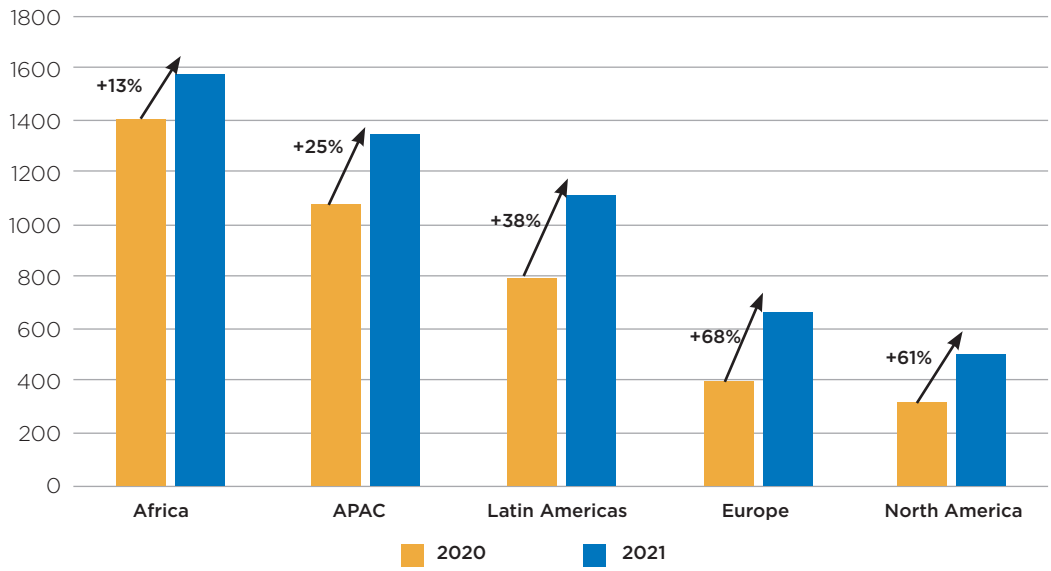
In 2021, the UK government introduced the Product Security and Telecommunications Infrastructure (PSTI) Bill to secure consumers from IoT threats and protect IoT devices. In 2020, the US government passed a new IoT cybersecurity law, the NIST Internet of Things Cybersecurity Improvement Act, to increase cybersecurity for IoT devices. Also, in 2020, the Australian government released a voluntary code of practice to improve Internet of Things (IoT) security in Australia, including smart devices. Finally, the European Technical Standards Institute (ETSI) has released ETSI EN 303 645, a standard for cybersecurity in the Internet of Things that establishes a security baseline for internet-connected consumer products.

With these and other planned regulation, the regulatory framework for IoT security is becoming progressively more stringent as governments are considering connected device-associated issues of enterprises as a serious risk. Tightening IoT security regulations are expected to drive the growth of the IoT security market over the coming years.

This year, the software segment is expected to account for the larger share of the IoT security market. The large share of this segment is attributed to the rising investments in R&D, increasing focus on software-centric security ▶

In 2021, the UK government introduced the Product Security and Telecommunications Infrastructure (PSTI) Bill to secure consumers from IoT threats and protect IoT devices

Figure 2: Weekly attacks per organisation by region (2020 vs 2021)
Source: Check Point Research



In spite of still recovering from the impacts of the pandemic and suffering the economic and material consequences of the Russia-Ukraine War, Europe continues to be an innovative region

capabilities, and increasing data and security breaches. However, the services segment is expected to grow at a higher CAGR during the forecast period because of growing demand for IoT security services among small and medium enterprises and the increased need to improve business processes and optimise business infrastructure.

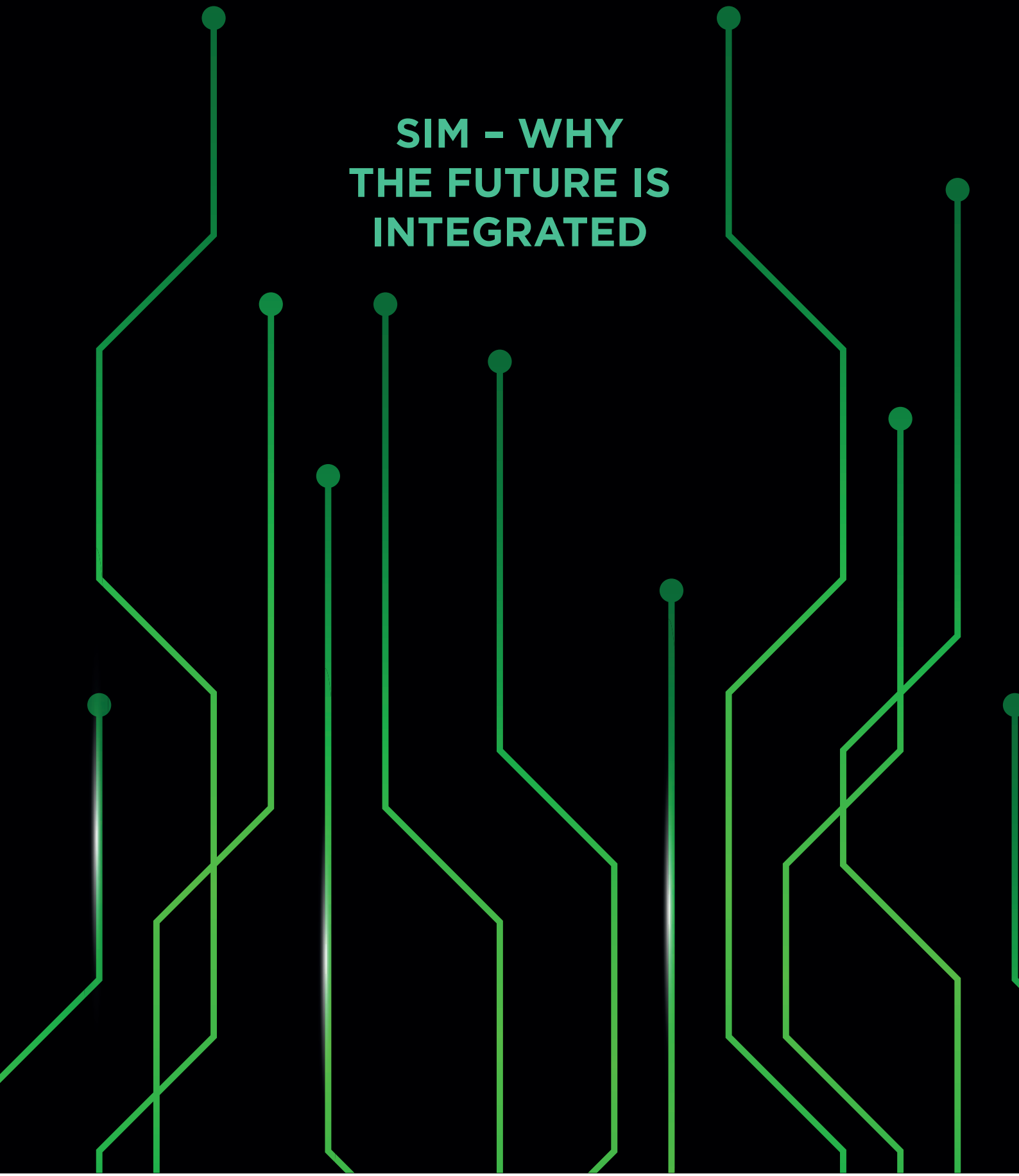
Based on security type, the IoT security market is segmented into network security, endpoint security, application security, cloud security and other security types. This year, Bloomberg predicts that the network security segment will account for the largest share of the IoT security market. However, the cloud security segment is expected to grow at the highest CAGR during the forecast period because of greater need to secure workload on cloud and the growing trend of bring your own device (BYOD) and working from home.

Regional differences are also apparent here with different regions experiencing various volumes of attacks. According to **Check Point Research**, Africa experienced the highest volume of attacks in 2021, with an average of 1,582 weekly attacks per organisation. This represents a 13% increase from 2020.

This was followed by APAC, which has an average of 1,353 weekly attacks per organisation (a 25% increase); Latin America, with 1,118 attacks weekly (a 38% increase); Europe, with 670 attacks weekly (a 68% increase); and North America, with an average of 503 weekly attacks per organisation (a 61% increase).

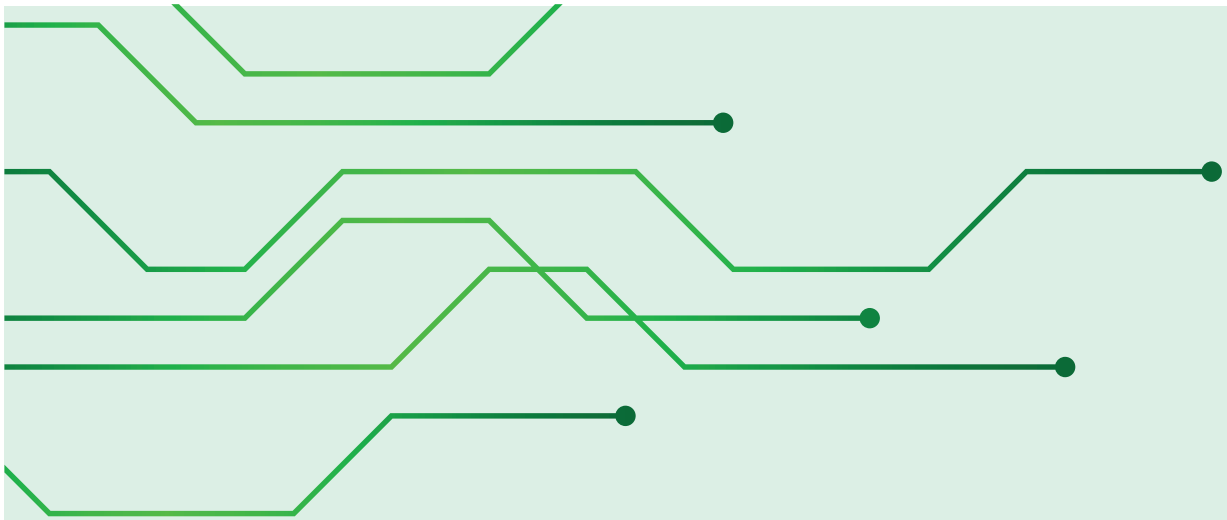
In spite of still recovering from the impacts of the pandemic and suffering the economic and material consequences of the Russia-Ukraine War, Europe continues to be an innovative region, open to adopting new technologies and investing in the infrastructure that is needed to enable them to operate efficiently. In IoT terms, this translates to sustained investment for a better future with the region's commitment to EV charging a clear indicator of continued spending. IoT is just one aspect of the region's digital future but with ample connectivity infrastructure, appropriate laws that protect users and IoT service providers and the R&D base to turn ideas into reality, European IoT looks to be set for massive growth inline with massive IoT.

SIM – WHY THE FUTURE IS INTEGRATED



Sponsored by:

Kigen



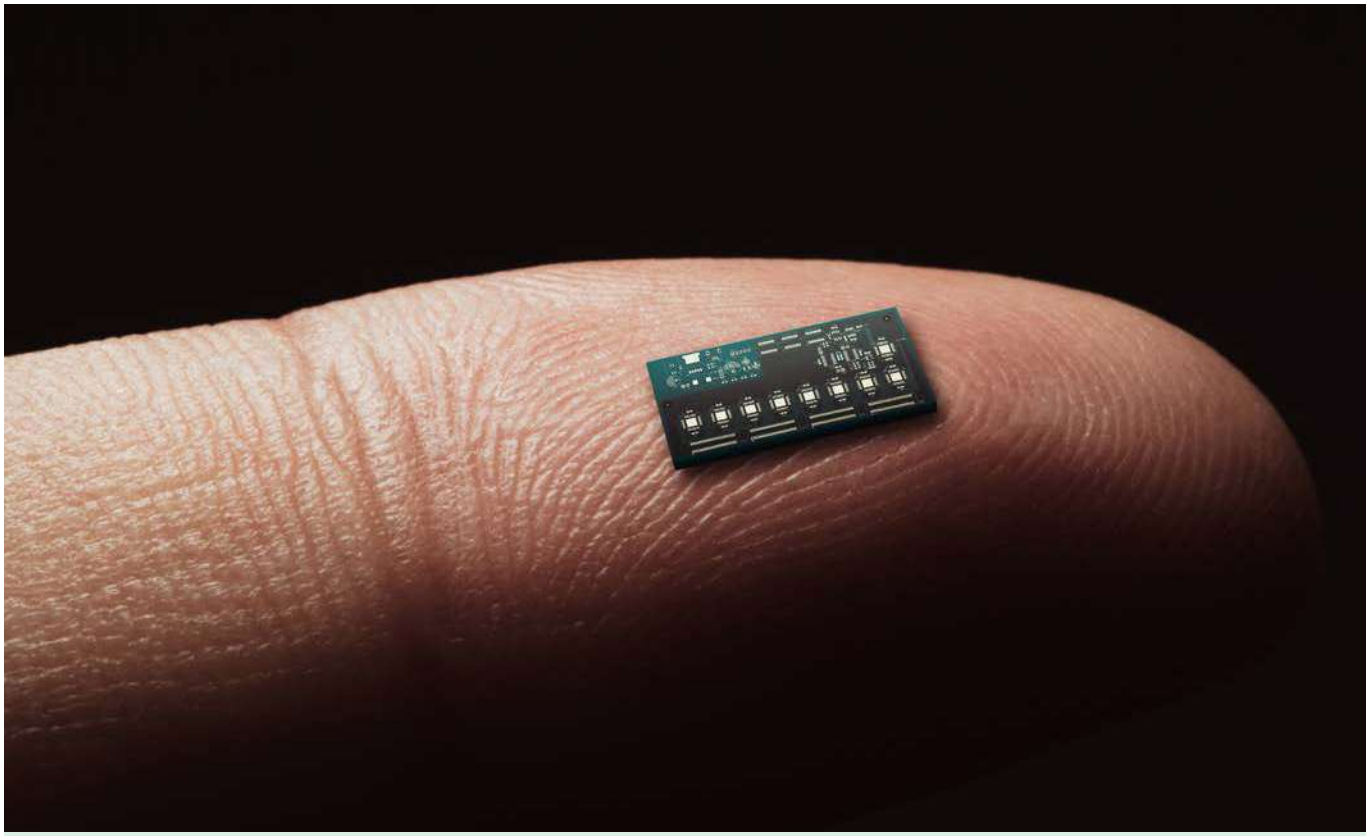
SIM - Why the future is integrated

Integrated SIM (iSIM) is the latest step in the evolution of SIM technology and presents appealing opportunities for product companies to make global devices that need out-of-the-box connectivity and ease of localised connectivity to national or regional connectivity providers. The iSIM can be designed into all products at the point of manufacture so a single variant can serve all markets. This has substantial benefits in logistics, warehousing, and balancing of supply and demand across different markets. iSIM also helps designers by streamlining development and accelerating time-to-market.

Simply selecting iSIM over the alternatives isn't the end of the story. iSIM comes at a cost – for many deployment types and, although this is a modest incremental addition, for high volume offerings that have low price points, iSIM and the associated provisioning and management systems can be an expense too far. Organisations therefore must carefully consider when to adopt iSIM.

In addition to authentication to secure global networks, an iSIM can be relied upon due to the integration with a secure enclave as proof of trust. This opens up revenue opportunities in new streams of secure data. Future device use-cases will increasingly rely on trusted secure devices to assure the veracity of data transmitted and that the device identity has not been tampered with. This is perhaps the greater benefit of iSIM as it enables new business cases and IoT opportunities, writes George Malim ▶

SPONSORED ANALYST REPORT



The subscriber identification module (SIM) used to be a simple, easy-to-address part of device design. The SIM was accommodated within a plastic card with a universal form factor that could be inserted into any appropriately designed mobile device and used to identify the subscriber and enable charging for network usage. Although a simple concept that has matured and evolved over 30 years, traditional SIM usage involves substantial logistical challenges that include installing the SIM locally because of the need to use a SIM from a local connectivity provider.

Plastic SIM means there is also inability to update or change service provider once the device is deployed without physically changing the SIM in the deployed device. Plastic SIMs are cheap in terms of upfront cost, but inflexibility and maintenance and logistics costs start to add cost throughout the life of the device. The apparent low cost of plastic SIMs can mask their overall costs. **Vodafone** for example has reported publicly that by halving the size of the SIM card holder it has reduced the amount of plastic used to provide customers with SIMs by around 340 tonnes a year – equivalent to a reduction of 1,760 tonnes of CO2e. By eliminating the SIM card holder altogether even greater savings would be made.

eSIM and iSIM are already in the device and can be adapted over-the-air during the life of the deployment depending on the management system adopted or the usage of remote SIM provisioning (RSP).

The integrated SIM (iSIM) moves the SIM from a separate chip into a secure enclave alongside the application processor and cellular radio on a purpose-built system on a chip (SoC). iSIMs are hardware-backed security, dedicated physical circuits rather than soft SIMs (or software). A secure enclave is hardware dedicated to protecting sensitive information that cannot be accessed. This in conjunction with a standards-compliant iSIM OS, gives iSIM it's security assurance.

Unlike a plastic SIM it can't be removed, so the subscriber identity is permanently tied to the device. This is poised to create a new market of opportunities enabled because the device identity and its communicated data can be trusted to be secure. **Counterpoint Research** estimates that iSIM-based cellular device shipments will exceed seven billion by 2030, demonstrating the fastest growth of any cellular-connected device.

The headline benefits of iSIM are that it consumes up to 70% less power than a discrete SIM, and is 98% smaller than an eSIM, measuring a fraction of a square millimetre. Further, depending on configuration of the iSIM operating system (OS), the secure enclave, process technology used and other optimizations, iSIM can deliver as high as a ten-fold performance enhancement over a discrete eSIM. The iSIM also reduces the bill of materials from three to one, with the iSIM bringing together the MCU, radio ▶

and iSIM OS running on a secure enclave into the module.

iSIM deployment status

Vincent Korstanje, the chief executive of **Kigen**, describes the current adoption status of iSIM as subject to the classic **Amazon** flywheel effect. First, the iSIM needs to be integrated into the radio chip, then the chip needs to be put into the module, and then the module needs to be selected by OEMs who create the products. Then, the mobile network operator will need to be involved to ensure the product has the right connectivity in the market in which it is deployed by creating a profile to go onto the iSIM.

"The more each of these steps happens, the faster you go around the circle and I think iSIM has now been around the circle two or three times so the momentum is growing," he explains. "The other aspect is the maturing of the iSIM ecosystem. Companies like **Sony Altair**, **Alif Semiconductor**, and **Sequans Communication**s have active iSIM implementation, and modules from vendors such as **Quectel** and **Murata** are leading OEM solutions on iSIM. We're also seeing several mobile network operators coming on board with eight out of ten module makers already adopting iSIM – some are public with their products. Commercial deployments start with 5,000- or 10,000-unit batches but we're increasingly seeing new use cases from customers who have never had cellular experience. This is a clear indicator how iSIM technology and the ecosystem approach is pulling in new players to take advantage of cellular for their IoT goals."

The mobile operators themselves are starting to embrace iSIM with **AT&T** and Vodafone announcing iSIM offerings. MVNOs have also adopted iSIM with three-to-four of the top five MNVOs in North America, Europe and APAC publicly embracing iSIM with Kigen. In the last six months, Kigen has announced iSIM MNVO customers including **floLIVE**, **Truphone**, **Soracom**, **iBASIS** and **Zariot**.

"We are entering a new chapter of iSIM's story," says Korstanje. "We now have a range of evaluation kits and hardware options to test out which one is best suited for their use case. What's exciting is this is done with not one company, but an ecosystem – so customers can advantage of deep industry expertise from multiple partners. This creates shared value for all ecosystem players, unlike the traditional value chain."

Why iSIM?

The compelling advantage of iSIM is that it offers an extremely small form factor which makes it ideal for low-cost asset tracking and a new breed of devices that are coming to market, such as adhesive labels for tracking goods in transit. Small form factor and low power consumption are important drivers for iSIM selection. "iSIM solutions are compact and usable and they can reduce device power consumption," confirms Loic Bonvarlet, the vice president of Product ▶

Marketing at Kigen. "The advantage with iSIM is that it's existence can be relied upon due to the integration, which is essential for authentication and in-field activation. The device can be turned on and there's out of the box connectivity."

"If you need optimisation, it's achievable with iSIM," he adds. "Before you were limited by a slow SIM interface. But now you can optimise the integration between the cellular chipset and the secure enclave so that you can reach stronger security and performance levels and remove the performance bottleneck that you might have with a traditional SIM."

Cost advantages

The scope and scale of this new market for secure, trusted devices is yet to crystallise, but eSIM and iSIM offer substantial cost savings over plastic removable SIMs. Recent research by **Transforma Insights** has revealed that, on average eSIM enabled devices cost 8% less to operate over the lifetime of a device than a plastic SIM and if that eSIM is part of an integrated module, the cost reduces by 11%. More substantial benefits come from iSIM, which is on average 13% cheaper than plastic removable SIMs.

