IoT Now: ISSN 2397-2793

Q3 2023 • VOLUME 13 • ISSUE 3

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

12-PAGE SMART CITIES SECTION INSIDE

INTERVIEW

floLIVE collaborates with Qualcomm to enhance global connectivity on the Qualcomm Aware Platform

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

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

CONNECTIVITY
Will module makers take on integrated IoT connectivity?
Read the IoT Now report inside this issue

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

PLUS: Libelium CEO explains how smart cities can go beyond the challenges they face • Juniper Research details how to unlock the potential of smart cities • iSIMs explained • Is Connectivity-by-Design the optimum approach for IoT? • Transforma Insights reveals best practice for delivering IoT connectivity • Why verticals needs specific capabilities in non-horizontal IoT • Three top tips for IoT security • News, Features and Interviews online at **www.iot-now.com**

UK Government

MADE IN THE UK SOLD TO AUSTRALIA AND NEW ZEALAND

"The new free trade agreements with Australia and New Zealand will make trade easier and cheaper and will help us grow sales, which I like the sound of."

Melissa Beckett, fintech developers, Kani Payments

Find practical advice on how to use the new agreements at **great.gov.uk/freetradeagreements**

GREAT
BRITAIN & NORTHERN IRELAND

CONTENTS

8 INTERVIEW
Nir Shalom, floLIVE and
Mohammed Ansari , Qualcomm Technologies

20 CASE STUDY

30 INTERVIEW

IN THIS ISSUE

04 COMMENT
George Malim considers whether experience should just be viewed as another brick in the wall?

05 COMPANY NEWS
IOTech expands north American presence with Dell investment, floLIVE and Qualcomm collaborate to enhance global connectivity

06 CONTRACT NEWS
BMW Group selects AWS for its Vision Neue Klasse, Karcher to use Deutsche Telekom IoT connectivity for drier scrubber

07 MARKET NEWS
Berg Insight predicts IoT satellite subscriber base to reach 23.9m by 2027, Alcatel-Lucent and Nokia support Grand Paris Express project

08 INTERVIEW
floLIVE's Nir Shalom and Qualcomm Technologies' Mohammed Ansari lift the lid on their collaboration to enable simplified, frictionless asset tracking with global connectivity that has been designed for things, not people

13 ANALYST REPORT
Our 7-page report, authored by experts at Analysys Mason assesses the opportunity for module makers to sell integrated IoT connectivity

20 CASE STUDY
Inside Bermad's deployment of narrowband-IoT connected irrigation controllers with floLIVE global connectivity

22 IoT NOW ONES TO WATCH
The companies that have caught our attention in the world of IoT connectivity

24 IoT SECURITY
Wireless Logic's Simon Trend provides his three top tips for IoT security

26 INTERVIEW
Tele2 IoT's Onur Kasaba explains why vertical capabilities are needed now the IoT market is no longer horizontal

SMART CITIES SECTION

30 INTERVIEW
12 pages of smart city content starts here with Libelium's Alicia Asin Perez telling George Malim how holistic, data-fueled IoT can drive smart cities beyond their challenges

34 ANALYST REPORT
Juniper Research shares its latest insights into how the potential of smart cities can be unlocked

40 FEATURE
Antony Savvas says that while most projects have not lived up to the hype, the latest developments are changing the smart cities story

42 iSIM
G+D sets out the benefits that integrated SIM (iSIM) can bring to your deployment

44 CONNECTIVITY-BY-DESIGN
Transforma Insights study identifies connectivity-by-design as the optimum approach for IoT

46 VISION STACK
Dr Brad Canham introduces the Vision Stack and explains why your company needs it for IoT success

51 ANALYST REPORT
Transforma Insights details its view of best practice for delivering IoT connectivity in a 7-page report

58 5G MMWAVE
Fibocom asks if 5G mmWave is the technology behind next-level connectivity for IoT