The Transforma research revealed that while very low-cost plastic SIMs can be acquired for as little as US$0.10, more durable offerings are priced between US$1 and US$1.50, which includes US$0.5 for the SIM tray in the device. This is in contrast to an eSIM which has component costs of around US$2. The gap could be readily offset by the reduced logistics and maintenance costs of an eSIM in comparison to a plastic SIM.

iSIM cost advantages are little harder to quantify because there is no dedicated component cost. There is the notional cost of the secure enclave to consider within the chipset and the royalties charged for SIM OS functionality. Transforma estimates this increases the Bill of Materials cost by about US$0.50.

For situations where the business case can bear the slight increase in upfront cost of an iSIM, the repayments over the life of a service can far outweigh the initial costs. Consider the dollar amounts involved in being able to optimise connectivity and the flexibility of being able to shift operators as the location of the device changes. iSIM offers enormous potential especially for providers of mid-value and above global services because of the efficiencies it brings to manufacturing and deployment. Even further extension can be achieved by adopting RSP technologies that keep the iSIM connectivity optimised for the life of the device.

Scale would be the key disruptive force. Where iSIM comes in being a source of root of trust services is with securing data. Over the life of a device, if it can unveil new ways to use, exchange, and even trade data that is verifiable, it may spark off a true economy of trusted things. Examples exist today where iSIM-based consumer electronics, from connected washing machines to electric vehicle charging points, can ▶

become trusted sources of how the urban smart grid balances demand and supply.

"In general, iSIM is more economical because it is integrated" adds Korstanje. "Over time, it will become ubiquitous and there will be very few reasons to have a standalone SIM."

iSIM use cases

Addressing the technical challenges of how to pack needed functionality and security in an increasingly compact size, lower bandwidth to extend battery life, and use novel connectivity networks have been the holy grail of IoT design. As discussed above, the costs of traditional SIMs were high for products with low price points and procuring suitable IoT connectivity needed significant in-house expertise. However, solutions such as Wi-Fi, LoRA, SigFox and others don't have the same security assurances and resiliency of global cellular along with coverage. By addressing scale and cost, iSIM opens up a range of new use cases we did not know were possible before to a whole range of non-traditional players.

Kigen sees applications in asset tracking, especially in the transport and logistics market. "The container industry is well-equipped for container tracking, but you can have the same level of traceability down to the package level because we can now reach cost points where the business case is still justifiable," explains Bonvarlet. "Efficient operations are becoming a priority on the agenda of all governments and cities. Being able to report on the condition and mileage for the carbon footprint or monitor key performance indicators from everything from trash collections to greenhouse gas emissions is a requirement. Being able to optimise asset usage is also important for public transport, for example, and I see iSIM fuelling the data that is needed to allocate assets and budgets."

Bonvarlet foresees potential use cases where iSIM can enable asset tracking at a cost that aligns with a reduction in insurance premiums, for example, for some forms of transported assets. This type of real-world application will accelerate iSIM adoption and create a more mature ecosystem for iSIM that widens its appeal across many more verticals and use cases.

Secure identity

GSMA Intelligence has reported that 98% of enterprises what end-to-end solutions that protect data from the place of collection to the cloud, and this drives the GSMA's IoT SAFE concept, of which secure identity is a fundamental ingredient.

The ability of iSIM to secure the device identity is a core part of its value proposition, as Korstanje explains. "The fundamental asset is the ability to update security because security is a continuously moving target," he says. "Device identity is now the most important part of your security chain, starting at the chip level. It is essential to have ability to update to maintain security."

This goes to the heart of the future of IoT. "iSIM is about opening the world of IoT for completely new players who need scale. Moreover, it's about creating higher business value," Korstanje adds. "It's great to have all these devices connected, but what is IoT for? For me, it's three goals: business transformation, enabling products as-a-service, and data trading."

"To enable these goals, it's really important to have trust built through the entire supply chain and that relies on secure identity," he explains. "The iSIM now provides chip-to-cloud trust and security that allows people to know that the data originates from an authentic device, whether the device has been hacked or blacklisted, and if there is a need for the device to be updated. We know the keys are off the specific device and it can sign things and pull the whole trusted chain together to enable much more value to be extracted from those high-level services."

iSIM, therefore, has the potential to create a large community within which actors can trust each other because of the secure identity that forms the foundation of the business chain. "We want to expand the usage of secure functions inside the chips and devices," confirms Bonvarlet. "It's the two sides of the coin – we have the chip-to-cloud as one, and the second is the trust-to-cloud use case. Hyperscale cloud providers have been key advocates, rightly appreciating the need for data to be verifiable and imposing the need for secure identity. Certificates that uniquely identify each party are required to onboard devices onto their IoT infrastructure. This has catalysed demand and raised much-needed awareness." ▶

Conclusion

IoT is evolving at a tremendous pace. Each use case has its own business logic and technical trade-offs to balance. No one technology can fit all or every type of IoT device. For those business transformation goals where companies are banking on connectivity being a radical innovation on which services can be built, there is a need to assess where and how connectivity adds value. This includes understanding what the value of secure data is when it is communicated in near real-time. This is where iSIM benefits outweigh any initial costs of adopting iSIM.

The compelling change is less about the enhanced flexibility and simpler logistics that iSIM offers and more about what iSIM enables by integrating secure identity into IoT devices. "With iSIM it's not just another step in the hardware, it opens up a gateway to a new set of digital revenues that we haven't even started to scratch the surface of yet. The potential lies in looking at situations in which cost-effectiveness and power and energy efficiency can play a part to liberate secure data revenue streams," says Korstanje.

"Once you give people the tools to do that, you can start trading data because you can be assured of its legitimacy, you can pipe it through your big data cloud and rely on it," Korstanje adds. "iSIM is often presented as an evolution of same SIM technology that has always enabled the mobile industry, but it actually presents a change in how it equips people to make powerful ideas and outcomes possible. That's the promise of iSIM." ■

Smart tracking for micro-mobility in smart cities

E-bike and e-scooter fleets have stormed from city to city in just two years, re-defining urban mobility and addressing some of the most vexing transportation challenges in cities congestion, emissions, air quality, and inconsistent access to transit. Research shows the sustainability benefits clearly: if the share for e-bike riding rises to 11%, we could see a 7% decrease in CO2 emissions from the urban transport sector by 2030 – potentially accounting for over 50% of urban trips in the US and 70% in cities like London

Behind the scenes, micro-mobility solutions are complex. They connect a diversity of stakeholders – government and city councils, product manufacturers, and platform operators – interoperability is important. Vehicle operators need a reliable, long-lasting solution to locate and retrieve lost devices or to re-distribute them to places of greater usage. Their success lies in the simplicity they present to the users, who will only change their behaviours if the services offered are significantly more convenient, trustworthy, and reliable. Those who sign up to use e-scooters also offer up a great deal of personal and sensitive data, including billing information and other involuntary analytics, such as location and individual vehicle information.

Urban mobility is re-mapping the way we experience our cities

Kigen's customer is a pioneer in the development of tracking and analytic solutions for managing and servicing large fleets of micro-mobility urban transportation. The customer needs to support a unified experience for customers whilst meeting the regulatory, security and safeguarding requirements of multiple cities, across many regions. This required simplified manufacture of a low-power and compact cellular IoT enabled device that can be personalised to meet local needs and associated carrier profiles, which would allow to offer locate and retrieve functionality, reporting of lost asset, and collect utilisation statistics to drive adoption.

Kigen's integrated SIM (iSIM) operating system (OS) combined with its strong partnerships within the module and chipset ecosystem provided a route to simplifying secure manufacture and late-stage personalisation eliminating the need for multiple product development routes and inventory management. To meet the needs of citizen data security, it was essential that these edge devices are treated with the most robust security protocols – implementing chip to cloud security with **GSMA**'s IoT SAFE security scheme. This approach offers further assurances on ease of data cloud integration and interoperability.

The results

By simplifying the manufacture of cellular connected micro-mobility vehicles to offer location tracking, pattern tracking and further usability features in a compact, low power and ready to connect out of the box solution, vehicle companies now have a solution that can scale seamlessly. To ensure that the early benefits of greening our cities are realized, operators of fleets and city councils can take advantage of well-established security frameworks ensuring data of the city, it's consumers and all IoT that serves them is cost effective, secure, and tamper-proof.

Kigen's iSIM OS and solutions are built with high-growth markets of massive IoT, such that enterprises can leverage strong security even at the most constrained size, power, and cost envelopes. Through greater integration of components, longer battery life and tamper-proof protection can allow to safeguard IP and innovation for manufacturers. Much as large fleets of urban vehicles, Kigen's iSIM OS is enabling edge devices in consumer lifestyle products, in mobile medical healthcare devices as well as point of sale devices. This in combination with standards-based security scheme such as IoT SAFE is a perfect combination to support the market's growth and strengthen the social contract with users. ■

Kigen's customer is pioneer in the development of tracking and analytic solutions for managing and servicing large fleets of micro-mobility urban transportation

Fibocom facilitates digital transformation in the 5G era

Lars Thyroff, the general manager of Fibocom Wireless EU, talks with Keith Kreisher, the executive director of the IoT M2M Council, about how the company's wireless connectivity services are bringing perfect wireless experience for the industry

The construct of edge versus cloud requires technology adopters to think about how they're building out their applications

Keith Kreisher: Can you talk about the market trend of IoT, and what kind of IoT applications do you think that will have enormous potential?

Lars Thyroff: It is not a secret that the IoT industry is a very fragmented business place. Today we have six to eight volume relevant vertical markets. However, following the analyst reports there is still a big and fast growing segment called 'others'. This means there are so many industries which are innovating and going to start Industrial IoT (IIoT) mass roll-outs in future.

One of them for sure will be the charging spots for electrical vehicles (EVs).

EV charging, for one, is having huge impact within the broader theme of micro-mobility. When you consider that 80-90 million new cars are sold annually, and we reckon that at least two charging stations will be required for each vehicle, the numbers are huge. If you need to drive from point A to point B, then you will need a charging station at both locations. Saying that you will stop producing combustion engines is one thing, but it requires a lot of infrastructure build-out. This market is clearly growing but it will take a lot of public and private investment.

KK: How about high performance for edge and cloud computing needs? What role does Fibocom module play to satisfy the need of the combination of artificial intelligence (AI) and IoT?

LT: Process intelligence and decisions between edge and cloud determine today the architecture definition and design of IIOT applications. It has to be decided where process decisions are made – at the edge or in the cloud. Time critical decisions or energy consumption can be optimised with the right architecture design.

The construct of edge versus cloud requires technology adopters to think about how they're building out their applications. To cite just one simple example, you can optimise for data management or for energy consumption. This requires a lot of thinking before development can even begin.

Fibocom provides for these scenarios a 5G prepared architecture portfolio – reaching from extended mobile broadband (eMBB), ultra-reliable low latency communication (URLLC), massive machine type communication (mMTC) and mobile computing with AI capabilities.

At Fibocom, we've restructured our product portfolio to support this kind of planning, with four different categories:

A) Mobile broadband

B) Reliable low latency communication

C) Machine-type communication

D) Mobile computing and programmable system-on-chip (SoC)

This portfolio architecture comes with respective software developer kits (SDKs) to support an easy edge and cloud integration. ▶

Lars Thyroff
Fibocom

KK: Fixed wireless access (FWA) for home and business is a frontrunner in the application of 5G technology, which is a scalable and powerful complement to fixed broadband. Tell me more about Fibocom's solution for 5G FWA?

LT: We've launched our FM160/FG160 (our 160 line) of modules this year, configured specifically for 5G FWA applications. The product family features 3GPP Release 16 capabilities, backward compatible with LTE/WCDMA network standards. Powered by the Qualcomm Snapdragon X62 modem chipset, the module delivers maximum downlink rates of 3.5Gbps and uplink rates of 900Mbps under 5G. Supporting NR CA, Fibocom's 160 module series significantly optimises 5G user experience with extended coverage, boosted throughput and increased capacity.

With multiple Internet protocols and industry-standard interfaces for main operating, FG160/FM160 can be used a variety of cellular terminals such as CPE, Mi-Fi, STB, IPC and ODU. It is able to cover mobile networks in Asia, Europe and Australia. The module also supports OpenCPU, optimising cost-performance and power consumption. With OpenCPU, it can be developed into an ideal FWA solution, enabling 160MHz bandwidth, 4096 QAM as well as Wi-Fi 6E.

We are proud to see that the module series has been nominated for an Innovation Award at the Embedded World show 2022 in the hardware category.

KK: We're also hearing a lot about private networking nowadays. How do you see this playing out?

LT: Private networks are playing a vital role in the further development of Industry 4.0, but we can see also that verticals like the healthcare, agriculture, building and utility industries deploying in hard to reach areas with a private network infrastructure.

Fibocom is accelerating CBRS-based (3.5GHz Citizens Broadband Radio Service) wireless network deployment with our LTE-A Category 6 wireless communication module FM101-CG. It is able to address the requirements of CBRS-based network applications for multiple scenarios, including but not limited to remote education, industry IoT, smart cities and others.

Powered by the Snapdragon X12+ LTE Modem, the FM101-CG supports LTE TDD Band 42/43/48 and delivers maximum data rates of up 260 Mbps downlink and 30 Mbps uplink. The module can provide seamless and reliable connectivity for various industries. Organisations can make use of their own private networks, ensuring fast, reliable and secure connectivity.

With these cutting-edge technologies in place, industries are empowered to develop innovative solutions and rise to the challenge of digitalisation. In partnership with global IoT industry innovators, Fibocom is dedicated to bringing advanced connectivity services to more vertical industries with our wireless communication solutions.

www.fibocom.com

Copenhagen calling: DTW shows service providers how to optimise AIOps and scale up next gen data revenues

It used to be said that human resources are an organisation's greatest asset. Today, some argue that data is number one. It doesn't matter which camp you fall into, says Jeremy Cowan, it's time to blend the two at **TM Forum**'s 3-day event ***Digital Transformation World***, held in Copenhagen, Denmark from September 20-22. (https://dtw.tmforum.org/)

Whether you're a service provider, solution vendor or enabler, at Digital Transformation World you can expand your knowledge of **Data & AIOps** (artificial intelligence operations), enable new partnerships in the **Growth Summit**, and get your technology fix at the **Tech Summit**.

Over three days, A-List speakers will share their expertise on how to better manage your data, starting with presentations on eliminating service provider silos, and enabling scale.

This is not just an event for data analysts, it has plenty for anyone in a commercial or managerial role. All 10 of the world's largest operators will be there, say the organisers, and you can use the DTW event app to manage your time, connect and meet like-minded delegates.

Broad agenda

On Day One, Tuesday September 20, **McKinsey & Co**. will walk you through the process of unlocking value in your data, from first insights to monetisation. Here, you can find out more about eliminating data silos and enabling scale.

Also see our COO in the Spotlight interview (below) with Amit Sanyal, EVP & chief operating officer for Growth Marketing Solutions at **Comviva**.

One of the highlights on Wednesday Sept 21st will be a session led by Amy Cameron, principal analyst at **STL Partners** with commentary from Ahmad Latif Ali, associate vice president, **IDC**. The session's speakers are:

Michael Bell, **Group GM: BI and Analytics, MTN**, talking on Embedding AI across an organisation for real world impact: Where to start?

Antti Liski, lead data scientist, Elisa: What is the opportunity: Understanding the unique benefits of utilising AI across industries

Shailesh Kumar, chief data scientist, CoE AI/ML, Jio: Emergent intelligence: The next frontier of AI for complex environments

Velu Sinha, partner, Bain & Company: Building an ethical framework for AI.

Thursday, Sept 22nd features a **Masterclass on a new era of data governance** hosted by Aaron Boasman-Patel, vice president of AI, customer experience and data at TM Forum, and Wim Stoop, senior director, Product Marketing at **Cloudera**. As they point out, in recent years data governance has become more vital, driving automation and innovation in telecommunications, while navigating challenging topics of privacy and security. At the same time, migrating infrastructures from on-prem to public cloud challenges the data architect and enterprise architect alike.

Other key speakers:

There is not enough room here to list all the agenda items, so you may want to check out https://dtw.tmforum.org/ for details of presentations from speakers such as:

- Aayush Bhatnagar, SVP, **Reliance Jio**
- Antonietta Mastroianni, chief digital & IT officer of **Proximus**
- Charles Molapisi, CEO, **MTN South Africa**
- Cornelia Schaurecker, global group director, AI & Big Data, **Vodafone Group**
- Dan Thygesen, SVP, Wholesale & Platform Operations, **T-Mobile USA**
- Elsa Chen, chief customer officer, **CityFibre**
- Hesham Fahmy, chief development officer, **Telus**
- Laurent Leboucher, group CTO & SVP, **Orange**
- Monika Gullin, CTO & EVP, **Nuuday**
- Peter Leukert, Global CIO, **Deutsche Telekom**
- Vikram Sinha, CEO, **Indosat Ooredoo Hutchison**
- Yessie Yosetya, chief strategic transformation & IT officer, **PT XL Axiata** ▶

COO in the Spotlight

Ahead of DTW we asked Amit Sanyal, EVP & chief operating officer for Growth Marketing Solutions at Comviva about the challenges for service providers planning digital transformations.

Amit, service providers (CSPs, DSPs, etc.) have faced challenges with data silos for years. How can they avoid repeating silo problems in next gen data-enabled services?

Amit Sanyal: Data is a critical business asset today. Service providers are sitting on a data gold mine. It's a struggle to utilise data stored in silos across units to form a single unified customer view for utilisation across business lines.

To solve the entrenched problem of silos, service providers need to incorporate a data-driven mind-set throughout the organisation. The end goal is to better understand customers, evolve the business model and drive new revenue models. This calls for a top-down approach along with a combination of change management while keeping in mind the far reaching potential of data.

How does the industry prevent artificial intelligence (AI) projects failing as we scale up enterprise data management? By better integration processes? More agile workflows? Enhanced sharing of relevant data within teams? Continuous AI governance? Or something else?

Amit Sanyal: The goal for all organisations engaged on AI projects is to achieve the promise of AI, which will enable organisations to stay competitive in the near future. Some of the foremost reasons why AI projects fail is a balance of Data Viability, Business ROI (return on investment) and Implementation Capabilities.

Data Viability includes consolidation of relevant data across touchpoints and driving meaningful insights that contribute business needs at hand. Business ROI requires a planned methodology for defining a problem statement and measurement criteria. Implementation Capabilities are a capability analysis that includes timely build and execution of AI/ ML (machine learning) models, along with the right fit on the consumer lifecycle.

Agile workflows and enhanced sharing of relevant data simplify the way projects operate. Continuous AI governance keeps a check on our progress against the set project objectives.

Are digital twins already enhancing enterprise transformations? Can you give any examples?

Amit Sanyal: In today's world, advance level digital twins have AI-enabled systems. These are equipped with AI/ ML algorithms that are trained based on collected data. Such systems can quickly detect abnormal behaviour and initiate corrective action.

The network twin showcases a telecom use-case utilising digital twins. This presents an area with a high consequences of downtime and network failure. The twin allows modelling of the existing network infrastructure, and predicts failure points during extreme high usage scenarios such as natural disasters and power outages. This twin is also useful because it can incorporate everything from weather pattern to location of street obstacles, to deduce the impact on signal strength and thus overall network quality.

Thank you. ■

Amit Sanyal
Comviva

The goal for all organisations engaged on AI projects is to achieve the promise of AI, which will enable organisations to stay competitive in the near future

Amit Sanyal of Comviva was talking to Jeremy Cowan, editorial director and publisher of VanillaPlus and IoT Now.

DTW aims to bring the target of enterprise digital transformation within reach

Digital transformation offers enterprises in all industry sectors the prospect of reduced costs, greater operational efficiencies, enhanced customer experiences and – underpinning it all – growing profitability. What's not to like? Well, it's harder to do than to say. So, ahead of *Digital Transformation World (DTW)* in Copenhagen, Denmark (20-22 September, 2022), Jeremy Cowan talks to Nik Willetts, CEO of the event organisers, TM Forum, to find out their expectations for the conference and exhibition. ▶

SPONSORED INTERVIEW

Jeremy Cowan: The global economic and business outlooks have changed drastically over the last two years. How are TMF members adapting their business and technology platforms to such rapidly evolving markets?

Nik Willetts: Service provider growth strategies have sharpened significantly in the last two years, with a clear focus on business-to-business (B2B) – direct to enterprise and ecosystem plays, or B2B2x – in most markets. We categorise the opportunities for growth into three layers.

Firstly, next-generation connectivity: transforming connectivity to meet the evolving needs of enterprise customers, and in doing so keeping a sizeable cash-cow of the telecoms industry alive. Disruptive market forces are ripe for a shake-up of B2B connectivity, equivalent to the shift from traditional to cloud compute over the last 15 years. For connectivity, this means moving from selling technologies (fibre, 4G/5G, etc.) through traditional channels, to selling connectivity solutions, or Connectivity-as-a-Service (CaaS), via multiple platforms. Being able to move fast enough and stay profitable in this market will require a new paradigm of operating efficiency and agility, with no room for legacy software, processes, or ways of working.

Secondly, a set of horizontal growth opportunities are now gathering pace, such as end-to-end security, Internet of Things (IoT) device management, and existing communications service provider (CSP) capabilities and data. While they represent a tiny fraction of CSP revenues today, they are already offsetting declines in traditional connectivity revenues, and will only grow. These services sit at the intersection of connectivity and other digital infrastructure such as central and edge compute and specialist PaaS/SaaS, such as artificial intelligence (AI). To seize this opportunity requires compatible capabilities to the above, but also a stronger focus on the ability to rapidly partner and leverage third-party platforms and ecosystems.

Finally, the exciting opportunities behind many 5G use cases still exist: to deliver tailored end-to-end vertical solutions. But here, CSPs are becoming more selective over which verticals to focus on, and realistic over what it takes to succeed. A carefully curated ecosystem of partners is proving essential to seizing these opportunities – in particular, partners with specialist knowledge and solutions experience, paired with the right foundations in terms of operating agility and platforms.

The speed and scale of this change can be disorientating, but when it comes to putting in place the software and capabilities required to seize these opportunities, the priorities are velocity, scalability, and openness. Velocity to react to new customer needs quickly and cost-effectively; scalability to ensure solutions can scale profitably, including ▶

Being able to move fast enough and stay profitable in this market will require a new paradigm of operating efficiency and agility, with no room for legacy software, processes, or ways of working

Nik Willetts, CEO of TM Forum, talks to Jeremy Cowan, editorial director of IoT Now and VanillaPlus.

Table: **Autonomous network level methodology**

Autonomous Levels	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Networks	L3: Conditional Autonomous Networks	L4: High Autonomous Networks	L5: Full Autonomous Networks
Execution	P	P/S	S	S	S	S
Awareness	P	P/S	P/S	S	S	S
Analysis	P	P	P/S	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/Experience	P	P	P	P	P/S	S
Applicability	N/A	Select scenarios				All scenarios

P: People (manual); S: Systems (autonomous)
Note 1: System including management system, O&M tools and network.

Automation can be applied to four broad classes of functions: information acquisition, information analysis, decision and action selection, action implementation

being reusable in a variety of use cases; and openness to enable rapid partnering – directly or indirectly.

It's these needs that are driving hundreds of companies to work together to co-create the Open Digital Architecture (ODA) and Open APIs in TM Forum. ODA builds on best-practices for cloud-native software by defining reusable building blocks to enable the velocity and flexibility required for growth, combined with scalability and openness to enable the business to experiment and flex to ever-changing customer needs. Open APIs enable openness and simplify aggregation and integration with partners. What started with a focus on revolutionising traditional Operations and Business Support Systems (OSS/BSS) is now rapidly expanding to meet the needs of Cloud Native Networks for new connectivity products.

JC: What are the next steps on the road to autonomous networks?

NW: TM Forum members have identified three key concepts that an autonomous network must support:

- Intent-based instructions (the ability for a requirement or instruction to be passed from one domain to the next based on the outcome that the requesting domain desires, the intent, without the requesting domain having to understand the technical details or technology of the responding domain)
- closed loop controls (the ability for a control loop to monitor several domains and control which domain is responsible for delivering the service or attempting to deliver the service based on the service level agreement (SLA) or outcome that the control loop is working to. Control loops are used to enable autonomous systems to adapt their behaviour to respond to changes in user needs, business goals, or environmental conditions), and
- self-healing domains (the ability for a domain to monitor itself, and based on learned patterns (AI/ML) respond to degrading service output by reconfiguring itself to maintain the required service levels)

These concepts need to be built into the management and operations of tomorrow's networks at all stages of the lifecycle, from the network design, plan and build and throughout the in-life operations. While most CSPs have now started the journey to autonomous networks, the road to fully autonomous networks will be a long one.

Market-leading CSPs are now implementing automation across their technology estate (both networks and IT) with the goal of reaching conditional automation (level three) by 2025. This will require the whole supply-chain to work together to enable automatic decision making, where AI models can be dynamically updated. It's an important next step for CSPs, allowing them to have some automatic decision making within pre-defined policies or rules. It's also an important stepping stone to end-to-end automation, allowing operators to learn what automation will mean for their networks in practice, and building the confidence and competence required for full automation.

The next major milestone will be intent-based networks. This is a real game changer for the industry, opening up a range of new business models and services, as it will enable CSPs to be more agile, deploying services at the speed and cost point the market requires. In short, intent enables you to tell a system what you want, without having to tell it how to do it. We'll be demonstrating this in action at our DTW 2022 conference (Copenhagen, September 20-22) with an impressive intent-driven autonomous networks proof of concept catalyst. ▶

JC: Can you describe TM Forum's model for autonomous network uses (levels 0–5)? How does it assess a network's maturity?

NW: Automation can be applied to four broad classes of functions: information acquisition, information analysis, decision and action selection, action implementation. Within each of these types, automation can be applied across a continuum of levels from low to high, i.e., from fully manual to fully automatic. A particular system can involve automation of all four types at different levels. Based on these frameworks for automation, the autonomous network level methodology has been co-created by TM Forum members, shown in the Table above.

Clearly defined autonomous network levels have the following benefits:

- Providing guidance to operators, vendors and other participants of the telecommunications industry for roadmap planning.
- Providing reference for gap and priority analysis for future work on network autonomy.
- Providing a basis for measuring the level of an autonomous network, or autonomous network feature, along with its components and workflows.
- Providing detailed process-oriented approach and effect-oriented metrics to achieve quantised evaluation.

Several major service providers are now using this framework to assess and plan their autonomous networks journey, from current maturity to longer-range objectives, and then creating a clear plan for delivery. We're looking forward to showcasing several of these companies at DTW in Copenhagen.

JC: One of the key questions facing CSPs is how to find and retain the necessary skills to create autonomous networks. What does Best Practice here involve?

NW: Every industry is facing a skills crunch, and more broadly competing in an increasingly fierce war for talent. While these challenges span 3Rs – Recruitment, Reskilling and Retention – we believe the industry needs to focus on upskilling first and foremost, to successfully deploy and manage autonomous networks. This applies across an organisation, starting with the executive board who need to understand the value, risks and challenges of automation, and the vital role that autonomous networks will play in maintaining current revenues and unlocking growth. Equally, DevOps teams need to be upskilled and understand the impact of AI on technology architecture, as well as understanding how to deploy and scale AI safely and securely. Of course, AI and automation have a huge dependency on the data teams, exposing the right data or feature sets to train, build and design the AI models, and maintaining transparency and regulatory compliance. Demonstrating effective control and governance of AI will be critical to success, and this means the whole organisation needs to be upskilled to know how to work with AI.

JC: AI, cloud and edge need to be blended well to deliver fully automated, self-healing and self-optimising capabilities. Can you give us examples of organisations doing this well?

NW: The intersection of cloud, connectivity and AI, and end-to-end management will be an exciting battleground in the next few years, both to stay relevant and unlock new revenues. There are many initiatives in this space, from multi-CSP partnerships such as **Bridge Alliance**'s Federated Edge Hub, through to hyperscaler-led programs such as **Microsoft** with their Azure for Operators platform which is specifically designed to bring cloud and edge together. We are hosting several exciting projects with companies co-creating the answers to the challenges involved, with a focus on maintaining openness to maximise market freedom and innovation.

JC: Some CSPs are pinning their plans for growth on delivering new services for financial markets. How significant will digital banking and mobile wallets be for Service Provider revenues in the next two years? And how should they build partner ecosystems to create a one-stop fintech solution?

NW: Mobile payments and mobile financial services more broadly are already an important market for many telecoms operators. For example, all four of the large African telecoms groups - **Vodafone**, **Orange**, **Airtel** and **MTN** generate 2-4% of their total revenues from financial services.

For these operators, the next wave business-to-consumer (B2C) service growth requires evolving these capabilities into true platform businesses, enabling innovation and growth across the financial services sector. Operators who make it easy, through their technology platforms, to be a foundation for innovation will stand the best chance of success. Deploying Open APIs - and demonstrating the availability of Open APIs to partners and innovators in other sectors - will be crucial. But it's also about designing IT systems in their own businesses that are designed as much for ecosystems partners - and meeting their requirements - as for CSPs' own customers.

The intersection of cloud, connectivity and AI, and end-to-end management will be an exciting battleground in the next few years, both to stay relevant and unlock new revenues


KORE®
Start with One Innovation to Power the Future
Start with KORE
The world's pure-play provider of IoT connectivity, solutions, and analytics. Our bundled solutions let you focus on innovating and creating, while we concentrate on simplifying the complexities. Learn more.
www.korewireless.com

US Mobile World Congress is a showcase for new things

The inaugural Mobile World Congress Las Vegas event takes place from the end of this month, and it is set to lay a roadmap for the issues and opportunities the mobile industry will meet on its continuing digital journey, writes Tony Savvas

Hosted jointly by the **GSMA** and US **CTIA** (the Cellular Telecommunications Industry Association), the event is the North America edition of the MWC Series. It was previously located in Los Angeles before this year's Las Vegas switch.

Between now and 2025, a staggering US$5 trillion will be contributed to the global economy by mobile technologies and services, says the GSMA, with one billion 5G connections forecast by the end of 2022 alone. The show will study and track this growth.

MWC Las Vegas will take place at the Las Vegas Convention Center's (LVCC) new West Hall, from 28-30 September 2022. CTIA will host its Everything Policy track, bringing policymakers together with key wireless industry stakeholders to discuss trends and developments in government and public policy.

New venue

MWC Las Vegas's West Hall location opened in 2021 and features 600,000 square feet of exhibition space. Over half the exhibition space is column-free, and at 328,000 square feet, it is the largest such space in North America. The West Hall's entrance lobby and atrium feature a 10,000-square-foot digital screen developed by **Samsung**.

The West Hall is also served and connected by an innovative underground transportation system, the Las Vegas Convention Center Loop. Designed by Elon Musk's **The Boring Company**, the system transports convention attendees throughout the 200-acre campus in under two minutes in **Tesla** vehicles, free of charge. In addition, the Las Vegas Monorail is an elevated, all-electric train system that provides direct access to various hotels/ resorts in Las Vegas. ▶

MWC Las Vegas will take place at the Las Vegas Convention Center's (LVCC) new West Hall, from 28-30 September 2022

ikotek

Your Trusted IoT ODM Partner

Join us at MWC - Las Vegas Convention Center, stand W1.520

Manon Brouillette
Verizon

Jeremy Legg
AT&T

Meredith Attwell
CTIA

Keynotes

As the recently appointed executive vice president and CEO of the **Verizon** Consumer Group, Manon Brouillette will make her debut public keynote at MWC Las Vegas. There will also be a joint keynote from AT&T chief marketing and growth officer Kellyn Smith Kenny and **AT&T** chief technology officer Jeremy Legg.

Among others, there will be additional keynotes from **Boingo Wireless**' chief executive officer Mike Finley, CTIA president and CEO Meredith Attwell Baker, and **Red Hat** president and CEO Paul Cormier.

"MWC is the industry's long-standing destination event to convene, get deals done and exhibit ground-breaking products," says GSMA CEO John Hoffman. "At MWC Las Vegas we will bring together the digital mobile ecosystem in a new light at the Las Vegas Convention Center's prestigious state-of-the-art West Hall."

Companies that are sponsoring, exhibiting and participating at the event include Verizon, **T-Mobile** for Business, **ServiceNow**, **Amdocs**, **Celona**, **Cisco**, **Dell Technologies**, **Hewlett Packard Enterprise**, **Kigen, KORE**, **Kyndryl**, **Movandi**, **NoviFlow**, **Palo Alto Networks**, **Red Hat**, **Syniverse** and **Teal Communications**, among others.

Show themes

Under the umbrella of Connectivity Unleashed, MWC Las Vegas will provide a platform to show how innovative solutions from the mobile and digital ecosystems are "truly transforming the digital world", says GSMA.

Attendees will have the opportunity to dig into the themes of 5G Connect, the Internet of Everything, CloudNet and Tech Horizon, across keynote stages, networking receptions, exhibition halls, an extensive conference and partner programme, and demos.

As for 5G Connect, Alizeh Abbas, conference content manager at the GSMA, says: "There will be one billion 5G connections this year and the growth is not only significant for the telco industry, but for all industries. We will be looking at 5G Advanced, 5G private networks, rural connectivity, green issues and gaming."

The Internet of Everything group of events will look at how IoT also cuts across different industries. "This is not just about the 'things'," says Abbas, "this is about how they connect with each other and how they speak with each other intelligently, and how we merge the physical and virtual worlds together. Among other issues, we will be considering digital twins, smart cities and security."

The Tech Horizon conference segment will be considering what new technologies and solutions, not just those in mobile, organisations can embrace to tackle the world's challenges and problems. The future of technology in manufacturing, health, financial services, gaming and entertainment, among other areas, will be considered.

As for CloudNet, the conference will consider the projection that the telco cloud is set to become a US$100 billion market by 2030, according to the GSMA. It will look at how telcos can make use of their existing relationships with cloud providers to become the new digital service providers at the edge, says the GSMA. ▶

MWC is the industry's long-standing destination event to convene, get deals done and exhibit ground-breaking products

Paul Cormier
Red Hat

Romil Bahl
KORE

Joe Peterson
Ikotek

Las Vegas summits

In addition, GSMA summits include the eSIM Summit, held on Wednesday 28 September. According to GSMA Intelligence's "eSIM: State of the consumer market and the road ahead" report, by 2025, 2.4 billion smartphone connections will use eSIM globally. The North America eSIM Market will see growth of about 15% during the forecast period (2022-2028).

eSIM has become more important than ever because of more devices being connected every day in every vertical market, and the requirement to manage devices remotely is increasingly growing too. Furthermore, the adoption of IoT devices in every market is increasing, leading to growing eSIM development to match different use cases.

This summit will focus on these trends and will provide the opportunity to get detailed information about the factors influencing market demand, growth, challenges and opportunities.

Matt Hatton, founding partner at analyst house **Transforma Insights**, says: "eSIM is a digital transformation process that mobile network operators (MNOs) have to navigate. As with other digital transformation exercises, the challenge is not in introducing a single new technology. It is in understanding the impact that the technology will have on the wider operations of the organisation."

"While the technological hurdles are significant, adopters must equally give ample consideration to the commercial implications of deployment, challenges of integration, and how to make the appropriate changes within their organisations," he says. "It is as hard to change organisational working practices, processes and business models as it is to adopt new technologies. And so it is with eSIM."

Open RAN opportunity

The Open RAN Roundtable will take place on the morning of Thursday 29 September.

The mobile infrastructure supply chain needs innovation and growth to meet the increasing demands of our changing digital society. Open RAN is emerging as a critical enabler to increase supplier choice, agility and flexibility to meet new use cases.

Open RAN is an opportunity, not a threat, says the GSMA, as it enables mobile operators to use equipment from multiple vendors for differing use cases and still ensure interoperability. "An open environment expands the ecosystem, and with more vendors providing the building blocks, there is more innovation, greater service flexibility and there are more options for operators to meet the demands of the 5G era," the GSMA says.

In the roundtable, attendees will discuss the deployment maturity of Open RAN solutions, the momentum Open RAN has created, its challenges, the opportunities that can be commercialised, and the scale Open RAN may well achieve by 2025.

On the same day, later in the afternoon, the Open RAN Summit will be an opportunity to hear about the latest Open RAN specifications, software developments, industry adoption and about successful network implementations in the US and beyond.

Also on 29 September, the 5G mmWave Summit will take place. Attendees will hear how 5G mmWave is unlocking the full potential of 5G and learn about deployment best practice from some of the industry's leading experts.

Industry issues

Shahar Yaacobi, head of strategy and growth at **Amdocs IoT**, says the subject of eSIMs, will definitely be a "lively issue" at the event. He says: "The recent launch of the iPhone 14 is yet another proof point that the embedded SIM is here to stay. Since Apple started incorporating the technology into its smartphones several years ago, followed by Google, Samsung and others, for owners of these phones, changing providers meant simply downloading a virtual SIM, no matter where you are – just like any other app. To date, eSIM has been adopted by all the leading device manufacturers and is in use in smartwatches, smartphones, tablets, laptops and many other consumer and enterprise IoT devices. In the long-term, the plastic SIM will no longer be available."

As he points out though, the ability to use an eSIM depends on both the device and the network provider supporting it. "While device OEMs widely adopted eSIMs, telcos were slow to respond and prepare for the digital transformation of the SIM card," Yaacobi says.

Transforma Insights' Hatton says: "The old plastic SIM will probably be consigned to the dustbin of technology history some time in the next decade. The eSIM is the future, not least because it will end up being cheaper and more customer friendly. Every MNO will need to change to reflect that."

He says billing and IT systems, customer care, customer lifecycle management, inter-MNO relationships, product offerings and user experience will all need to adapt to the "new reality". These are significant changes that MNOs need to make in a relatively short timeframe. They will need partners, and they will ideally use a proven and scalable cloud-based solution to deliver all of the necessary complex interwoven elements of an effective eSIM strategy, adds Hatton. ▶

Sponsored by:

ikotek
Your Trusted IoT ODM Partner

KORE

Romil Bahl, the president and CEO of KORE is looking forward to the show. "MWC Las Vegas is a great forum to reach a diverse audience of forward-thinking individuals from a variety of industries," he says. "We have prioritised our investment in the event and expect to see engagement and growth from it."

KORE says it will be introducing several new industry collaborations in Las Vegas, as well as sharing details on new innovations. One of its demonstrations at the show will focus on the new KORE Connected Hub, as the next key release within its Connected Health Telemetry Solution. Organisations face myriad complexities in secure data transmission between patient and provider when delivering health solutions like remote patient monitoring, medical alarms and personal emergency response systems, and medical equipment monitoring.

Bahl says: "Most connected health providers are forced to develop their own telemetry solution, when in fact, their real expertise is developing the analytics, workflow, care delivery optimisation and use of the data to improve patient care and outcomes. Our Connected Health Telemetry Solution helps these solution providers accelerate the time-to-market and adoption of large-scale connected health initiatives."

Joe Peterson, the CEO of Ikotek, the IoT original design manufacturer (ODM), says: "Organisations looking to bring devices to market face a range of challenges, including the cost of design, development and manufacturing, as well as the complexity of global certification, all of which can delay IoT projects. At the show, Ikotek will be discussing with its current and future customers how working with a specialist IoT ODM can help eliminate these risks, reduce costs and bring IoT devices to market faster."

He adds: "Attending is a great opportunity to introduce Ikotek as a trusted, specialised, US-headquartered global ODM provider for IoT."

Whether it's learning more about the evolution of IoT networks, considering the effects of the global 5G roll-out, or how mobile networks are becoming more scalable and intelligent, there's plenty for everyone who attends the show.

MWC Las Vegas will take place at the Las Vegas Convention Center in the West Hall on 28-30 September.

KORE says it will be introducing several new industry collaborations in Las Vegas, as well as sharing details on new innovations

Many technology complexities lie under the surface of the IoT iceberg

The Internet of Things (IoT) at a high level is relatively simple – you have sensors in IoT devices that take readings and communicate that data through the internet and into the cloud, to another device, or to some type of analytics user interface. Essentially, data is collected and can then be interpreted into actionable insights. If you have a piece of equipment on the production line in a manufacturing plant with a sensor-based IoT device attached. This device is monitoring the health of that machine to make sure that the needs of the machine are met before damage or downtime occurs. Unplanned downtime is one of the biggest cost drivers in industrial manufacturing posing a US$50 billion annual threat to manufacturers

These industrial IoT (IIoT) devices are a critical factor in a successful production run, so it stands to reason that manufacturers rely heavily on the ecosystem of these devices to work. It is increasingly likely that modern, cost-efficient IoT devices are replacing older technologies to measure all types of information within an industrial plant, such as temperature to avoid overheating and damage to equipment and products, pressure in tanks that hold liquids, and so forth.

This is what **KORE** refers to as the visible part of the iceberg when it comes to IoT. The end user, which in this example is the manufacturer, is overseeing, managing and benefitting from their IoT-enabled solution represented by the part of the iceberg above the water line. But underneath the surface is so much more that supports what is seen above the surface. And this is where all the complexity comes in.

The rest of the iceberg

What is under the surface – the other 80-90% of the iceberg – are all the intricate complexities of IoT that drive an IoT ecosystem's operations and successes. It begins with the device itself. That device needs a SIM card – whether that is a traditional SIM or an embedded SIM (eSIM) – which needs to be activated on a carrier network and the device needs to be configured to the network. This process allows devices to work out of the box when they arrive as part of a deployment. Then a gateway or router is required, which needs to be device and network compatible.