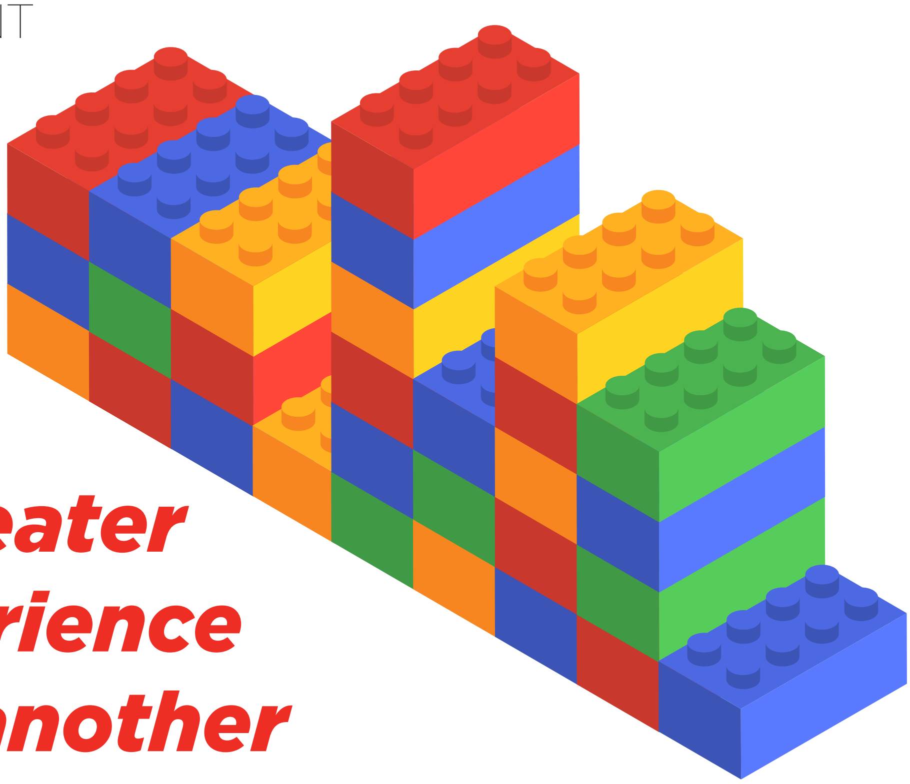
60 REGULATION
As IoT matures, regulation becomes tighter and more necessary. We take you through the latest developments

62 EVENT DIARY
Where to go and what to see

flo. LIVE

Cover sponsor: floLIVE operates the first and largest hyperlocal global cellular data network, based on local POPs in dozens of locations worldwide. With the largest global connectivity library of its kind, we provide centrally managed, localised connectivity for any device, anywhere.

Global means no limits on where you do business; local means low latency, high performance and full compliance.
Our network has been designed to comply with the emergence of privacy acts, data regulations and roaming restrictions. Best of all, we provide direct access to our network, that lets you control your connectivity as if you were the carrier. Monitor your devices, access real-time network events and usage, switch operators remotely, and troubleshoot failures ahead of time, so your devices never miss a beat. For more information, visit **www.flolive.net**



Is greater experience just another brick in the IoT wall?

An executive commented in a recent interview with IoT Now that their company's knowledge has enabled it to gain experience in enabling customers' IoT projects. That experience creates greater knowledge and contributes to a virtuous circle of improved capability

George Malim, managing editor

Obviously to start something you need some knowledge so, a provider of a device, such as a chainsaw, might look at its business and consider how connecting its products could enable new revenues and better customer experience. The knowledge that cellular networks, for example, exist and are ubiquitous is enough knowledge to know a device can be connected but it certainly isn't informed by the experience of whether services based on connecting the device will be successful.

The knowledge that you can do something doesn't mean you should do it. The experience of deploying a connected device and understanding what improvements could be made from the performance of the pilot creates greater knowledge that can be applied to the next version to handle challenges such as scaling up or creating a global solution. So knowledge empowers experience which creates more knowledge which in turn feeds deeper experience.

This virtuous laying of building block after building block composed of knowledge and experience is creating a sense of maturity in IoT. The baseline is raised with each layer of blocks so more and more organisations see potential in IoT-enabling their businesses. The combined knowledge and experience then federates across multiple industries and technologies so further knowledge and further experience are added to the knowledge base.