All hardware needs to be kitted and shipped in a manner that is aligned with the organisation's deployment, which if devices or hardware are coming from multiple original equipment manufacturers (OEMs) or wholesalers, can get relatively complicated rapidly. As the IoT infrastructure is built, composed of device, networks and applications, more and more touchpoints are added, and each requires a certain number of tasks and considerations so that everything works properly.

What has just described is mostly concerned with the initial deployment of an IoT solution. The management of IoT can be just as complex. Imagine that you are an OEM, and you have 1,000 IoT devices on your manufacturing floor helping you manage operations for five different product lines or devices. Each line has 200 devices helping to monitor the health of the production line, and each group has its own lifecycle, which might be anywhere between two and ten years. ▶

What happens when one group of devices reaches the end of a lifecycle? Suddenly, the carousel of device management and logistics never stops turning, and it is a constant effort. You must deploy new devices using the same process of ordering, activating, configuring, kitting and shipping as before. It starts to get complicated just running the logistics of keeping the right number of devices online and working.

We could further complicate this scenario by including any regulatory compliance to which this OEM must adhere when introducing devices into operations or data collection and storage. This is certainly true when you consider IoT in connected health deployments, which have regulatory compliance intricately weaved into the many aspects of patient data collection and transmission. Or, if you want to deploy solutions globally, devices, network communications, data storage and so on fall under different regulations and compliance as your IoT deployment of origin. And of course, different connectivity protocols – or even if the deployment is entirely in LTE – different MNOs are required for resilient, high-quality local connectivity.

All of this demonstrates how IoT solutions can get very complicated, and that can hinder success because, as I previously stated, the end user is interested in the tip of the iceberg and might not have the time, resources, or finances to manage the under-the-surface details that support success. Further, one might argue that they should not need to worry about these details – their concern should be driving their desired outcomes, not putting the Lego pieces together – and finding a partner that can do many of these pieces for an enterprise end user is increasingly a critical success factor in IoT.

Tackling complexities below the surface

Beecham Research famously published a study a few years ago, 'Why IoT Projects Fail'. In the survey, only 26% of those surveyed reported being successful with their IoT initiatives. That amounts to a pretty high failure rate. While there are many factors at play, including some objectivity on what might be considered a success, a lot of the struggles and issues listed in the study fall under the umbrella of IoT managed services.

The whole picture of IoT is made up of those smaller, yet critical pieces, such as lifecycle management, logistics, configuration, and so forth. That is what drives success and what drives return on investment. But it can be incredibly difficult to bring all those pieces of the puzzle under a single roof while trying to prove the value of the IoT solution. It gets to be time-consuming, expensive and hard to justify. ▶

All hardware needs to be kitted and shipped in a manner that is aligned with the organisation's deployment, which if devices or hardware are coming from multiple OEMs or wholesalers, this can get relatively complicated rapidly

One growing segment in the medical industry is using IoT to digitise healthcare and treatment delivery

One growing segment in the medical industry is using IoT to digitise healthcare and treatment delivery. On one side of this emerging segment called connected health is remote patient monitoring (RPM), which utilises patient-controlled devices that collect data that is then sent to a medical provider to monitor. For example, if a patient has chronic cardiac disease, it could be important for a provider to monitor the blood pressure of that patient and watch for trends proactively instead of it becoming a crisis that leads to patient hospitalisation. The patient takes their own blood pressure and that data is sent directly to an interface that the provider can access. This can lead to improved outcomes for the patient, since they are proactively managing a chronic disease, and it also can lead to growth opportunities for providers without the overhead of expanding a physical location.

On the other side of the segment are decentralised clinical trials (DCTs). When creating new treatments, the traditional in-clinic approach to clinical trials can have challenges, including inaccurate data collection, patient participation throughout the trial, as well as recruiting patients that are able to make frequent trips to the clinic for data collection. These hurdles can slow time to market and be costly to the contract research organisations (CROs) and pharmaceutical companies running the trials. By using the same type of patient-driven medical devices to collect patient data, as well as digital diaries, data collection and discovery can run much smoother. The benefits of connected health solutions can be clear, but the path to launching these solutions can be difficult. The logistical and management side of an IoT infrastructure is not something to overlook when building out solutions. Effective and efficient configuration, kitting, shipping and returns management are crucial in connected health solutions. Whether it's equipping hospitals, medical practices, clinics or direct to patient, getting solutions deployed and running out-of-the-box is incredibly important. Mobile device management (MDM) is also a significant task and working through a fragmented ecosystem can be an overwhelming burden.

Hardware procurement, logistics and lifecycle management are all another significant slice of the pie that require a lot of attention and detail. Many healthcare solution providers do not have the internal resources to manage the wide and complex hardware and product lifecycle required in connected health solutions.

Finally, regulatory compliance is, of course, vital to any healthcare ecosystem. CROs and pharmaceutical sponsors can go two routes with the hardware procurement and kitting of devices. The first path is using light-touch managed services by having a third-party source, test and ship the individual device and hardware pieces.

Then the CRO can assemble the entire hardware kit in-house through their own regulatory compliance.

The second path is to use a full managed services provider that includes MDM, deployment and logistics, and project management all through FDA- and ISO-certified facilities. The opportunity to enter the market in DCTs is expansive, but implementation is complex, and requires the careful orchestration with CROs and experienced IoT managed service providers.

KORE is an expert provider of managed services for IoT both for general applications, as well as connected health applications. For deployments that require light-touch managed services, the KORE team in Westbury, New York, allows organisations to quickly receive devices and hardware while supporting regulatory compliance.

The KORE Westbury office has a track record of success including providing services for:

A US-based a medical company that leads the way in digital transformation of life sciences, was in urgent need of 5,000 global iPhone devices with established connectivity shipped to Europe and the USA within a two-to-three-week timeframe. With a robust ecosystem of partners to acquire hardware, KORE was able to provide the company with the supplies it needed by linking KORE's global vendors to secure the **Apple** units ▶

required and delivered the products in the timeframe needed by the customer.

A leading provider that issues technology solutions and clinical research services, needed to bring connected devices and SIMs to South America – a region that had previously not been shipped to due to strict importation rules. KORE quickly collaborated to resolve the importation matter. KORE served as a one-stop-shop for the company's global sourcing in the connectivity and device management space.

Another example is a government programme that provides funding to schools and libraries across the US for those in need of remote learning protocols due to COVID 19. In 2021, **T-Mobile** contributed a large portion of donations to fund these services, as well as enabled primary agents, such as KORE BMP and its registered partners, like **OmniPro** to deliver connected laptops, tablets and equipment to schools and libraries for students. For full-scale managed services, KORE has a state-of-the-art facility in Pittsford, New York, that can manage comprehensive staging, kitting and logistics, both forward and reverse, under one roof all while meeting regulatory compliance.

KORE has also been instrumental in helping solutions delivery for a top-three global supplier of cardiac rhythm management devices. This multinational company creates solutions where patient transmitted data is uploaded to a proprietary, safe, and secure web-based data management system that is protected with industry standard safety protocols. The ability to do this is a difficult feat, and the company needed help, so it turned to KORE.

KORE provides the company with a comprehensive service model that includes hardware selection and sourcing, wireless connectivity, and ongoing device management and support. With this customer relationship, the company can essentially place an order with KORE to roll out more solutions. KORE takes care of the complexities in hardware procurement, connectivity and management. This, in a way, makes KORE a valuable extension of the company, almost as an independent IoT department.

Success in IoT

Harking back to the statistic mentioned before about the success rates for IoT and how slim the chances appear to be for organisations to enjoy the optimisation and efficiency benefits of IoT. That number is going to grow larger and larger because of IoT enablement solutions that overcome those complexities.

The benefits of IoT – whether that's in an industrial or clinical setting or in fleet, automotive, and transportation, assets, utilities, and on – are too great to be ignored because it seems too challenging and IoT managed services are designed to help.

KORE provides the company with a comprehensive service model that includes hardware selection and sourcing, wireless connectivity, and ongoing device management and support

www.kore.com

IoT innovators turn to ODMs to accelerate design, manufacture and certification

As IoT businesses look to bring products to market, they need to accelerate the design to deployment process, assure compliance and optimise costs. These activities rely on specialised people, dedicated facilities and deep knowledge of global markets. For most, whether they're established corporations looking to digitise their business model using IoT or a start-up looking to bring innovation to the market, assembling all these skills, capabilities and capacity is out of reach. The alternative is to shift tasks to an original design manufacturer (ODM).

These typically take away the pain of a discrete process or have deep understanding of a single geographic marketplace but what's really needed is a global ODM that can handle multiple processes from design through manufacturing to testing, validation, certification and launch. Delivering that end-to-end, global capability is the goal of Joe Peterson, the chief executive of Ikotek, a US-headquartered IoT ODM aiming to streamline the product introduction process for IoT companies large and small.

Peterson has more than 27 years of industry experience having worked at Motorola, Siemens, Gemalto, Telit and Inseego. He most recently held the position of vice president of IoT Sales for North America at Quectel Wireless Solutions where he spun out and launched Ikotek as a US entity to serve the global ODM needs of the IoT sector as it matures into a mass market. Here, he tells IoT Now why the market needs a global IoT ODM and how Ikotek can help companies accelerate their launches, optimise costs and handle the complexities of certification ▶

SPONSORED INTERVIEW

Joe Peterson
CEO, **Ikotek**

Until Ikotek, there had not really been a true US-based IoT ODM that is focused on serving the mid-market

IoT Now: Why has Ikotek been established now and what are the drivers in the IoT industry that encourage enterprises to look for an ODM service provider?

Joe Peterson: Until **Ikotek**, there has not really been a true US-based IoT ODM that is focused on serving the mid-market. There are number of legacy ODMs that have significant penetration and a lot of feet on the street but we have found these are not purely IoT focused and tend to pick and choose only high volume IoT projects targeting only the top two or three customers.

We can support those organisations too but we feel there's a much broader need out there for a US-based IoT ODM to serve the mid-market. Our goal is to offer an extensive ecosystem of resources and help our customers bring products to market quickly and cost-effectively. We're certainly already doing this.

IoT Now: What capabilities does Ikotek have that make it stand out from the other joint design manufacturer (JDM) and electronics manufacturing services (EMS) providers?

JP: Our team is purpose-built for IoT ODM, JDM and EMS capabilities. We're registered and incorporated in the state of Delaware and we've brought in individuals with the experience of doing full system solutions. We focus on system level designs and full product level designs and we're also ensuring products are certified. We're a one-stop-shop for design, development, manufacturing and certification and all of that is done on a global basis. We cover the world with design centres and manufacturing capabilities in all regions and have IoT experts available at every step of the way.

IoT Now: Would you say that customers are driven by the need to accelerate their time-to-market, by the shortage of IoT-specific technical skills in the market, or possibly both? ▶

IoT companies are driving their core business focused on recurring revenues enabled by connectivity and their platform services and that's why we exist

JP: It's a combination of both. Time-to-market for everybody nowadays is even more critical that it has been in the past because competition is fierce. There are always new entrants coming in who want to try and take over and be a step ahead of companies that have been an incumbent for years. In some areas, the race is on for innovators to get to market first and have such a lead they can dominate the sector.

In either case, a lot of companies now don't want to bring resources in-house to build hardware. They want to focus much more on their platform and services and have somebody else on the outside do the design and development for them. That results in a tight collaboration with the likes of Ikotek so that we build the hardware to their specifications.

IoT companies are driving their core business focused on recurring revenues enabled by connectivity and their platform services and that's why we exist. Companies don't want to have hardware engineers on staff when product lifecycles are long and innovation is driven from platforms and software.

Our ability to keep a broad scale of the types of IoT devices under development means we're constantly sharpening our experiences and understanding of where things are headed. We're constantly bringing in the right resources, experts and capabilities. In the second quarter of this year alone, we added 140 new engineers and we continue to hire which means we have the ability to bring in the competency to stay ahead of where the market is going. We can therefore ensure that we get our customers to market in a quicker fashion, but also that we do so while keeping ahead of the technology shifts to support innovative customers using the latest technologies.

IoT Now: Is it fair to say that in general, there is a shortage of technical skills available on the market? Is that something that you have found as you as you build the business?

JP: I would say that skills exist but the challenge is whether you can get that many people into an organisation and whether you want to carry the burden of the cost? Most enterprises struggle to recruit at volume or afford the wage bill focused on a limited number of products or devices. ▶

For us, we can attract skilled people and combine them across our business. This means we quickly can assemble a team of experts for a specific project and support our customers' needs comprehensively for the duration of their project. We're staying ahead of the curve by building teams of engineers and experts across every step of the IoT value chain – from hardware and software engineers to platform and testing experts. That's in contrast to a lot of companies who might have to go out and constantly try to hire to make sure that that competency exists inside their organisations.

IoT Now: How important is it to offer a complete portfolio of services so a company could come to you and get everything from design through to certification and not have that headache when it comes to hardware?

JP: I think having the one-stop-shop capability is a very key component to what makes Ikotek stand out amongst the competition. A lot of companies today need to outsource because projects come and go. A lot of times, you'll see that certain companies will develop a solution and it's one that they'll keep in the market for four or five or maybe even ten or 20 years. If they're not constantly innovating for example in the hardware, they've got a bloated organisation with staff who bring little value to the business at substantial cost. Whereas, if they outsource to Ikotek, we can be that extension for them for the period of time that they need us in all of the disciplines across design, development, certification and manufacturing. They could just give all of that to Ikotek as a one-stop-shop, and then don't need to worry about right-sizing resources.

When customers come to us, they know that from top to bottom, the individuals inside our organisation, which make up a broader team, have all those competencies, and they don't have to worry about lack of expertise that they might not have in-house and constantly have to hire for.

IoT Now: Outsourcing is usually a way to be quicker, but it's typically expensive for customer organisations. How have you structured Ikotek to ensure quality and speed can be delivered, but the price is still appealing to customers?

JP: We address cost optimisation through our global structure and setup. Being a US-headquartered organisation means we've got a staff of individuals here, a management team, and also across the globe, whether it's in Europe, Americas or Asia. We've distributed the resources accordingly and appropriately to first make sure that we manage to the local requirements of the region, but also in terms of finding competence centres that keep us cost competitive. We ensure our global presence matches the needs of our customers.

IoT Now: What are your plans for developing Ikotek's business?

JP: We continue to build our organisation and competencies across commercial and technical teams on a global basis. We're now set up in the US, Europe and Asia and we're growing out our broader organisation in each region to ensure we can support all our customers' needs across every step of the ODM process.

IoT Now: How do you see the trend towards this kind of outsourced approach to IoT? Do you think that IoT hardware development will continue to become more prevalent?

JP: We see a strong trend for IoT hardware design and manufacturing services. A lot of the design wins that we have today are from long-time, well established and very knowledgeable IoT companies. The fact that they're trusting Ikotek, to take on everything from design all the way through to manufacturing and certification, says a lot. It means Ikotek is validated by some of these longstanding IoT companies who have traditionally always owned their own hardware development. This is a clear sign that validates who we are, our business model, customer value and the plan we have in place.

We believe we're on the edge of a large volume move towards IoT ODM. It's just in its infancy right now, but IoT is a very fragmented market and that has made it difficult for a lot of players to enter the market. We know how to manage the fragments and have scale and resources to handle the huge growth of connected devices. The market is massive and is only going to continue to grow.

We've seen the scale of growth and many of the new use cases that continue to be brought to life. As the new entrants come, a lot of them have the great concepts and innovation, but not necessarily the knowledge and in-house resources to do that. Outsourcing design and development is becoming a much broader practice than it's ever been and we're in the right place at the right time to make our customers' ideas reality.

I think having the one-stop-shop capability is a very key component to what makes Ikotek stand out amongst the competition

www.ikotek.com

SIMPLE SCALABLE SECURE IOT

Enable and manage reliable and secure global IoT connectivity with VELOS IoT.

- +600 Networks in +200 Countries
- LPWAN & NextGen Network Services
- Carrier-grade Management Platform
- eSIM / Multi-IMSI

velosiot.com

velos

How will OEMs manufacture the smart factories of the future?

Sponsored by:

THALES
Building a future we can all trust

velos

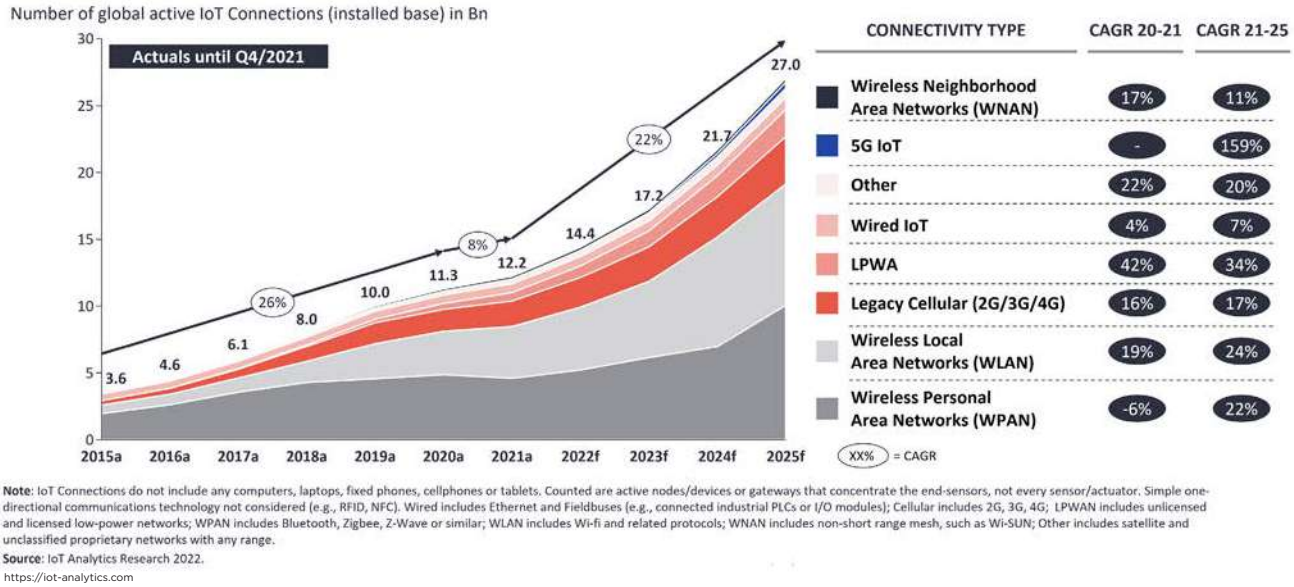
Will OEMs be able to manufacture the smart factories of the future?

IoT relies on manufacturing efficiency to get massive volumes of devices out into the market at an acceptable price and rapidly enough to take advantage of opportunities. Manufacturers have been challenged to ensure all the capabilities an IoT device needs can be accommodated within often small form factors without causing interference or excessive power consumption. These design issues then become production issues as the factory environment needs to be able to take account of variations while working within size, weight and price constraints.

Automation and robotisation are stripping costs from manufacturing environments and IoT organisations are practicing what they're preaching by using sensors, robots and other devices to drive efficiency. The rewards are enormous because the sheer scale of IoT means that every cent saved in manufacture is multiplied many times over because of the large volume of devices that original equipment manufacturers (OEMs) are constructing. This is exacerbated in markets such as the automotive sector in which complex systems and sub-systems involve multiple devices and components which need to be pre-integrated where possible in the factory.

The advantage of adding as many functional blocks as possible at the point of manufacture is that it simplifies and accelerates deployment and installation of IoT devices enabling use cases to become reality faster, less expensively and with minimised manual or physical interactions. From security to connectivity more can be designed-in to devices and built-in at the factory, enabling simplified logistics, fewer device variants and smoother routes to achieving global compliance ▶

SPONSORED REPORT



Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2022.

https://iot-analytics.com

Figure 1: Global IoT market forecast in billions of connected devices
Source: IoT Analytics, May 2022

Although easy to understand from a conceptual point of view there are substantial production complexities, security, connectivity, reliability and compliance issues for OEMs to overcome and they must do so as their production lines scale up to meet demand for the next generation of IoT devices

Research firm **IoT Analytics** has reported that in 2022, the market for Internet of Things is expected to grow 18% to 14.4 billion active connections. The firm estimates that by 2025, as supply constraints ease and growth further accelerates, there will be approximately 27 billion connected IoT devices. Someone is going to have to manufacture these and OEMs are gearing up to enable as many functions as possible to be integrated into the devices they build. The advantage of this approach is that fewer steps are needed in the process of bringing a device to the point of use and significant cost and time can be saved.

To achieve this across all industries and global markets, further standardisation will be needed but industrial regulation, communications technology legislation and IT standards provide a broad foundational framework for manufacturers to work to. This includes contract manufacturers making IoT devices on behalf of others alongside brands that also build their own hardware. To bring the price down and speed up, manufacturers will have to adopt IoT technologies in their factories to power their digital transformations and enable improved productivity, increased efficiency, lower costs and faster reaction times.

Get the factory right first

None of this is easy and although consulting firm **McKinsey** projects IoT could enable US$5.5tn to US$12.6tn in value globally by 2030, it warns that organisational challenges, technology cost, cybersecurity threats, lack of interoperability and convoluted installation requirements have resulted in many initiatives becoming stuck at the pilot stage. The starkest example of this, the firm says, is in factories where 70% of manufacturers have been unable to scale beyond pilots. ▶

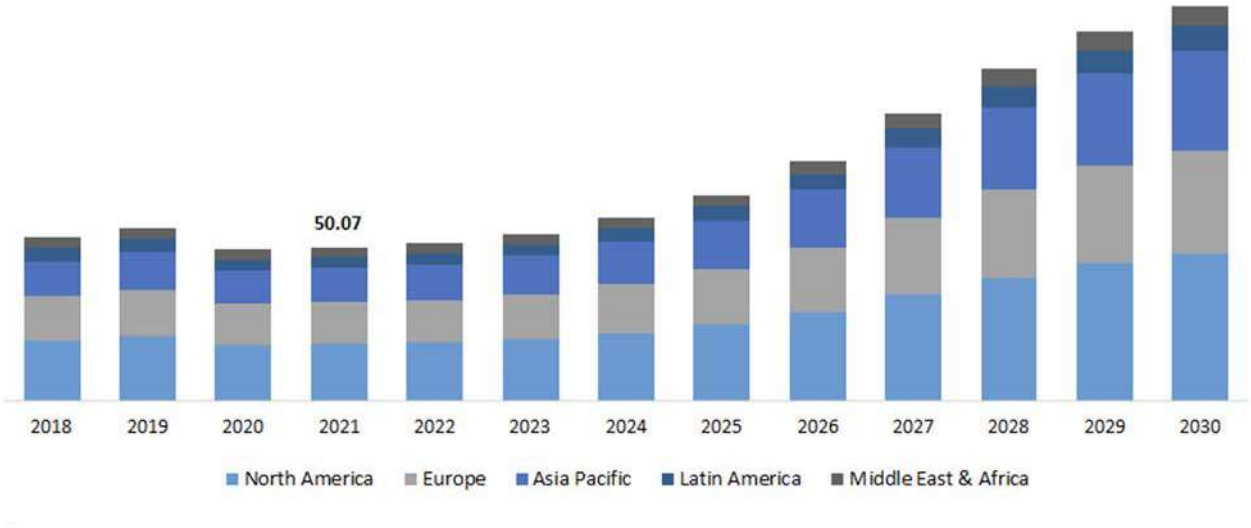


Figure 2: IoT in manufacturing market size by region 2018-2030
Source: Polaris Market Research

The smart factory is an essential enabler of smart manufacturing and the capabilities that massive IoT demands and therefore needs to be prioritised so it can deliver the performance IoT brands, service providers and product companies need. This isn't new and manufacturers have already made substantial investments in their own digital transformations.

ABI Research has predicted that spending on smart manufacturing will grow from US$345 billion in 2021 to more than US$950 billion in 2030. "As manufacturers advance their digital transformation initiatives, they drive up spending on smart manufacturing with investments in factories that adopt Industry 4.0 solutions like autonomous mobile robots (AMRs), asset tracking, simulation and digital twins," the firm's research director, Ryan Martin, has said.

Polaris Market Research sees significant expenditure specifically on IoT solutions in manufacturing. It reports in **Figure 2** that IoT in the global manufacturing market was valued at US$50.07bn in 2021 and is expected to grow at a CAGR of 12.3% over the period 2021-2030 when the revenue is forecast to hit US$129.42bn. Implementing technology in a wide range of applications across many industries has created a huge opportunity for companies in the market, the firm says.

The manufacturing sector's increased demand for automated machines and equipment will lead to increased usage of IoT technologies, according to Polaris Market Research. IoT in the manufacturing industry will need to respond to growing demand for customisation, heightened expectations for simpler products and the requirement for efficient and reliable data. Innovations including sensing devices and virtual and enlarged reality will add further pressure while concerns about data protection and privacy and a lack of precise standards for interoperability and connectivity limit what OEMs can do to stimulate IoT and hit large volumes.

Why manufacturing is so important

If you can't build hundreds of thousands – or potentially more – of devices that can be shipped anywhere in the world at a price-point that is viable while offering the connectivity, security, compute power and compliance with regulations that sales demand, your IoT concept will not become reality. OEMs and manufacturers therefore play a fundamental and critical role in making IoT happen at scale.

When McKinsey assessed the potential for economic impact in 2030 across a range of business settings, the factory setting had the greatest economic potential. The firm estimates that the economic impact of IoT ▶

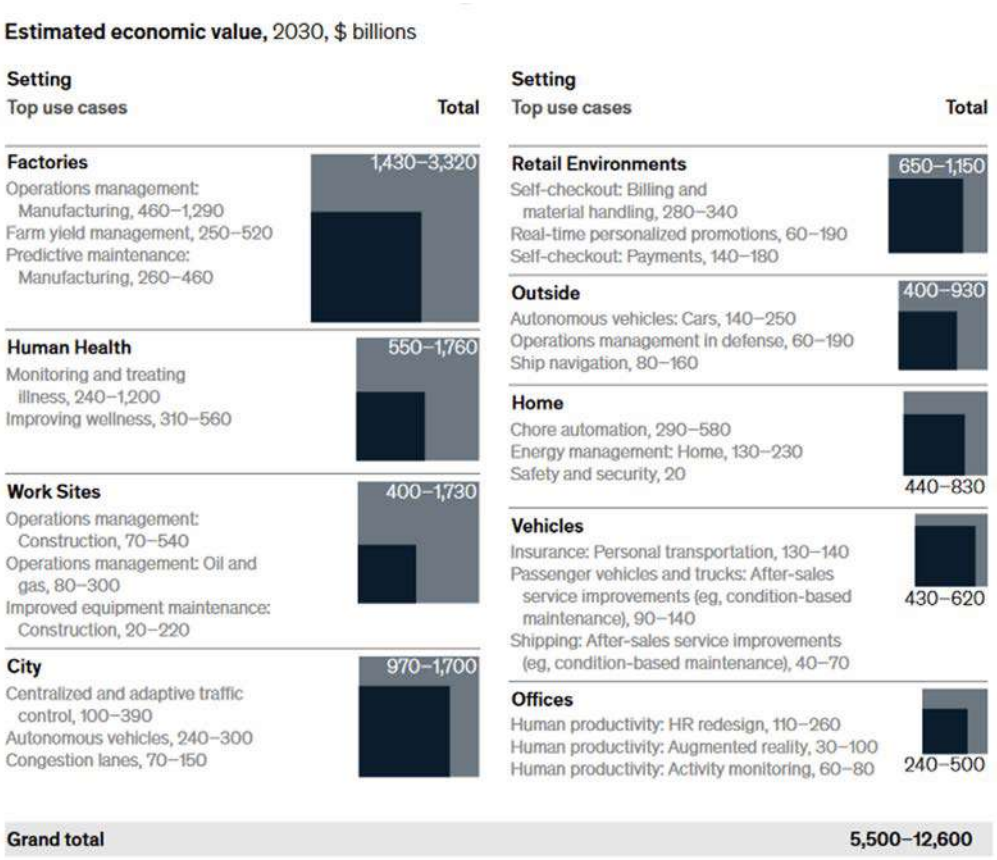


Figure 3: Factories lead in estimated economic value in 2030
Source: McKinsey

in factories could range from US$1.4 trillion to US$3.3 trillion by 2030 and factories could represent 26% of IoT's overall economic potential in 2030. Within this, the firm puts manufacturing itself at a value of US$1 trillion to US$2.3 trillion.

Based on its research, see **Figure 3**, the greatest potential for value creation is in optimising manufacturing operations – making the day-to-day management of assets and people more efficient. Overall, operations management applications in manufacturing could account for about 32-39% of the total potential economic value created in factories, that's about US$0.5 trillion to US$1.3 trillion by 2030.

There are now many examples of factories that have deployed IoT at scale and are capturing significant value from successful deployments. McKinsey cites **Schneider Electric**'s 50-year-old Le Vaudreuil site in France which was able to save 10% on energy costs using IoT sensors and to reduce diagnosis and repair time by 20% by supporting factory workers with augmented reality. Examples such as this illustrate the gains that can be made but manufacturers now need to look outwards as well to ensure they are well-positioned to manufacture efficiently and scale up their IoT-enabled systems so they can support the future of IoT itself.

Five challenges for smart manufacturing to overcome

There are five key challenges facing digital transformation in manufacturing as OEMs grapple with IoT demands but these are not always the same challenges that IoT devices themselves want to see manufacturers address. **Figure 4** sets out how respondents to an IoT Analytics survey view the smart factory and the goals it should deliver to their business. Many of these advantages feed through to the cost, time-to-market or compliance of IoT devices but some are manufacturing-specific.

Examples of performance gains

Typical IoT device manufacturing challenges, in contrast to purely factory-based challenges, include:

- Production complexity
- Security
- Connectivity
- Quality control
- Configuration/installation

The advances made in embedded SIM (eSIM) and integrated SIM (iSIM) enable IoT products that are to be shipped to multiple regions to be pre-installed with SIMs. This enables a single variant and one stock-keeping unit (SKU) number for the IoT device, ▶

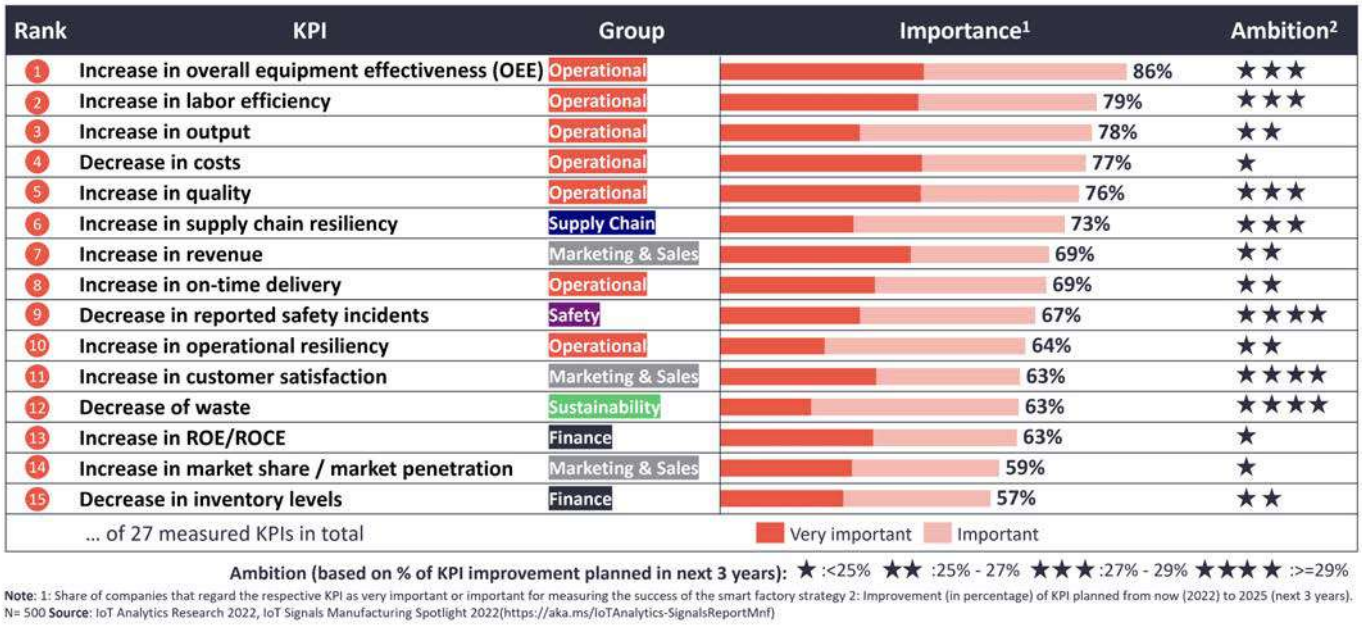


Figure 4: Top 15 smart factory key performance indicators
Source: IoT Analytics Research, 2022

contributing significantly to reducing production and logistics complexity. Supply and demand spikes that affected regional or nation-specific products can be smoothed out across a global product with a single SKU. An additional benefit is that the eSIM requires no physical handling which can introduce errors.

Developments in security are also enabling OEMs to embed secure approaches and follow through on companies' security by design strategies. Trusted key infrastructure which encompasses the generation and storage of keys can work across multiple electronics manufacturing services (EMS) partners without requiring specific security standards, special certifications or particular trust roles. The provisioning of keys, secure communications and secure maintenance enable complete lifecycle management and the addition of tamper-resistant storage in a secure element within the device adds further security. The ability to provision the key securely only when the device is in the field is a critical element of secure provisioning and essential for critical infrastructure such as smart meters because it prevents the cloning of devices.

Networking is also providing more options to IoT service providers with 5G arriving, private networks gaining further adoption and greater flexibility being delivered via SIM innovations. For 5G IoT devices, vendors offer SIMs that provide global connectivity out of the box with true always-on connectivity achieved by allowing devices to switch to a fallback provider if there is a service disruption.

This flexibility is supported by vendor-provided activation services which simplify switching providers and the process of moving between private and public networks. It also means there will be fewer service trips because plastic SIMs don't need to be swapped out when the network provider is changed. Connectivity is also making smaller demands on space within devices with 5G available on an M.2 card form factor while low power requirements can be addressed by low power wide area network (LPWAN) technologies.

OEMs also need to address quality, testing and validation challenges. The presence of an eSIM means after the device has been tested, the SIM can ▶

be switched from a test network to the live network. Troubleshooting and debugging can also be addressed securely through test environments and hardware with data fed back to developers so efficiencies can be integrated to future versions. These processes are essential to achieving compliance so devices can be sold in regions but also provide vital data to enable predictive maintenance and other use cases.

Improvements to efficiency don't begin and end in the factory. OEMs can contribute significantly to simplified device configuration and better preparation for easy installation. Configuration and settings that are easy to deploy and change during manufacturing can be accommodated and this is especially important for high volume deployments such as smart meters or connected alarm panels in which the business case benefits from fast device installation that requires limited training.

Future manufacturing

The smart manufacturing environments of the future present a more active and dynamic environment that the factories of the past. Products will no longer be presented to OEMs and manufacturers as static, finalised propositions and the manufacturer will be expected to adapt and refine the product throughout its production lifespan. Incremental gains will be achieved in this way across security, installation, connectivity, compliance and operational performance.

Being able to take live data from a deployed device and identify how the next generation of devices can be improved and adding that swiftly into the manufacturing chain is the ultimate goal and this introduces the possibility of continuous development. To accommodate this, factories will have to be smarter still than they are today and OEMs will need to apply IoT techniques to achieve this smartness across the multiple dimensions of manufacturing.

The goal of continuously variable manufacturing allows for increased personalisation but also simplified standardisation for bulk products. It all depends on the ultimate business case and the target cost of the product in question. Smart manufacturing will need to make room for both approaches in the factories of the future. ■

OEMs look to simplify design, streamline development and accelerate time-to-market

With IoT now well into the billions of connected devices, original equipment makers (OEMs) and smart manufacturers are utilising IoT innovations to power their own digital transformations. This virtuous circle is strengthened as developments in connectivity, device management, security and testing and validation are applied to smart manufacturing environments enabling these to produce goods at a speed and price-point that massive IoT demands. IoT Now managing editor George Malim spoke to Thales' Jose Sanchez, the head of product line management for IoT solutions, Stefan Mahr, the product marketing manager for 5G and security, and Sahil Bahri, a product line manager for IoT and 5G, to see where the efficiencies can be gained

George Malim: How does Thales help address the production challenges OEMs experience?

Jose Sanchez: Across our work in projects ranging from smart metering to connected health devices to manufacturing and automotive, we've seen a series of challenges and painpoints that we aim to mitigate or eliminate. Manufacturing itself is going through digital transformation and we are taking a comprehensive approach to solve challenges relating to device security, 5G introduction, quality control and device deployment.

There are improvements to be achieved in addressing production complexity and we are making these by simplifying existing processes or introducing new innovations. As massive IoT becomes a reality, the connectivity attributes of 5G, the control of private networks, the flexibility and security of embedded SIM (eSIM) and the testing and configuration capabilities enabled remotely by software are transforming the productivity of manufacturing.

This is essential for IoT in order to keep costs down, speed up the introduction of devices to the market and hit environmental targets.

GM: Robust connectivity is essential for the always-on digital economy but it has always been complex and challenging to manage. How do private networks put enterprises in control of the complexity?

Stefan Mahr: I agree that connectivity has been difficult to manage for manufacturers and there is a clear need to get rid of wired connections and the legacy in order to have the robust connectivity that can support smart manufacturing. Regardless of whether it is for connecting a robot arm or every level of a production line, with 5G you get more control, a different level of security, improved capabilities, ▶

Manufacturing itself is going through digital transformation and we are taking a comprehensive approach to solve challenges relating to device security, 5G introduction, quality control and device deployment

Jose Sanchez
Thales

the ability to control quality of service (QoS) and zero downtime. Now, with the latest 5G Release 16 we have started on the road to ultra-reliable low latency communication (URLLC) which will be super-critical for smart manufacturing.

GM: What is Thales' role in supporting OEMs and manufacturers in their launches of private networks?

SM: When private networks are installed, typically the network equipment vendors are contacted first. Interestingly, we're seeing ongoing discussions in Europe about the need to replace network components from certain manufacturers for security policy considerations.

While espionage is the most obvious concern, in fact even simpler methods could threaten the continuity of factory production. For example, if an embargo was placed against delivery of firmware updates or patches to apply political pressure - as Russia is currently doing with the delivery of gas.

These issues are even more important for network equipment in private networks in factories, as confidential data and knowhow must be protected and continuous long-term operation is required. Another important question for our customers is about who controls the firmware in the modules in the connected devices in a private network. The highest level of protection is required, but at the same time, there are needs for an access point for troubleshooting and optimisation.

As a leader in cybersecurity, **Thales** is often approached to provide these highly secured solutions which still are accessible remotely for diagnostics and software updates. For example, we're involved in a trial with a Bavarian car manufacturer, where a private network at the production plant needs to be improved, to enable efficiencies as the vehicles move around the plant. ▶

Many companies without experience in setting up and maintaining their own network, will need to quickly understand how to do this in a secure, stable way

GM: How does Thales help OEMs and manufacturers optimise their private networks?

SM: Thousands of private networks will be created and people will need to maintain them. These networks will need to be set up and tested under real network conditions and information about the network needs to be provided securely. Besides modules for connectivity, we also provide equipment, services and embedded software features for enhanced diagnostics, to help set up and optimise a private network.

Many companies without experience in setting up and maintaining their own network, will need to quickly understand how to do this in a secure, stable way. An integration, testing and compliance phase is underway that is bringing new devices to the market and our role is to support customers in their adoption of private networks by taking away the complexity and making it easier for non-networking experts to manage their private networks.

We enable our customers to get real-life data from the network so they can perform systems and performance validation tests. It's part of our support offering and forms a significant part of our comprehensive approach to providing OEMs and manufacturers with everything they need to simplify design, streamline development and accelerate time-to-market.

GM: There is a lot of talk about 5G but is it really the answer to the demands of IoT?

JS: In the first conversations we have about 5G, the focus is on practical reasons to use the technology. For a robot arm that used to require a cable connection which might break or make it hard for the arm to be relocated, replacing the cables has obvious benefits. Beyond that straightforward assessment there are many other possibilities and lots of opportunities in the background, such as use cases that rely on detailed positioning.

Improved control is the key benefit that manufacturers get with a private 5G network. You get to control the QoS and you get a far better idea of what is going on in your network.

SM: Our potential customers have a number of options. Wi-Fi might be impacted by non-exclusive use of frequencies, LPWAN is primarily designed for devices that need lower bandwidth, but 5G has some real advantages today, with more to come in the pipeline with upcoming releases.

Sahil Bahri: In terms of 5G, the network slicing part is compelling. Now is the time when public networks are starting to deploy Release 16 and that is providing improved security and control because you are either on a public network with a manufacturing slice or you're on a private network and your parameters are all set by you so you can have improved QoS.

GM: Reliability is essential for mission critical IoT but also for long lifecycle use cases in which the business case relies on minimised physical maintenance and repair visits. At the same time, use cases that have to comply with industry regulations must be accommodated. How does Thales see these requirements being addressed?

SM: With our expertise in cybersecurity, we support well-protected designs of our customers by providing security enhanced cellular modules, services and security consulting. For example, recently, regulatory frameworks like the Radio Equipment Directive (RED) in the EU significantly increased cybersecurity requirements, to ensure network protection, protection of personal data and protection from fraud.

Today, there is a much bigger focus on security, when someone plans to deploy millions of connected devices, like smart meters, alarm systems or industrial gateway routers. Security is central to all our offerings for connectivity of critical assets.

JS: This aspect is crucial because Thales supports manufacturers who are supplying to critical infrastructure like smart meters. The manufacturers want to give devices a trusted ID to ensure they cannot be cloned and recognise that ▶

Consider a product such as an alarm system that sells hundreds of thousands of products in many different places

Stefan Mahr
Thales

security starts at the point of manufacture - actually already during the design phase: Security by design is key here.