The blocks continue to build to the extent that each gain of knowledge or experience becomes just another brick in the wall of IoT progress.

Enjoy the magazine!

George Malim

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

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

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

DESIGN
Jason Appleby
Ark Design
Tel: +44 (0) 1787 881623

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

© WeKnow Media Ltd 2023

All rights reserved. No part of this publication may be copied, stored, published or in any way reproduced without the prior written consent of the Publisher.

SUBSCRIBE COMPLETELY FREE ONLINE:
www.iot-now.com/register
(You can cancel any time).

EDITORIAL ADVISORS

Robin Duke-Woolley, CEO, Beecham Research

Andrew Parker programme marketing director, IoT, GSMA

Gert Pauwels head of commercial and marketing IoT and M2M, Orange Belgium

Robert Brunbäck director, Connectivity, Lynk & Co

Aileen Smith chief strategy officer, UltraSoC

David Taylor Board advisor on Digital and IoT innovation

IOTech expands North American presence with investment from Dell Technologies Capital

IOTech, has announced an expansion in the North American market, fuelled by additional investment led by **Dell Technologies Capital**. The investment will support go-to-market in the region and accelerate product development of its open edge data platform. To help further drive growth in the US, IOTech has also appointed David King to its board of directors.

The recent investment included existing investors Dell Technologies Capital, the holding company of the **Périer-D'Ieteren** family, **Northstar Ventures** and the **Scottish Investment Bank**. "IOTech's platform lets enterprises capitalise on the massive volume of data generated at the Industrial IoT edge," said Gregg Adkin, the managing director of Dell Technologies Capital. "Its technology has proven to be valuable to manufacturing and energy customers. Building out in the North American market creates opportunity to address new vertical use cases, and to help more organisations realise the full potential of their edge data."

North America represents IOTech's largest market opportunity and additional funding will allow company to invest in expanded sales, marketing and pre-sales support to deliver deployments and future customer engagements. As part of its expansion across North America, IOTech recently expanded its technology skills with the addition of field CTOs.

Gregg Adkin, Dell Technologies Capital

IOTech makes industrial data easily accessible, actionable and manageable for providers and consumers of industrial edge solutions. Its partners and customers are comprised of some of large industrial original equipment manufacturers (OEMs), independent software vendors (ISVs) and systems integrators (SIs) across industrial automation, renewable energy, building automation and other vertical markets. Customers include **Accenture**, **EATON**, **Fluence Energy**, **Johnson Controls**, **King Steel** and **Schneider Electric**.

"The industrial edge is the key to extracting the full value of industrial organisations' data and IOTech is well-positioned to take that key and open the door to new business opportunities for its customers and partners," said King. "It's an exciting and pivotal time for the company and I'm looking forward to serving in an active role in its continued growth and success." ■

floLIVE and Qualcomm collaborate to enhance global connectivity on Aware platform

floLIVE has announced that it is working with **Qualcomm Technologies** and its subsidiaries to enhance global connectivity on the new Qualcomm Aware platform. By unifying and optimising hardware, software, developer-friendly tools, global connectivity, and positioning capabilities at the chipset level, Qualcomm Aware is set to help add digital intelligence, visibility, and control to enterprises while alleviating the market fragmentation challenges and deployment complexities that currently exist, in a more simple, security-focused, and scalable way.

The addition of floLIVE technologies to the Qualcomm Aware ecosystem advances intelligent global connectivity capabilities due to a hyperlocal global cellular network offered by floLIVE that's designed to cater to demands of OEMs and global enterprises. The floLIVE solution intelligently works together with a broader suite of Qualcomm Aware technologies and intelligence to provide virtually seamless local connectivity on a global scale and aims to redefine how IoT devices connect and communicate globally.

"Qualcomm Technologies' integration of floLIVE into the Qualcomm Aware Platform to help enhance global connectivity is a testament to our dedication to delivering innovative and impactful global connectivity solutions," said Curtis Govan, the president for Americas at floLIVE. "We are excited to collaborate with Qualcomm Technologies to bring our hyperlocal cellular network expertise to the Qualcomm Aware Platform, empowering businesses to harness the full potential of IoT with confidence."