GM: Do you expect global standardisation to be driven by embedded and integrated SIM availability that enables single global products to be created rather than requiring regional variants?

JS: eSIM has the ability to solve challenges associated with trusted device identifiers, the security of devices and the inconvenience of having to handle plastic SIMs. We have our connectivity activation service that is making eSIM adoption simpler because it addresses the complexity of eSIM activation that is currently putting a brake on eSIM adoption.

We aim to make eSIM more accessible for industrial IoT by using the pull method, well known and already proven in the consumer space. This simplifies product complexity because all you will need is one stock-keeping unit (SKU), so there is just one product variant. We offer bootstrap connectivity so the device can be provisioned with the optimal connectivity provider at the point of deployment or before at the last stage of production.

SM: Consider a product such as a connected alarm system, that is sold in vast quantities and marketed across a broad geographical region. Previously, a local SIM would need to be inserted when the product is installed, adding cost to the solution. Alternatively, a SIM for a local provider could be embedded but this would mean creating numerous versions of the device for shipment to specific markets. Each device variant had its own SKU, creating logistics challenges.

Now, our IoT eSIM solution allows for the mobile network operator to be selected on-site at the point of deployment. This can even happen automatically with no physical interaction with the device needed. In this way, network operators can be changed remotely and resilient connectivity can be maintained over the entire lifetime of the IoT device. ■

www.thalesgroup.com/iot

Simplicity, scale and security accompany coverage and control on IoT organisations' target list as the mass market arrives

As the IoT industry continues to accelerate, deployment volumes are growing rapidly bringing greater complexity and putting previously minor challenges under the magnifying glass. George Malim, the managing editor of IoT Now, interviews David Traynor, head of Operations at Velos, to understand how IoT organisations can mitigate their growing pains while achieving greater simplification and improved control of their operations. Velos is a carrier-independent IoT connectivity provider and is the new name for JT IoT, the IoT division of Jersey Telecom that was acquired by Perwyn in 2021.

Traynor runs operations for Velos and is driving the business transformation to accelerate growth while holding responsibility for risk management and overall compliance. In addition, he participates in industry initiatives focused on securing IoT and the furthering of embedded universal integrated circuit cards (eUICC). Traynor's experience is in product management and operations at a range of internet, mobile and communications software firms. Prior to his current role, he has held positions at ASPIDER (now Kore), Fairmarket (now eBay)FTP and Firefox (now NetManage) ▶

SPONSORED INTERVIEW

George Malim: Let's start by asking about the recent name change from JT to Velos. Why have you introduced the new brand?

David Traynor: In the past year we have revolutionised our business: firstly we acquired new owners to give us the independence and control we need; secondly we have evolved from being a mobile network operator (MNO) as part of JT to being a multi-carrier mobile virtual network enabler (MVNE) so we can commit 100% of our attention to our IoT business; thirdly we have acquired new businesses to broaden our offerings and drive innovation. This transformation of our business demanded the transformation of our brand – it signals that we are not the same animal we were a year ago. Hence Velos and the derivation of the word Velos which helps reinforce principles around speed and precision.

GM: Please can you share a little more on the numbers?

DT: We have been delivering IoT solutions to our customers for about ten years and have built the growth to above average levels. And we are very pleased to have new owners, last year we were bought in a deal that valued JT IoT at more than £200 million by Perwyn, a European private equity investor specialist. Its focus on excellence and ambition really helps us drive our innovation and agility, it is a great fit.

GM: IoT has now matured to the extent that projects are now mass scale and this brings substantial challenges from pricing, the bill of materials, integration and packaging. How can Velos help customers plan for scalability and address these challenges?

DT: Scalability touches many dimensions of manufacture, from the logistics to provisioning to the onboarding, and each presents gains for IoT service providers. However, scale also magnifies error and inefficiencies. A few cents of additional cost or complexity multiplied several times and then by the number of devices in a deployment can make some projects unviable or put a substantial dent in profitability.

When it comes to packaging, customers need higher levels of integration to simplify device configuration and to help reduce costs. This includes SIM form factors like the MFF SIM that are smaller and can be soldered into devices… and also integrated SIM (iSIM), which has the SIM functionality fully integrated into the system-on-a-chip or SOC. This enables fewer components to be specified but also aids operational efficiency. This improved efficiency in onboarding is providing reliable ways to deploy devices and can also help speed deployment and reduce hassle for consumers. For enterprise applications this can ensure that devices can be adopted into private corporate networks with automatic provisioning that allows different modes for different stages of the lifecycle.

In addition, there are functional benefits that can be realised if optimum components are selected. In the modems and SIMs, for example, benefits can include reduced power consumption and a reduction in the amount of real-estate taken up in the device because of the optimised form factor of these components.

GM: How important is managing overall cost so manufacturers can manage scale and deliver flexibility to can generate the most value through the complete product lifecycle?

DT: Reducing costs is always a goal and we always look to having the components, tools and systems that can deliver the economies of scale that our customers need. This can be as simple as bulk activations, or providing warehousing facilities in the country of manufacture.

New functions and features can also help to extend product life and improve cost of manufacture. A good example is the use of the remote SIM provisioning (RSP) that allows the SIM to be swapped electronically over the air after manufacture, removing the need to change SIMs for improved rates, quality or coverage.

This remote SIM provisioning, often referred to as eSIM, helps provide single global stock-keeping unit (SKUs) for OEMs because the SIM can bootstrap its own connection at the point of deployment. The benefit here is that local plastic SIM cards do not have to be installed in the country they are deployed and regional or national variants of products do not need to be created.

This ongoing capability provides flexibility to ensure the device is connected to the best provider in its location and helps future-proof the service in case of outages or technology changes. Knowing that the lifespan of a device can be extended without human interaction for several years has obvious benefits to the total cost of the service and therefore knock-on implications for profitability and viability.

GM: As connected device numbers proliferate and IoT populates the mainstream, the threat surface has radically expanded and security now presents a potential bottleneck for many organisations' IoT deployments. How is Velos positioned to help customers build trust in the apps, devices and data their IoT solutions generate?

DT: Security is an essential ingredient of successful IoT deployments and increased scale only increases the scope of the challenge. Managing the risks from the ever-expanding vulnerabilities for IoT is a major concern for all manufacturers. We provide management of the access point names (APNs), IP addresses, ports and firewalls to reduce these surfaces and we protect data transiting the internet with virtual private networks (VPNs) and authentications to help reduce attack risks and detect attempts. ▶

David Traynor
Velos

Scalability touches many dimensions of manufacture, from the logistics to provisioning to the onboarding, and each presents gains for IoT service providers

When it comes to network integration there are only a few IoT MVNEs that fully understand the complexity of the overall integration needed to deliver this vision of flexible connectivity

Security is not just about managing threats, it's also about providing methods to help authenticate the devices, applications and data. As more and more IoT applications handle personal data for wearables, or for vehicle control, or for asset tracking, there is an increasing demand to be able to prove the authenticity of the data and the device to comply with policies to protect citizens, and the country legislation. For example, signing functions can be easily deployed to help deliver auditable methods to prove that we can trust that image has not been tampered with, and that it originated on that camera, on that date, in that location.

Just as we saw in the world of the web browser, we are now seeing increasing demand for complete transport layer security (TLS) stacks and initiatives like IoT SAFE from GSMA to further improve the trust that can be delivered to these IoT applications. This is a big topic since getting adequate security takes expertise and resource that has traditionally been missing in the IoT space. As an industry we need more manufacturers to use the standards-based tools that we have in our products that deliver cross authentication or secure channels using industry recognised Java and Global Platform approaches.

GM: How does Velos deliver capabilities that improve value and extend your capability beyond connectivity?

DT: All our offerings are delivered via application programme interfaces (APIs) and web tools, and they provide the location, security, billing and usage analysis that manufacturers and enterprises need to better manage their applications. More and more, our customers need better integration into the control plane so they can measure and manage the way that devices and applications behave. Advantages can be uncovered across the board and range from improving signalling efficiencies to reducing battery drain (or even improving carbon footprints). In addition, we can help them protect the content to comply with emerging applications that require compliance to GDPR, HIPPA, or Patriot Act regulations.

GM: Mature IoT deployments are high volume, cover multiple countries and have coverage requirements that rely on reliable, secure connectivity. What are the challenges of providing these capabilities at the same time as enabling flexibility so IoT organisations can control and manage their deployed estate of devices and software?

DT: Coverage is the essential capability that IoT demands and we supply. The value of interconnected things is that they can deliver derivative value to many applications - so the connectivity must meet the needs of the thing. The value is more about QoS and policy - not just simple megabytes. The beauty is that we also provide the flexibility for that connectivity to be changed on the fly like the RSP topic we covered earlier.

GM: What tools and management systems are needed to integrate connectivity, devices and applications and apply intelligence to better understand overall behaviour?

DT: When it comes to network integration there are only a few IoT MVNEs that fully understand the complexity of the overall integration needed to deliver this vision of flexible connectivity. Some are just mobile virtual network operators (MVNOs) that focus on selling only their native connectivity, while others have simple roaming agreements but do not have the flexibility of full integration to multiple core networks, and some simply rely on the billing aspect of an online charging service.

Increasingly now, our customers demand access to all of these services with the ▶

latest diameter, message queuing and interop facilities needed. Our customers include many of the IoT MVNEs in the market, they use our international mobile subscriber identities (IMSIs) to give them the coverage they need, and the APIs for the control they need, and access to the user plane and control plane to improve their offerings. This provides both the independence they need and the integration they need to deploy global solutions.

GM: How does Velos help automate controls to allow the agility that organisations want in a way that can be independent of the carrier, country or technology they deploy?

DT: There is no one-size-fits-all approach in IoT and simple zones just do not cut it. Almost all of our 1,000 manufacturers have their own coverage schemes and many have variants to meet specific use cases and product needs on a region-by-region basis, by regulator environments or by carrier. We provide simplicity and control across these differing needs and support customers to achieve compliance for devices, roaming, data sovereignty and tax. It's certainly no longer just about carrier-neutral connectivity.

GM: What is your view of the current status of IoT? Do you think we have reached or even passed the tipping point at which massive volumes of devices are making the initial IoT vision a reality?

DT: There are still a number of hurdles that we face as an industry and for me, the three most important are scalability, security and simplicity. Forgive the trite alliteration here but it does help us all remember our objectives are to help stimulate this business for all of us.

To achieve simplicity the IoT service and device has to be easy to integrate, easy to manufacture, easy to deploy, easy to maintain. I think our industry knows this and most players understand this well.

When it comes to scale, getting the first 100,000 devices deployed is fairly easy but the ceiling of one million, or ten million cannot just be solved without reliable processes and integration. Building for scale takes experience and many of the players haven't solved the reality of chip shortages, carrier certification, electricity price hikes, or avoiding the massive impacts of failures from the third-party IPX, colocation, cloud or IP transit providers. Many are starting to understand reliability and what it takes to deliver a world-class service.

In my opinion it is security where IoT, as an industry, is most vulnerable. I believe that we as suppliers have to become the catalyst to push these technologies and tools to our customers. We have the functionality inside our platforms and SIMs to help our industry make huge strides in security, but very few customers are actually using what is available. We have to educate and apply industry standard approaches - from Global Platform libraries and the baseline Java functions that are in all our SIMs, to the certificate authority functions that are commonplace for the billions of web browsers on our planet, but sadly, in very few of the billions of IoT devices. We have to stimulate change here, we have the tools and the knowhow, we have to find the right commercial approaches to build IoT applications that we can rely on and that comply to our legislation. These must be solutions that are simple to deploy, that can scale and that we can trust. ■

www.velosiot.com

To achieve simplicity the IoT service and device has to be easy to integrate, easy to manufacture, easy to deploy, easy to maintain. I think our industry knows this and most players understand this well

Nanolink's success lies in its ability to enable precise and reliable tracking of numerous tools

Nanolink enable tool tracking for enterprises with Velos

When Nanolink a provider of equipment and asset tracking that provides inventory management for large manufacturers, construction and healthcare companies, needed seamless connectivity with simplified provisioning, it turned to Velos to provide the pricing, coverage, service and support it needed to support its global clients

Misplaced or lost equipment can cause business significant losses for enterprises of all types which is why **Nanolink** has developed its offerings to address needs to track assets accurately. Nanolink improves efficiency and saves cost because it allows companies to cut the time spent looking for or replacing missing tools by providing clear, precise and real-time mapping.

Nanolink's success lies in its ability to enable precise and reliable tracking of numerous tools. This is done through a small Bluetooth low energy (BLE) beacon with extensive battery life. Nanolink's GGT100 tracker operates as a normal GPS for transporting equipment, but the device has the added capability to connect to the Nanolink beacons mounted on the tools. This provides the capability to track all tools within range on the Nanolink map application and account for every item in the inventory.

Reliable connectivity

To achieve success, finding a service provider that could offer a reliable connectivity solution and seamless connectivity was of vital importance. The initial onboarding of previous providers proved to be tremendously time consuming as was the deployment of the tracker devices themselves. It was impossible for Nanolink to activate SIMs manually, hence the need for an application programme interface (API) integration solution built within the deployment workflow. Pricing, coverage, service and support also played a big role in Nanolink's selection.

Control the SIM estate

Having more than 600 roaming agreements globally, **Velos** has enabled Nanolink to deploy reliable and secure real-time asset tracking for its clients. Velos's easy API integration, international coverage and 24/7 support has enabled Nanolink to take control of its SIM estate connectivity through a single platform. This has allowed it to provide efficient deployment of a large number of trackers, while optimising expenses and making sure no tool is left unaccounted for. ▶

SPONSORED CASE STUDY

Scale, integration and roaming

With Velos's global IoT connectivity solution, Nanolink can swiftly deploy a large number of trackers for customers without the hassle of having to activate SIMs manually.

Velos is providing important API integration for remote SIM management, which has been successfully built into the existing deployment workflow. This allows Nanolink to construct, provision and monitor its entire SIM estate remotely.

Velos's non-steered, open roaming SIMs offer fast, reliable and secure connectivity; building the bare bone infrastructure for Nanolink's GSM implementation. With Velos's solution, Nanolink can offer reliable asset tracking at competitive prices on an international scale.

"Velos provides the service and solutions you'd expect from a large provider yet somehow the support and response times are that of a local business," says Klaus Meldegaard Keith, a partner and the chief technology officer of Nanolink ApS.

Supported by team of more than 120 experts and with over 600 global networks, Velos provides customers with sustainable, scalable, compliant and secure access to connectivity.

Velos aims to deliver the agility and resilience IoT customers require and it has shipped over 12 million SIMs worldwide, offering services to businesses of all sizes – from small specialist players to huge manufacturers. The company's portfolio includes flexibility in integration options covering features around security and resilience. ■

www.VelosIoT.com

THALES
Building a future we can all trust

Improving IoT cyber security

through eSIM-based scalable trust

How IoT SAFE improves IoT cybersecurity whilst being simple to deploy at scale

Security in IoT has often been listed as a development priority but then postponed or neglected with negative consequences. As the attack surface expands and new threats proliferate, traditional approaches to securing devices are too inflexible, too expensive or too complex to integrate to meet the timescale and volume needs of IoT enterprises. Current security methods address security concerns but are fragmented and this prevents them from being able to scale up. In the field of cellular connectivity, the GSMA's IoT SAFE initiative provides an alternative for IoT enterprises that is independent of mobile operators and provides a standardised method for securing IoT devices. This, Stephane Quetglas, the director of marketing for embedded products at Thales, tells George Malim means IoT can be secured end-to-end at scale, with flexibility to change connectivity provider and without the need to re-invent the wheel for every device or service ▶

Stephane Quetglas
Thales

We've seen the attacks on IoT devices and services for more than ten years and IoT security remains a significant concern for us

George Malim: What are the challenges of addressing the sheer volume of IoT attacks?

Stephane Quetglas: We've seen the attacks on IoT devices and services for more than ten years and IoT security remains a significant concern for us. There have been some substantial disruptions caused by security and the situation has not improved much over the years because there are more and more companies wanting to connect their devices and to deliver more value and have more mobile services. Companies have started to put functionality and the service itself at the top of their list and not the security. This is because they haven't been sufficiently aware of the security issues that exist and the additional security issues that exist when you connect a device to a network.

The scale of IoT is enormous and is well beyond the availability of skilled security experts in the industry so companies tend to forget about security or use very simple methods such as log-in passwords. When you use passwords and don't pay attention to them, you risk having a password that is too simple or shared across devices, making all of them vulnerable at once.

The main barriers come down to shortage of security skills and the cost of implementing security in IoT. Implementing security has a cost and whatever the device it is important to diversify the secure credentials that you deploy in the device. This is so that if a device is attacked, other devices are not vulnerable to risk, but this process is costly.

The other big reason that implementing security in the proper manner is very costly is the need for solutions that address both the level of security required and the level of scalability needed. This is in the context of billions of IoT devices so the scale is huge and will be even larger in the context of the new generation of 5G and low power networks which are arriving and bringing an even greater number of connected devices.

In addition, there are use cases where there's a need for securing the connectivity of the device to the IoT application and this relates to the value of data. Apps increasingly are deployed in the cloud and that means you need secure connections so you can sign data when you send it back and it can be verified. For example, in use cases in the energy, automotive or healthcare industries the value lies in the type of data that is exchanged, not in the fact that the platform is cloud-based..

In addition to public networks, in private networks you have use cases where the data circulating needs to be certified so it can be trusted. IoT in private networks such as at manufacturing sites relies on the ability for devices to sign data and prove it is genuine. There are more and more use cases emerging that require security in this way so scalability is essential.

GM: How does the GSMA's IoT SAFE initiative solve the issues by making use of the hardware's tamper-resistant element?

SQ: The tamper-resistant element is the subscriber identification module (SIM) or embedded SIM (eSIM) already in use in connected cars, smart meters or container trackers. That's the first element so the obvious choice is to build on what is already in the connected device. It is the first step to address scalability requirements because you don't have to add another chip or element to your bill of materials (BOM). The SIM and eSIM offer a very high level of security and ▶

Security by design is for us at the heart of what we do but lack of skills and the complexity of security means companies in IoT are not comfortable with it

have been used for many years so they are a perfect platform for a security solution.

The second choice is to adopt an approach based on public key infrastructure (PKI) which provides a cryptographic method used for strong authentication between cloud and devices and data integrity. Typically, you might use this method on your computer to access online banking. The PKI technology allows you distribute strong credentials in a secure and scalable manner unlike a login/password.

The two main choices therefore come down to re-use of the field-proven tamper resistant element that is the foundation of SIM and eSIM, with a PKI approach, which is very appropriate for addressing the security issues IoT faces. When done in a standardised manner like IoT SAFE, this is ideally suited to scale and manage large volumes of connected objects.

GM: What is your view of security by design and is this approach being taken by the IoT industry?

SQ: It is very important and needs to be considered as an essential part of device or service design. Security by design means that you consider security at the earliest stages of your process when you first think about creating an offering or business. If you do this, you will have the right foundations.

Security by design is for us at the heart of what we do but lack of skills and the complexity of security means companies in IoT are not comfortable with it. This is counter-productive because it is very difficult to fix security issues when products are already in the field and you face issues that you cannot repair or address.

Security is increasingly put as a high priority by IoT companies, and they are interested in relying on security specialists to try and bring the right approach. This is partly to do with the skills shortage but also because security is evolving all the time. To be effective, you need to know the security ecosystems, learn skills and understand new attacks and ways to counter them.

This continuous process is difficult to implement, especially for small-to-medium enterprises. Don't forget IoT is made up of lots of small companies, it's not just a few big names so for many it's very difficult to develop in-depth security skills.

GM: How are the IoT SAFE specifications being integrated into hardware tamper resistant elements?

SQ: What is key for IoT SAFE is that this is a standardised approach that utilises the eSIM independently from the mobile network operator. If you use IoT SAFE in the eSIM in your connected devices, you can choose a network operator to provide connectivity and use IoT SAFE to connect devices to your IoT cloud and later on, if you want, you can change the mobile operator for your connectivity without impacting your IoT service.

Indeed, devices will still be able to connect to the same cloud with the same credentials even after the mobile operator has been changed. IoT SAFE is not included in the mobile network operator profile, but in a dedicated security domain sitting beside the SIM application on the same tamper- ▶

We work with providers of security stacks and middleware vendors to make sure IoT SAFE is already supported and thus the integration made easy for device makers

resistant element. The flexibility this provides is important for IoT enterprises because IoT SAFE can be independent across the connectivity provider and the security provider.

The freedom this provides means there are fewer constraints in terms of vendor selection and the security can scale which is not the case when you have fragmented systems.

GM: What is Thales' approach to IoT SAFE and how does that deliver scalable trust for IoT applications?