Mohammed Ansari, the senior director of business development at Qualcomm Technologies, added: "We are excited to welcome floLIVE into the Qualcomm Aware ecosystem as a collaboration partner to intelligently enhance global connectivity of IoT devices. A key differentiator of Qualcomm Aware is the ability to embed and optimise connectivity on IoT devices globally, with security as a focus, and intelligently manage the link from device to the cloud in a way that is designed to address the needs of customers across diverse industries." ■

News in Brief

Quectel expands R&D centre in Penang

Quectel Wireless Solutions has expanded its research and development centre in Penang, Malaysia. The centre has moved to larger premises in the city and has added functionality including a testing lab and anechoic chamber, alongside manufacturing facilities in the centre. The expansion will enable Quectel to provide customised and off-the-shelf products and services to its Asia-Pacific and global customers in future.

"We are thrilled to grow our operations in Penang," said James Cai, the general manager of Quectel's R&D facility in Penang. "The expansion will allow for accelerated innovation and development based on customer requirements and provide regional support and production."

Founded to meet precise requirements of IoT customers and to guarantee response to product development needs and market deployment, the R&D centre is equipped with an advanced testing laboratory and an anechoic chamber, covering hardware and firmware design, testing skills, and more, rendering it an optimal setting for exhaustive testing, debugging and customer device evaluations. ■

BMW Group selects Amazon Web Services for its automated driving platform

BMW Group has chosen **Amazon Web Services** (AWS) as cloud provider for its automated driving platform. BMW Group will develop its future advanced driver assistance system (ADAS) using AWS to help create new features for its vehicles, such as Neue Klasse, which it is set to introduce in 2025. The cloud-based system will use BMW's pre existing cloud data hub on AWS, and will use AWS compute, generative artificial intelligence (GenAI), Internet of Things (IoT), machine learning, and storage capabilities to help accelerate delivery of highly automated BMW vehicles.

"In the next decade, consumer habits and expectations will drive more changes in the automotive industry than we've seen over the past 30 years," said Nicolai Martin, the senior vice president of driving experience at BMW Group. "This is just the beginning of a new era of highly automated driving, fuelled by innovations in technology and engineering. By collaborating with AWS, the BMW Group, along with our partner, **Qualcomm Technologies**, is building our new automated driving platform on AWS's scalable, secure and reliable infrastructure. We're tapping into AWS's ability to help empower the next generation of BMW's automated driving and parking functions."

BMW Group has also joined Qualcomm, to co-develop automated driving systems based on open and modular Snapdragon ride platform. The systems feature an integrated ride vision software stack to enable 360-degree perception for vehicles. Together with AWS and Qualcomm, BMW Group's engineers have access to hardware, vision software and cloud capabilities in an end-to-end automated driving development platform. Placing BMW Group's automated driving platform in cloud helps break down development silos within vehicle software teams at BMW Group and helps foster greater global collaboration with suppliers to accelerate automated driving.

The BMW Vision Neue Klasse

Kärcher to use Deutsche Telekom's IoT network for cleaning robots

Kärcher has connected its autonomous robot scrubber drier to the Internet of Things (IoT) using **Deutsche Telekom**'s IoT network. Cleaning specialist Kärcher's new Kira B 50 scrubber drier can be used in production and storage facilities, supermarkets and shopping centres or hospitals. The cleaning robot navigates autonomously by means of a number of optical and acoustic sensors. Kärcher uses an IoT tariff in Deutsche Telekom's LTE network to transmit the machine's cleaning reports and operating data securely to the cloud for digital fleet management. An industrial-grade Deutsche Telekom SIM is built into a wireless module during the robot's production. The wireless solution can be retrofitted into other Kärcher cleaning machines.

Thanks to the devices' IoT connectivity Kärcher customers, such as building services providers or facility managers, have a constant overview of their machine fleets, their deployment locations and times, the fill levels of water and their battery status. In the event of malfunctions users can be notified by email or text message. Software updates that might be needed for troubleshooting can be downloaded onto the device over-the-air. "The feedback from our customers was clear and unequivocal: what they wanted was remote access to their machines and to view the status of the machines," said Alina Seitter, product manager for robotics at Kärcher. "They also wanted to receive error reports immediately by smartphone and to download digital cleaning reports. Deutsche Telekom's IoT connectivity enables us to do all of that."

Thanks to Deutsche Telekom's international cellular networks and global roaming agreements Kärcher can market its new autonomous cleaning machine in all 80 countries around the world where Kärcher's more than 150 subsidiaries are located. Kärcher does not have to look for local network providers. "Our key account customers often demand extensive device tests in different countries," added Seitter. "Thanks to Deutsche Telekom's global network coverage we can fulfill this requirement at any time."

Kärcher's Kira B 50 scrubber drier

News in Brief

Gorilla Technology commences smart government project in Egypt

Gorilla Technology Group has begun a project to provide the Government of Egypt with a smart government security convergence solution. The project will contribute to Egypt's Vision 2030 objectives.

"Driven by global threats, we are pushing the boundaries of cutting-edge technology innovation and progress for defence networks," said Jay Chandan, Gorilla's chairman and chief executive. "We are thrilled to kickstart the project and embark on this journey. I am extremely proud of the Gorilla team and elated to share a profound commitment that beats at the heart of my endeavours, the unwavering dedication to transforming Egypt into a technological giant. With our keystone project in Egypt progressing, we have begun generating revenue and cash flow, increasing our cash balance and providing ample runway to capitalise on the growth opportunities ahead of us."

Global satellite IoT subscriber base to reach 23.9m by 2027, says Berg Insight

Johan Fagerberg, Berg Insight

According to a new research report from IoT analyst firm **Berg Insight**, the global satellite IoT communications market is growing at a steady pace. The global satellite IoT subscriber base grew to surpass 4.5 million in 2022, the firm says. The number of satellite IoT subscribers will increase at a compound annual growth rate (CAGR) of 39.6% to reach 23.9 million units in 2027. Only about 10% of the Earth's surface has access to terrestrial connectivity services which leaves a massive opportunity for satellite IoT communications.

Satellite connectivity provides a complement to terrestrial cellular and non-cellular networks in remote locations: and is especitially useful for applications in agriculture, asset tracking, maritime and intermodal transportation, oil and gas industry exploration, utilities, construction and governments. Incumbent satellite operators and more than two dozen new initiatives are now betting on the IoT connectivity market. The new study covers a total of 44 satellite IoT operators.

"**Iridium**, **Orbcomm**, **Inmarsat** and **Globalstar** are the largest satellite IoT network operators today", said Johan Fagerberg, the principal analyst at Berg Insight. Iridium grew its subscriber base by 20% in the last year and reached the number one spot serving 1.5 million subscribers. Originally a dedicated satellite operator, Orbcomm has transitioned into an end-to-end solution provider, delivering services on its own satellite network as well as being a reseller partner of Inmarsat and others. At the end of Q4-2022, the company had 1.1 million satellite IoT subscribers on its own and Inmarsat's networks. At the same time Globalstar reached 0.44 million subscribers.

Other players with connections in the tens of thousands include for instance **Myriota** in Australia, **Kineis** in France and **Thuraya** in the UAE. In addition to the incumbent satellite operators a number of new initiatives have appeared on the market recently. Examples of some high-profile projects are **Astrocast**, **AST SpaceMobile**, **CASC/CASIC**, **E-Space**, **Fleet Space Technologies**, **Hubble Network**, **Kepler Communications**, **Kineis**, **Ligado Networks**, **Lynk**, **Myriota**, **Omnispace**, **Skylo**, **Swarm Technologies (SpaceX)** and **Totum**.

Alcatel-Lucent and Nokia to support Grand Paris Rail project

Alcatel-Lucent Enterprise and **Nokia** have partnered to support Grand Paris Express. The future subway includes 200 kilometres of rail that will create four additional lines around Paris (lines 15, 16, 17 and 18) and extend the existing line 14. In addition, 68 subway stations will be built, helping to create sustainable urban centres in these locations.