SQ: We embraced IoT SAFE immediately. We are convinced of the need for improved IoT cybersecurity and the requirement to provide a security solution to IoT players that provides something standard and therefore scalable. Standardisation is the right way to go so the security solution can be deployed everywhere.

IoT SAFE is standard but of course you have some additional value as a vendor that you can provide to your customers. We work with providers of security stacks and middleware vendors to make sure IoT SAFE is already supported and thus the integration made easy for device makers. We also provide a touchless provisioning service which is a way to totally remove the cost impact of adding security into a device when the device is manufactured. When you use Thales' IoT SAFE in the device, there is not additional activity and no additional charge in the process because our solution will automatically generate and validate credentials when the device is first used on the field.

This is how we provide additional value. Of course, we have connectivity management solutions and we're a leader in eSIM and remote SIM provisioning (RSP) solutions and this means we are able to provide our customers with complete solutions for connectivity and security.

GM: What are the alternatives to IoT SAFE?

SQ: The most popular alternative is a device-based approach where security is implemented as software in the device memory. This solution works from a functionality perspective but is quite bad from a secure path point of view because a general purpose processor in the device is not protected and is very easy to defeat. In addition, device-based solutions are usually proprietary or bespoke to a specific device so you need to repeat the same work for every device or implementation and this approach can't scale.

Another alternative is Generic Bootstrapping Architecture (GBA) which is a user authentication method based on the SIM application. This is mobile operator-centric and was standardised a long time ago. Adopting this method means you require a security service provided by your mobile operator: as a consequence, you lose the service if you change operator and need to integrate with the security service of the new operator. In addition, this does not provide true end-to-end security up to your cloud platform.

IoT SAFE can be deployed in the same way across all of your devices and it is not linked to your mobile operator. The security provided is end-to-end so you are truly protected.

GM: Are IoT enterprises adopting IoT SAFE?

SQ: We are seeing strong interest in IoT SAFE today and people that are using cellular technology for IoT are highly accepting of this solution because secure network connections and data are very important to their business cases. Having said that, awareness needs to be developed further to detail the potential of the technology. We're working to make sure IoT players are aware they can use and rely on it to relieve some of their pain points and ensure their IoT operations are secure.

Sponsored by:

THALES
Building a future we can all trust

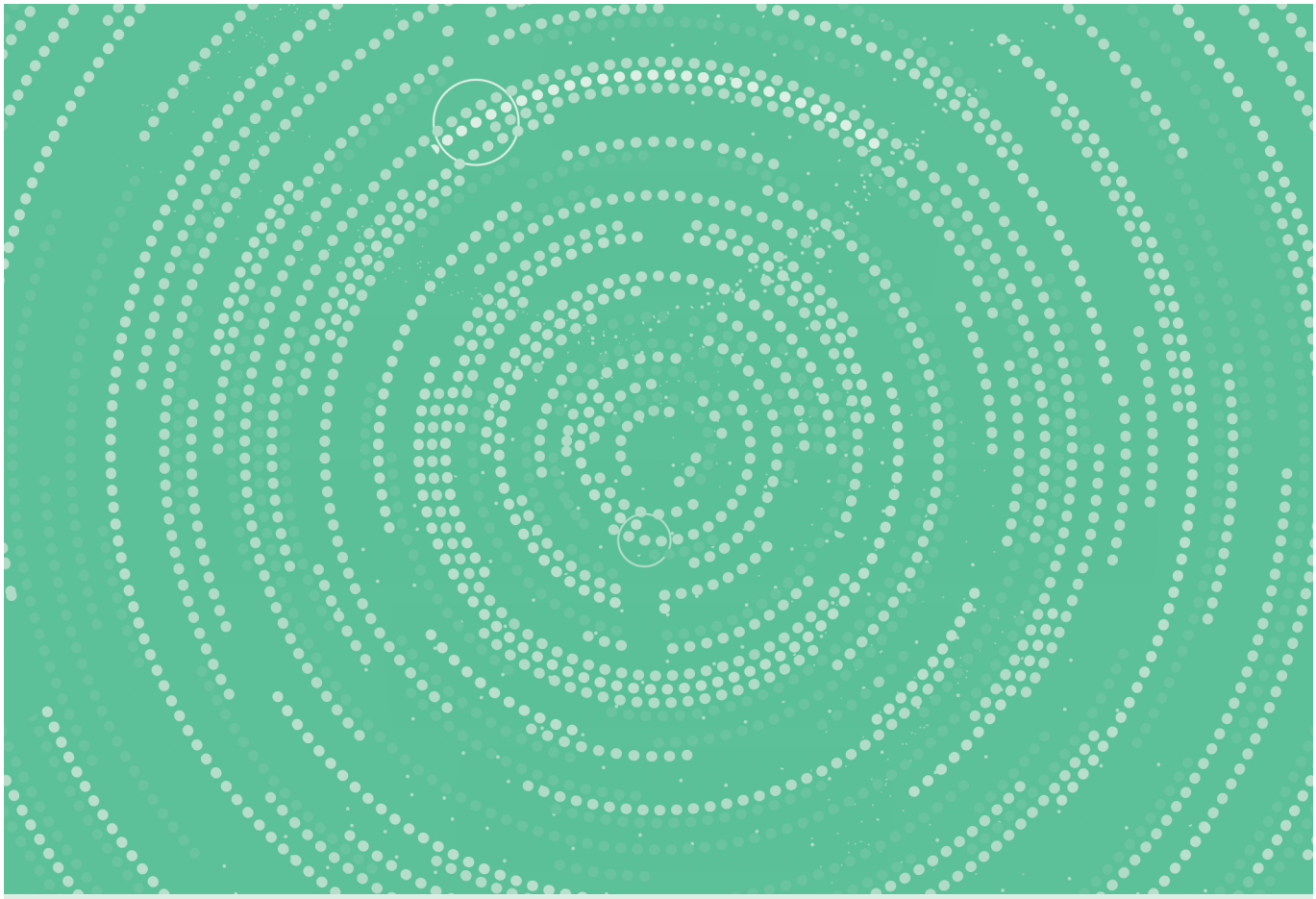
How OEMs and IoT solutions providers can address the challenges of achieving security by design

As IoT continues to mature and the volumes of connected IoT devices increase, the attention has turned to securing IoT. The larger number of devices have resulted in an expanded threat surface and greater opportunities for cybercrime. For OEMs and IoT solutions providers this presents two fundamental challenges: reducing crime and strengthening trust in IoT devices and the data they transmit

Analyst firm **Gartner** reports that more than 80% of organisations have implemented some form of IoT and close to 20% have detected an IoT-based attack in the past three years. This demonstrates an ever-growing number of IoT enterprises feeling the negative effects of security breaches but there is still significant failure to put adequate IoT cyber security in place. The firm says fewer than one-third of chief information security officers are confident their information security can reliably assess and mitigate IoT risks. This will not help breed trust and confidence in IoT devices and data among users and customers.

Reducing crime and the opportunity to commit cybercrime are obvious priorities but being able to trust IoT devices, their identities and their data is the foundation of many IoT business cases and represents the future of IoT revenues. Only when data is trusted to come from a specific device and the security of the data itself can be assured can it be relied upon and used to feed the business need it serves. Fostering trust is therefore as important as preventing frauds and cybercrime to the success of IoT initiatives. ▶

SPONSORED ANALYST REPORT



Importantly, IoT clouds are also under attack so threats are not just confined to device security. FireEye's threat intelligence and incident response unit **Mandiant** has identified a flaw in a component of the Kalay cloud platform that can be exploited to hack systems. Many Kalay users are video surveillance devices and the vulnerability has the potential to allow attackers to intercept live audio and video data. This hack relies on accessing a Kalay user's unique ID but it illustrates that IoT devices should not be seen as the only weak point and IoT cloud security will increasingly need to be addressed.

Regardless of where the attacks come, the reality is that they are increasing in frequency and systems designed to secure devices are themselves potential points of vulnerability. Cybersecurity specialist **Kaspersky** detected 1.5 billion attacks against IoT devices in the first half of 2021 via its network of honeypots which simulate a vulnerable device. This is twice as many attacks as the honeypot network recorded in the first half of 2020.

From cameras to combines, the attacks proliferate

Examples of IoT device security breaches range from surveillance cameras to combine harvesters. Last year, a group of hackers claimed to have breached a massive store of surveillance camera data collected by start-up **Verkada**. This allowed access to live feeds of 150,000 cameras inside hospitals, police departments, prisons and schools as well as at enterprises. Companies that had footage exposed included **Tesla** and **Cloudflare** and hackers said they had access to the full video archive of all Verkada customers.

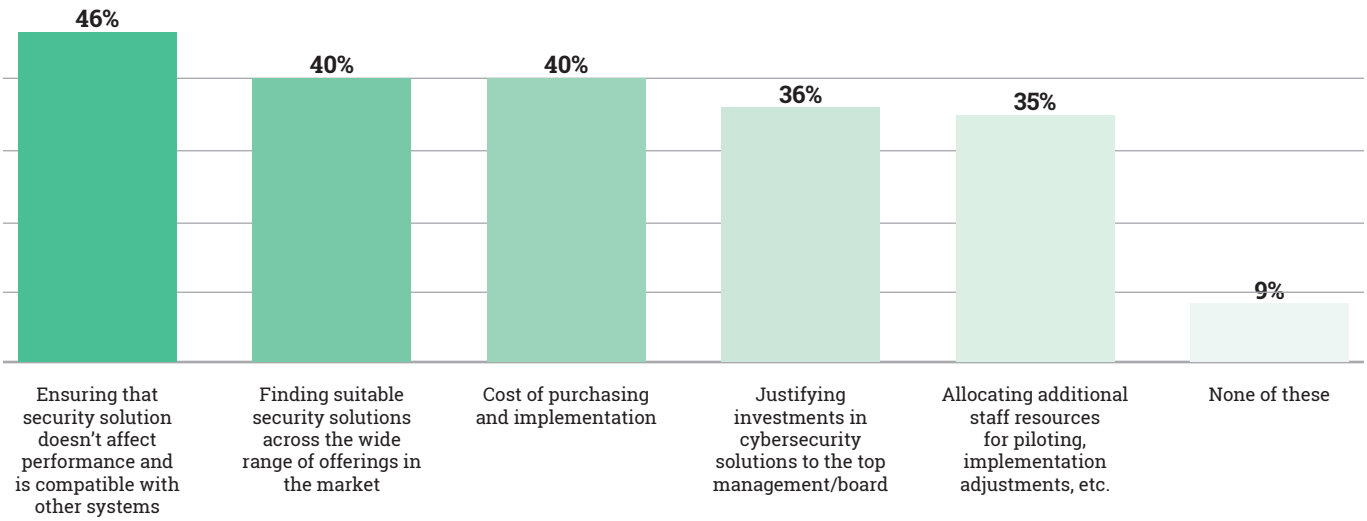
These types of examples illustrate the need for IoT service providers and original equipment manufacturers (OEMs) to adopt a security by design approach that prioritises thinking about security at the design stage and sets out what mechanisms will be used and how these will be deployed and managed when large volumes of devices are in deployment. Of course, in lower-end IoT services this needs to be accommodated at very low cost so the cost of securing the device doesn't outstrip the value of the service it provides.

Can IoT afford the cost of security?

Today there are 8.6 billion IoT connections, according to **ABI Research**. By 2026, that number will nearly triple to 23.6 billion and securing these will involve substantial investment. The firm says total revenue in the IoT security market will reach US$16.8 billion by 2026. That suggests that a typical IoT connected device could be generating revenue for security providers of 66 cents. For many types of deployment that additional cost will break the business case, while for others it will reflect tremendous value.

However, it may not be possible to extrapolate the ▶

Figure1: Top issues organisations face with cybersecurity solutions
Source: Kaspersky



numbers so simplistically. ABI Research says the amount of IoT security revenue does not always correlate with the amount of IoT connections, and some markets are expected to experience disproportional revenue as companies spend to address security.

The headline figure does illustrate a market in which there is willingness to devote sustained investment to security and that is encouraging. Even so, there's a substantial hill to climb even with this level of projected investment. In addition, not every organisation is fully-aware or committed to securing their IoT devices – yet.

Kaspersky reports that, while two thirds of organisations (64%) globally use IoT solutions, 43% don't protect them completely. This means that for some of their IoT projects, businesses don't use any protection tools. The damage to customers, the brand and its reputation cannot be allowed to continue so greater investment is needed.

For OEMs and IoT service providers there are several important concerns, which Kaspersky has highlighted in **Figure 1**. It says 46% of businesses fear that cybersecurity products can affect the performance of IoT while 40% feel it can be too hard to find a suitable solution. There are also concerns about lack of skilled staff or specific IoT security expertise within the business, with 35% citing this as a top issue.

How to improve IoT cyber security

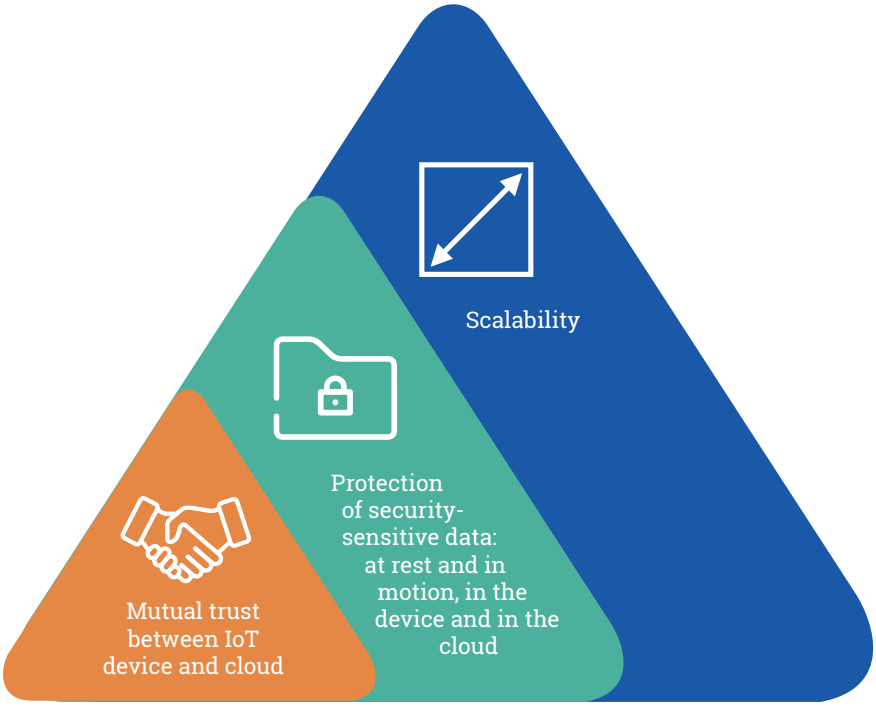
The wide array of attacks from distributed denial of service (DDoS) to malware and hacks on passwords creates a series of challenges for OEMs and IoT service providers to address on behalf of organisations that deploy IoT. In some cases, enterprises will try to address issues themselves but IoT service providers and OEMs are typically better-placed to secure IoT.

This is because they have experience of working across multiple types of devices, use cases, markets and jurisdictions so they are well aware of the correct techniques to use. They have both the IoT and security-specific skills needed, that are in short supply in the market. It will, for example, be hard for an enterprise to find the right people and the right structure to position their security stance effectively to protect their IoT operations.

The utilisation of cybersecurity is an important step but having the correct policies in place to support secure IoT is essential. Too many devices ship with default passwords or are subject users who change their password to something as simple as the word: "password."

A large proportion of security breaches can be attributed to human error so efforts made by OEMs and IoT service providers to take matters out of users' hands and embed security into IoT devices promise strong results. ▶

Figure 2: Hardware tamper-resistant elements deliver scalable trust for IoT applications.
Source: Thales



The alternative is for enterprises to do it all themselves and invest in cybersecurity software, vulnerability management tools, password management software, network intrusion detection systems and so on. Each of these must be kept up-to-date, managed and maintained and adds a significant non-core list of tasks for an enterprise.

What can OEMs and IoT service providers do?

In addition to bringing their experience to customers they can assist by setting out how security by design can be achieved. Security by design is an approach to software and hardware development that moves security from being a bolted-on afterthought to a primary consideration undertaken at the design stage of an IoT device or service. Security by design will always outperform retrospective measures to addressing existing vulnerabilities and patches and is becoming essential in IoT as connected devices are readily addressable over the internet.

OEMs and IoT service providers can use their knowledge to assist customers to design security into their devices and ensure manufacturing itself is secure so authentication, for example, is protected. Other innovations are arriving to simplify key IoT security requirements and enable improved functionality.

The IoT SIM Applet For Secure End-to-End Communication (IoT SAFE) is a **GSMA** initiative that allows the SIM to be used as a hardware secure element or root of trust to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted that the SIM or eSIM (embedded SIM) is ideally suited for this purpose because it offers the best protection against hacking, offers advanced security and cryptographic features and it is fully standardised.

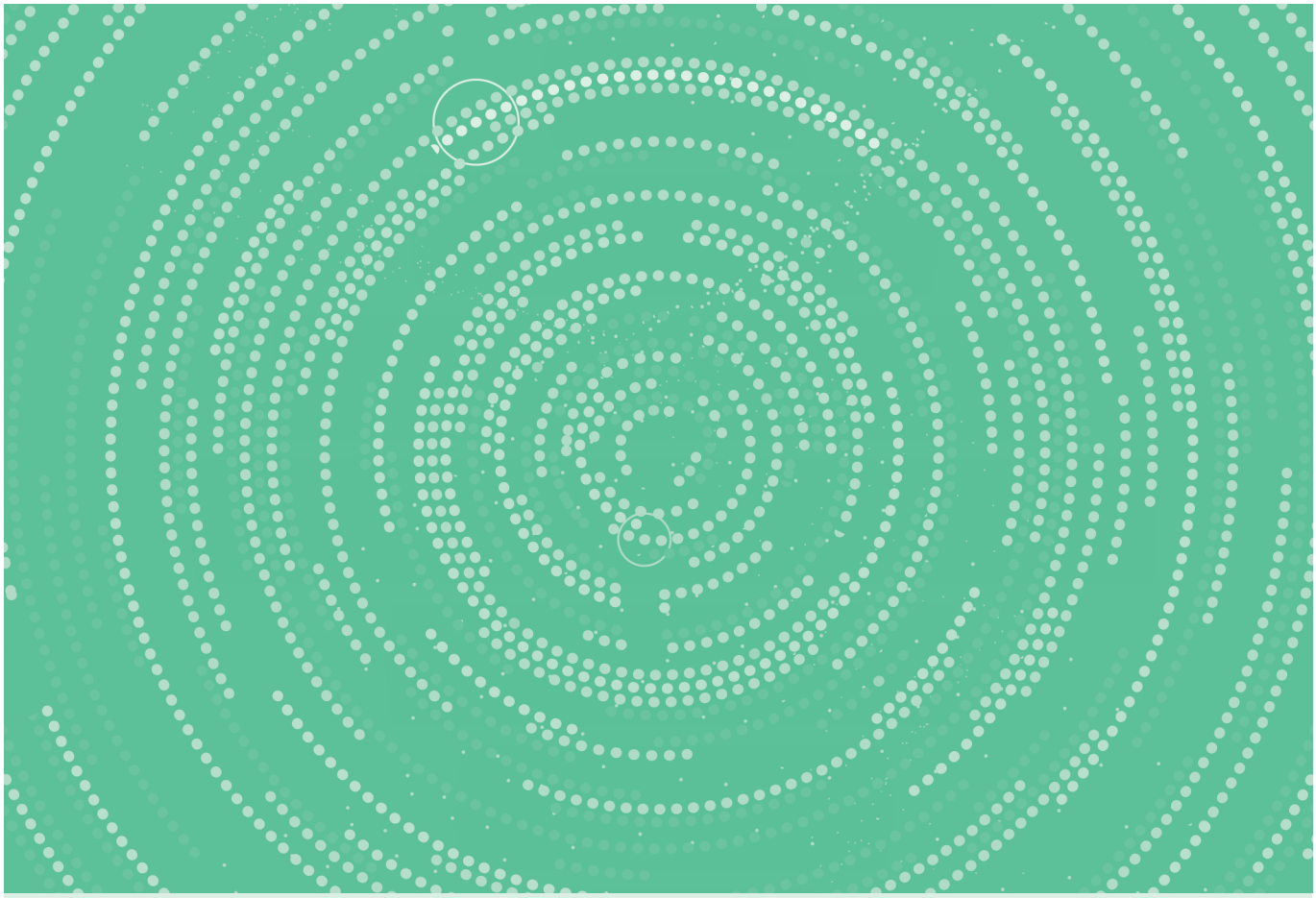
Hardware tamper-resistant elements – with the hardware expressed as an integrated or embedded subscriber identity module (iSIM or SIM) that also contains a secure element - within the device are a standard technology that integrates the new GSMA IoT SAFE specifications. These help to deliver scalable security by design using well-known, proven SIM technology that is already in billions of devices and has been used for decades.