Alcatel-Lucent Enterprise and Nokia combined their offers to provide certified and integrated end-to-end mission-critical infrastructure for Grand Paris Express. These offers are with solutions that include a Nokia multi-service IP/MPLS (internet protocol/multi-protocol label switching) high-speed backbone network which includes a router portfolio to meet all operation and maintenance requirements of Grand Paris Express. "We are very proud to partner with Nokia, to deliver state-of-the-art digital transformation for the Grand Paris Express smart mobility project," said Rukmini Glanard, the chief business officer at Alcatel-Lucent Enterprise. "Together we will provide a certified mission-critical network, supporting carbon-free transportation. This project is a perfect example of our 'Technology for Good' strategy."

Nathan Stenson, the vice president of global partner channel at Nokia, added: "We are thrilled to strengthen the relationship with our technology and go-to-market distribution partner Alcatel-Lucent Enterprise, providing mission-critical end-to-end network architecture based on Nokia IP/MPLS technology. This state-of-the-art technology enables a powerful multi-service IoT network that provides air quality and video monitoring in stations with 13,000 cameras and artificial intelligence (AI) to enhance safety and security throughout the Grand Paris Express."

News in Brief

Ooredoo joins IoT World Alliance

Ooredoo Group has joined **IoT World Alliance** as the sole operator representing Middle East and North Africa region within the Alliance. The IoT World Alliance is a mobile network operator cooperative. Acting as a global forum of telecoms providers, it is dedicated to tracking IoT connectivity trends and sharing skills with partners and customers to help reduce complexity associated with worldwide deployments of connected devices.

As an Alliance member, Ooredoo is now an integral part of global IoT discussions, sharing valuable insights from its presence in region and gaining access to programme for exchanging knowledge and experiences. Ooredoo Group will also be able to assist other operators in facilitating ideal connectivity for customers entering its region. This advantage positions Ooredoo as an important partner for operators looking to expand their IoT services into new markets.

Simplified, frictionless asset tracking and monitoring relies on connectivity designed for things, not people

When Qualcomm Technologies developed the Qualcomm Aware Platform, its intention was to create a simple way for enterprises and developers to create scalable and security-focused solutions that add connected intelligence to a wide range of industrial uses. To achieve this, Qualcomm Technologies leaned on its decades of expertise as a wireless technology leader and innovator, and strong relationships with a variety of hardware and software partners to help address a fragmented IoT ecosystem that has been a key roadblock for enterprises who sought to add connected intelligence to their operations. A key area that Qualcomm Aware aimed to simplify is on the connectivity side by taking a differentiated approach through offering the ability to embed and optimise connectivity on IoT devices globally.

In order to achieve a true digitalisation solution, there needs to be uninterrupted global connectivity with flexibility to scale up as required. For this reason, Qualcomm Technologies has collaborated with floLIVE as an early ecosystem partner to enhance global connectivity capabilities on the Qualcomm Aware Platform. Nir Shalom, the chief executive of floLIVE, and Mohammed Ansari, the senior director of Business Development for the Qualcomm Aware Platform, explain to IoT Now managing editor George Malim, how the platform benefits organisations and how the two companies have collaborated to keep things simple for customers

George Malim: What makes the Qualcomm Aware Platform a unique, new offering?

Mohammed Ansari: The Qualcomm Aware Platform is designed to reduce the friction hardware designers face in developing IoT solutions and also for web and app developers to be able to get data from Qualcomm-based devices into any cloud and any enterprise system much more easily. There are several optimisations for different use cases our broad portfolio of system on chips (SoCs) supports. Until now, we've had SoCs that address use cases from low power to those that can run artificial intelligence (AI) at the edge but what we haven't done before is connect edge intelligence to the cloud.

The Qualcomm Aware Platform seeks to address a wide variety of uses across industries, beginning with asset tracking and condition monitoring solutions. We chose these use cases because several industries face problems with accurately tracking their assets and fleets, especially as environmental and operational conditions change and impact operations.

Location technology and positioning capability are central to Qualcomm Aware and from an accuracy perspective we're able to support anything from one kilometre to the centimetre-level, thanks to a variety of signal types and positioning algorithms that can be used depending on the intended application. We will cover the whole range of requirements within the next one to two years and address the complexities inherent to various use cases. For example, variations in the frequency of location updates and reports can range from daily or longer down to 15 minute increments for shipments of pharmaceuticals.

The complexities behind enabling diverse use cases are what we are abstracting behind configurable application programme interfaces (APIs) and the Qualcomm Technologies' location positioning engines. All of that will make customers be able to make designs based on the service configuration and this will be done in real-time. Further complexity is abstracted away in the connectivity, with different technology available for different use cases and for condition ▶

SPONSORED INTERVIEW

Nir Shalom
floLIVE

Mohammed Ansari
Qualcomm Technologies

monitoring we'll have sensors in our SoCs or in peripheral functions.

GM: Can you elaborate more on why providing integrated connectivity to devices operating on the Qualcomm Aware Platform is a natural fit for floLIVE?

Nir Shalom: Mohammed started by talking about the friction that exists in the market. If you look from the device level to the connectivity layer and on to data management and cloud services, many of these different elements of the IoT value chain have evolved significantly in the last few years, but connectivity hasn't. It's a legacy solution that is very limited in what it can provide and it doesn't correspond with the price points the market requires. Furthermore, it's not always up to meeting the speed, security and data performance requirements of the market.

The reason for this is that connectivity providers took what they had for the consumer cellular market and tried to adapt it for IoT. This isn't a natural fit because IoT devices don't behave and aren't utilised in the same way as your mobile phone. We created floLIVE to solve all the problems inherent to the old approach - a global solution built from the ground up for things, not people. It's very modern by nature and cloud-native, hence very flexible and scalable. In essence, we're building a global, hyperlocal network that is purpose-built for IoT.

GM: What are the main complexities currently facing enterprises who want to add more connected intelligence to their businesses?

MA: Nir explained some of the issues with traditional cellular connectivity and it's true that, in general, cellular connectivity has been broken because it was designed for a different use case – the smartphone. The challenges of connecting industrial assets is that they are very diverse assets with diverse use cases. These range from being in open sky settings to being indoors to moving through areas of different network coverage.

The total cost of ownership is always a challenge in asset tracking and there are significant recurring costs involved that go beyond the initial installation cost. Cost is therefore a key consideration and when we look at connected intelligence we see cellular connectivity as the most cost-effective method but there are areas where cellular won't work so we look at satellite, indoor sub-1Ghz network with both star and mesh network topologies that can have significant impacts on battery life and power consumption. ▶

A Qualcomm Aware device

Collaborating with floLIVE through an API-first approach makes it easier to deliver an embedded and optimised solution

For customers, we're wrapping all of this complexity, including on the connectivity side by collaborating with companies like floLIVE, to embed and optimise technologies to work in a power-optimised and intelligent way on Qualcomm Technologies' chipsets, and making it easy to access, deploy and build on through Qualcomm Aware APIs.

The other important point about cost with Qualcomm Aware is the amount of data that goes from the edge to the cloud. We're uniquely positioned to make decisions on what data to send which can reduce customers' costs and improve security thanks to our very capable edge compute platforms.

GM: Why is connectivity such a core component of Qualcomm Aware and in what ways does floLIVE's offering align with the API-first, cloud-native, integrated design of the platform?

MA: From an API-first perspective we know that Qualcomm Aware solves part of the problem customers face. It's not a full stack solution because the use cases are fragmented and capabilities are diverse. This is why our API-first approach means the solution can be available to developers, enterprises and independent software vendors (ISVs) to build upon.

Collaborating with floLIVE through an API-first approach makes it easier to deliver an embedded and optimised solution. For example, the floLIVE dashboard and insights could be useful to us or our customers. We do not expose all of it to customers because they don't care in-depth about connectivity, they're mainly interested in location tracking and condition monitoring. Our customers want connectivity and complexity to be abstracted further away from them. They want services enabled via our APIs.

NS: When you build a network for things, not cell phones, you realise that different things connect differently. For example, some connect for a short period of time and then shut off, some will need immediate response from the network in order to preserve battery power while others will not be so power-sensitive.