Hardware tamper resistant elements are important because they address the three key IoT security requirements:

1. **Mutual trust between the IoT device and cloud**
   This end-to-end mutual authentication enables a TLS connection

2. **Protection of data at rest and in motion**
   Data integrity
   Data confidentiality

3. **Scalability**
   There are already billions of secure elements in the field ▶



The hardware tamper resistant elements then act as the root of trust and a cryptographic toolbox that stores private keys, digital certificates and security services. IoT SAFE deployment use the SIM or eSIM as a miniature crypto-safe inside the devices to establish a TLS session with a corresponding application cloud/server. IoT SAFE provides a common application programme interface (API) for the highly secure SIM to be used as a hardware root of trust by IoT devices and is compatible with all SIM form factors.

The IoT SAFE applet runs on the SIM/eSIM OS and solves many of the challenges associated with IOT scalability because it enables the IoT device middleware to use the credentials and security in the SIM card for IoT. In essence, the secure element in the SIM/eSIM ties the device identity to the device and assures it as a source of data.

The use case of SIM, eSIM and more recently innovation in iSIM as a root of trust for end-to-end security for IoT products and services is compelling. In particular, eSIM and iSIM enable production, logistical and operational enhancements because there is no need for a physical plastic SIM and iSIM or eSIMs can simply bootstrap a localised connection at their point of deployment which means regionalised product variants are not needed. However, as a root of trust, the SIM becomes the enabler of a secure, trusted device that communicates data in support of whatever use case the enterprise requires.

Conclusion

SIM and eSIM vendors along with chipset manufacturers, cloud service providers and mobile operators have collaborated to develop the GSMA IoT SAFE standard and analyst firms such as Berg Insight expect the standard to gain significant traction this year.

The ability to take a security by design approach and install an IoT SAFE standard-compliant secure element into an IoT device at the point of manufacture addresses the requirement for both a root of trust and flexible connectivity within the device. Coming at the cost of the software for the secure element, the value proposition is attractive. OEMs and service providers are well-placed to roll-out IoT SAFE on behalf of customers with the possibility of creating IoT devices that have 'security inside' on behalf of their customers.

To learn more about IoT SAFE, security by design and the root of trust capabilities of the next generation of SIM technology, visit: **https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements/gsma-iot-safe-specifications**

The green power of the IoT

Climate change is the most crucial challenge of our time. The growing number of extreme weather events makes this evident, to cite just one example. We have to stop heating our planet by emitting CO_2 if we want to maintain the same standard of living or achieve a higher level of life quality. Decarbonisation and digitalisation show the way to break out of the old vicious circle of economic growth and a higher standard of living at the expense of the environment; they are interlinked and offer great potential for the challenges we are facing. This is not just about lifestyle but is also a necessity for the well-being of humans. The objective, explain Infineon's Thomas Rosteck and Adam White, is to slow down or even stop climate change, while at the same time mitigating its effects as far as possible. But countermeasures are not only necessary for the global climate, they may also be relevant to personal health in the shorter term.

Microelectronics is a key lever in reducing global CO_2 emissions while utilising limited resources in the most efficient possible way. Semiconductor technologies give us comprehensive energy efficiency solutions that help minimise losses, generate clean and green energy, enable higher device and application performance and make energy use responsible and smart. They make renewable energy more reliable by converting to green electricity very efficiently so that we can stop burning fossil fuels. They make our grids smarter to balance energy production, transmission and storage and thus help compensate the differences between day and night or north and south. And: semiconductors help manage and consume available energy more efficiently by enabling IoT applications. IoT technologies have proven to be crucial in every step of generation, transmission, storage and especially consumption of electricity. ▶

This year temperatures in many regions went up to values that are difficult to bear for many people or even dangerous to their health

Semiconductor solutions as an elementary component of IoT

Semiconductors connect the real with the digital world and thus make the IoT happen. This takes five steps: sense, compute, actuate, connect and secure.

- **Sensors** capture environmental information and convert it into digital data. Thus, they mark the beginning of any smart action, since they can measure a wide variety of data such as temperature, presence of people and more.
- **Microcontrollers** make products smart by processing the data and initiating actions based on machine learning.
- **Actuators** convert these control signals into action, such as motion, for example, turning a fan, heat and switching lights on and off.
- **Connectivity solutions** such as 5G, Wi-Fi and Bluetooth link devices to each other and to cloud services. These solutions are vital to making devices talk to one another and execute corresponding actions.
- **Security** is indispensable in preventing fake or manipulated data from entering the system and initiating unintended actions. In addition, all IoT applications need to be protected from becoming gateways for unwanted access to networks and infrastructures.

A smart air conditioner solution is equipped with semiconductors that see, hear, feel and understand its environment and is connected to the Internet of Things

Smart building applications help improve the CO_2 footprint

Residential, public and office buildings account for one of the largest shares in global energy demand. In the EU, buildings are responsible for 40% of energy consumption and 36% of CO_2 emissions[1]. However, intelligent sensors make it possible to reduce their energy consumption by 30% and to turn buildings into smart buildings.[2] In addition to that, IoT technologies make it possible to improve heat, light and fresh air management and to monitor, communicate and trigger actions. And beyond shutters, air conditioners and heating, connected and energy-efficient home appliances, entertainment, lighting and home automation also help save energy. Ultimately, smart home and smart building solutions help cut operating costs, improve security by dovetailing different systems and technologies, increase comfort and make energy use more efficient at the same time.

It's worth taking a closer look at a concrete example, such as a smart air conditioner: This year temperatures in many regions went up to values that are difficult to bear for many people or even dangerous to their health. Therefore, the demand for air conditioning is rising. However, this also increases power consumption. Climate change is making the issue even more urgent. For instance, researchers at Penn State University warn that in the southern US demand for air conditioning could exceed available energy in the early 2030s if neither energy infrastructure nor air conditioner efficiency is improved. The growing number of heat waves and the extensive need for air conditioning even bear an additional risk of blackouts, which means we urgently need solutions.

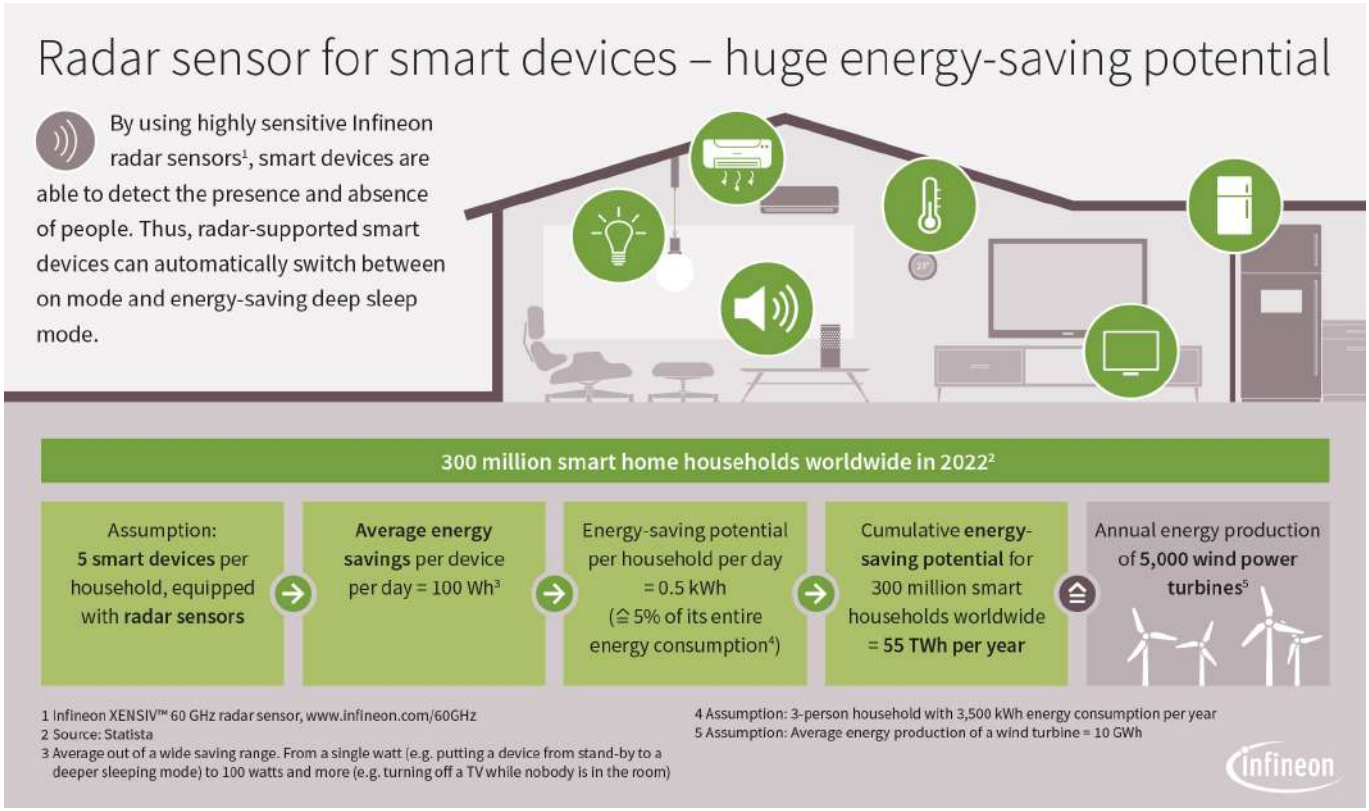
A smart air conditioner solution is equipped with semiconductors that see, hear, feel and understand its environment and is connected to the Internet of Things. Sensors detect the location and number of people within a room or space, turning the air conditioner on and off or adjusting the fan speed and swing mode depending on the location of the occupants. The air conditioner can measure temperature, CO_2 concentration and air quality to decide when to supply fresh and cool air. Direct processing of the data generated is therefore indispensable and takes place on a constantly increasing number of computing devices. Artificial intelligence complements this by deciding whether the data needs to be transmitted securely to the cloud or whether the data could or even must be processed directly at the edge. Ultimately all this information and these processes can be used to automate the control system in order to reduce the energy consumption of the air conditioning system – while increasing quality of life at the same time. Thus, the IoT can turn an air conditioner from a device into a smart service that optimises living conditions. All of this heralds a game-changing user experience and unprecedented levels of energy efficiency.

Smart energy management in buildings improves our energy consumption behaviour

IoT technologies help us successfully manage our behavioral change towards a more conscious and effective use of energy. Smart energy management in connected homes and buildings can enable additional energy efficiency. In addition to the pure energy consumption of individual smart devices, the interconnection of smart things opens up far greater potential for making buildings greener and applications more sustainable. For example, based on the data generated by all smart home devices in your home the system can learn your personal temperature preferences in different situations and can make you feel more comfortable in your own home while simultaneously saving a lot of energy.

Using the unlimited potential of sun and wind requires combining different devices in a smart system where everything communicates with ▶

1 European Commission: "Energy efficiency in buildings"; Feb. 2020
2 Office of Energy Efficiency and Renewable Energy (EERE): "Building Controls"; Aug 2022



everything else. Optimised load shifting to ensure the best possible utilisation of electricity generation and its use at the right time is therefore a major lever in energy management, given the great fluctuation uncertainties of renewable energy sources – and is only conveniently possible thanks to intelligent devices. For example, intelligent smart home networks could help automatically run washing machines and dryers when solar power is available, or store the power for use at night according to user demand. Edge AI is key in unleashing the potential of vastly reduced processing latency, thus enabling reduced energy consumptions.

This is a very reliable way to simultaneously reduce costs and emissions while driving the transition to renewable energy. Furthermore, semiconductors integrated in radar sensors help avoid unnecessary energy consumption by turning off lights, heating and air conditioning when no one is in the room. These sensors reliably enable presence detection without identifying individuals. Loss of privacy is often cited as a concern in the context of camera-based motion detection in particular, since camera-based systems invade private spaces, meaning users do not fully trust them. In addition, smart thermostats and learning algorithms manage usage in the most intelligent manner, significantly reducing unneeded energy consumption.

Another important use case for IoT technologies is predictive maintenance. Machine downtime can cost companies and consumers a lot of money. Systems that are not running optimally often consume more energy before breaking down. These are just two good reasons to avoid accidental downtimes. This is what makes predictive maintenance so important. It provides the ability to optimise maintenance tasks in real time throughout the life of the system, maximising asset life and operational flows without interrupting operations.

However, it is important to remember that predictive maintenance, or even better, predictive maintenance services, are built on information generated using millions of data points, sensors and machines. Many companies are already using predictive maintenance solutions which continuously evaluate data from machinery and compare it with past samples. This makes it possible to detect impending malfunctions before they actually occur.

A typical use case is the maintenance of heating, ventilation and air conditioning (HVAC) systems where sensors monitor current, vibration and ▶

Reliable and trustworthy data forms the basis of a digital twin, representing for example a machine or a smart building

airflow in motors, compressors and fans. A comprehensive IoT solution combines sensors with microcontrollers, connectivity solutions and algorithms for data generation, transmission and big data analysis in the cloud to predict maintenance needs at the edge. Nevertheless, security is becoming a relevant prerequisite, enabling secure collaboration while protecting the manufacturing process and entire value chain.

All these parts are building blocks for reliable predictive maintenance applications. However, they also need to be protected against unauthorised access and against manipulation. Useful algorithms can only be found by analysing trustworthy data and using artificial intelligence as well as machine learning.

Reliable and trustworthy data forms the basis of a digital twin, representing for example a machine or a smart building. The data lets us simulate the interaction of people with their environment, their offices, meeting rooms and cafeterias and ultimately optimise the control of temperature, light and fresh air. Corresponding behavioral models help in understanding the derivations of the lifetime of such a system. That makes it possible to detect, recognise and understand every bias in operation and to predict – or, even better, prevent – the moment the system or a part has to be repaired, renewed or exchanged.

Thomas Rosteck
division president, Connected Secure Systems
Infineon Technologies

Digitalisation offers outstanding potential for decarbonising both economy and society. The Internet of Things (IoT) is a game changer for intelligent use, analysis and smart control of connected devices and services.

While smart grids are key in bringing green energy from north to south and from day to night, intelligent use of energy in an increasingly technologised world is the order of the day when making a relevant contribution in private life situations as well as in industrial contexts. Energy is not only closely intertwined with economic growth but is also an essential component in the transformation to a more sustainable world. IoT provides the foundation necessary to accompany this shift. Intelligent, connected and without human intervention.

Adam White
division president, Power & Sensor Systems
Infineon Technologies

Sensors mark the ‘point of beginning’ of every IoT system, collecting data from the environment surrounding a connected device. They provide senses almost similar to those of human beings. Sensors can measure temperatures, they can smell, detect presence, feel pressure, hear sound and sense movement. Thus, they provide the decisive basis for optimised controls that are perfectly adapted to the respective application scenarios. By incorporating our sensors, we can transform formerly non-intelligent devices - such as simple timers for lamps - into intelligent devices that improve energy efficiency without sacrificing quality of service, for example in the areas of heat, light and ventilation.

Infineon at Electronica: Driving Decarbonisation and Digitalisation. Together.
Microelectronics is the core of every smart and energy efficient solution. Sensors, actuators, microcontrollers, communication modules and security components underpin every IoT device. Infineon’s system solutions, including software, let new functions and services link the real with the digital world. Together with our customers, we build smart IoT solutions to decarbonise both economy and society by increasing energy efficiency. This is our contribution to preventing climate change and improving quality of life at the same time.

If you’re interested in more information and insights on our smart HVAC solution and much more, come visit us at electronica, the world’s leading trade fair and conference for electronics, November 15-18, 2022, in Munich or digitally:
http://www.infineon.com/electronica

Connecting Wireless Data
Deploying IoT Everywhere

As IoT becomes increasingly essential for business operations, the need to deploy IoT applications everywhere puts greater emphasis on wireless connectivity of all types – including cellular, LoRa, satellite and Wi-Fi.

- Numerous satellite IoT constellations are now deployed or being deployed
- LoRaWAN is taking off everywhere
- 5G rollout is putting cellular IoT on steroids
- Private cellular networking is now hugely attractive for enterprise IoT
- Wi-Fi has graduated to Wi-Fi 6 and soon Wi-Fi 7 with IoT as a key target

beecham research

Shaping the IoT future

This 100+ page, independent analyst report is the latest addition to Beecham Research's popular 'Succeed with IoT' series.

> "LoRa lines-up well from a cost perspective. You have the ability to roll-out a fully private network that is actually cellular like."
>
> VP Business Development. Providing LoRaWAN, NB-IoT gateways, sensors and custom applications.

> "A feature of satellite IoT is that many operations have critical communication needs, in that high reliability is essential."
>
> Director, Product and Commercial (Global). Providing global coverage and high broadband capacity on LEO constellation.

> "The potential for NB-IoT and LTE-M is huge."
>
> Network Engineer. Providing solutions in 5G, LTE, IoT private nets, global services, management and security.

- Exclusive interviews with business leaders
- Survey findings
- Market analysis
- Use cases and case studies
- Technical insights

Report sponsored by...

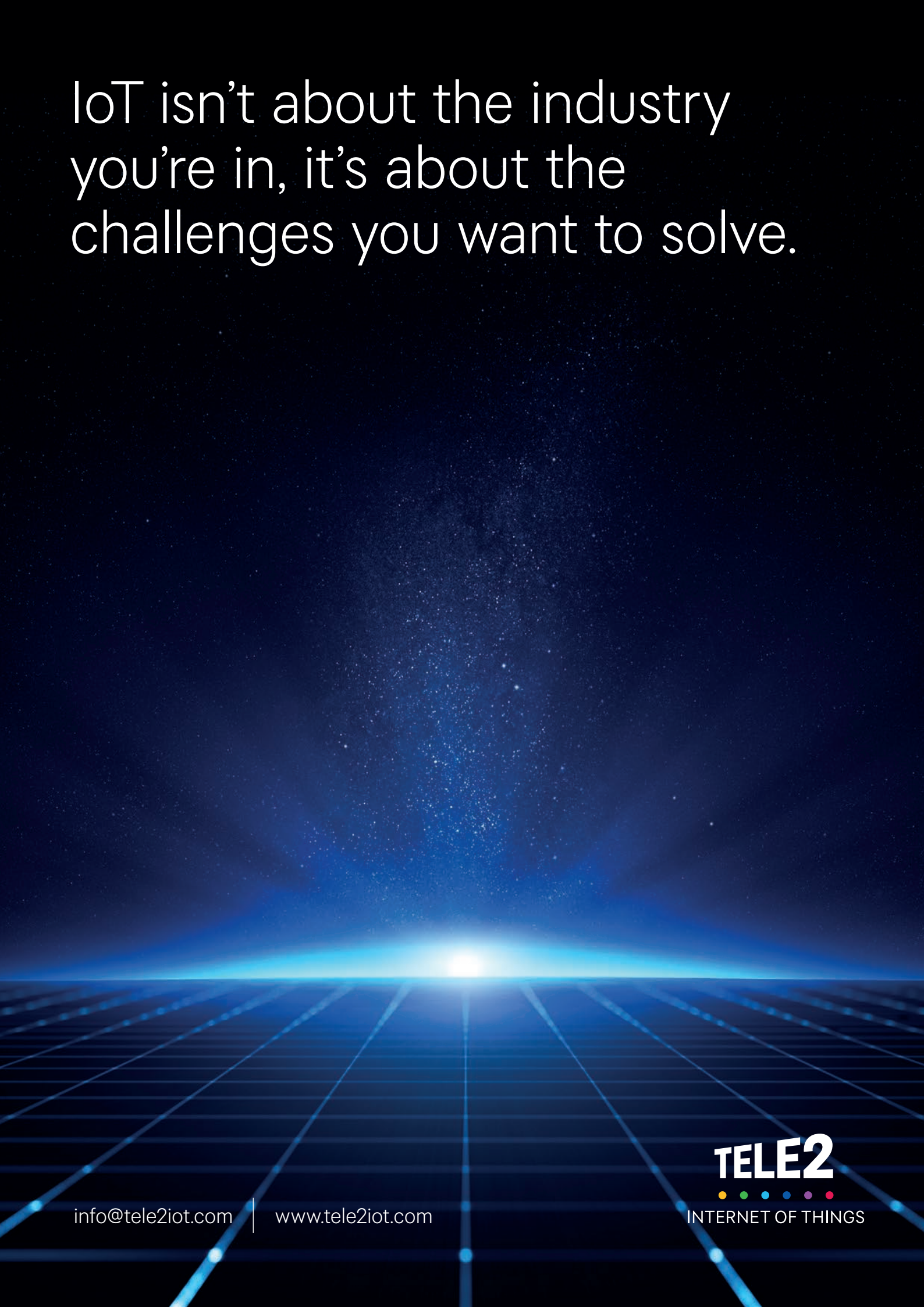
Airgain

iridium

MULTITECH

THALES

Dowload for FREE at: www.iot-everywhere.com


IoT isn't about the industry you're in, it's about the challenges you want to solve.
info@tele2iot.com
www.tele2iot.com
TELE2
INTERNET OF THINGS