We believe we can help Qualcomm Aware intelligently enhance its connectivity solutions, with global connectivity that's built for different types of things that can be connected throughout a device's lifecycle; this is what the market needs, because customers are used to obtaining better control and greater visibility into their infrastructure.

Another aspect we're going to help with is connectivity-related information, that's provided in real-time regardless of the specific network to which the device is connected. floLIVE's global network was designed to be a real-time solution, allowing a great deal of control for diverse use cases while also enabling cost optimisation.

Customers are looking to transform their businesses but are constrained by TCO considerations which we address in two ways: the first is that we're cloud-native which means we can support the capability to scale up or down as required. The second is that our philosophy has been to develop the entire set of connectivity components in-house. Other providers mix and match components from different vendors, which is difficult to manage; we have the core network, SIM technology and charging capability to keep costs under control.

GM: Traditionally, end customers would have been responsible for obtaining connectivity in the regions they operate in, but with Qualcomm Aware, enterprises and developers receive a complete package that includes the product, integrated connectivity and a host of other features out of the box. What are some of the pain points offering integrated connectivity will help solve?

MA: A big part is to not have to worry about the underlying radio access network (RAN). With 2G networks being shut down and 3G networks also ▶

floLIVE. Your Backbone For Hyperlocal Global Connectivity

being closed at some point, carriers are ramping up low power wide area (LPWA) networks and narrowband-IoT (NB-IoT) as alternatives. Qualcomm is a big proponent of LTE Cat 1 bis because of its advantages in cost but this shouldn't matter to the customer. We make this possible and also offer flexibility so customers' diverse verticals can be served. We intend to partner with innovative and leading connectivity providers to enable the Qualcomm Aware services platform globally.

Our ability to be global also addresses a major pain point. floLIVE has built a world class platform and we believe in the team. Our plan to collaborate with floLIVE first underscores that it is doing things right.

GM: There are several global connectivity providers with varying definitions of global. What do you see as your differentiators and advantages?

NS: There are two main things we do differently: one is that we have developed our technology in-house and the other is that we are investing in integrating many network operators around the world into our global network; other connectivity providers 'mix and match' different technologies, adding cost and complexity to their business operations; they also do not share our philosophy of trying to obtain as many local or edge partners as possible.

We have multiple networks with integrations into local providers all over the world as part of our global hyperlocal network, all centrally controlled and managed via an API that's fully exposed to Qualcomm Aware. All these networks are controlled in the same way and our global architecture can be minimised onto a set of APIs that can be managed by any enterprise around the world.

GM: The IoT market is fragmented with a significant number of IoT service providers. Do you feel that floLIVE is viewed as a competitor or a complement to other IoT service providers?

NS: When we looked at our portfolio, we thought we'd sell connectivity services to global enterprises to start with, but it's those customers who want to build global solutions that are onboard our platform. It would take a huge effort and very high cost to compete with us, especially now that the options are to simply use floLIVE or compete with it. Every quarter, additional IoT MVNOs become customers of floLIVE and we welcome them to join us so they can focus on what they're good at while leaving the complex task of managing, maintaining and extending the global connectivity infrastructure to us.

GM: You've just completed another investment round. Can you tell us about your plans to use this funding to evolve floLIVE's capabilities and features?

NS: We've just completed an investment round that included significant participation from existing investors including Qualcomm Ventures as well as new investors. We see this as a vote of trust in the alignment of investors with our vision and the funding allows us to accelerate in three key areas - first, we'll keep investing in our in-house technology to make it better and faster to market.

Next, we'll keep expanding our global network and look for mobile network operators to integrate with, thus improving our network presence, performance and optimisation in each region. Finally, we'll add on a new set of services in the security and data transport domains that will help customers solve another piece of the complexity they face – these services will be provided on top of our growing global network infrastructure.

GM: What has the experience of working together been like?

NS: Working with Qualcomm is amazing. To collaborate with a partner that really understands both business and technology, coupled with such high standards and willingness to innovate and bring something fresh to the market is a great journey to be part of. It's exciting as a technologist to work with Qualcomm Technologies and to think about how to develop in the best way possible is a great experience.

MA: Qualcomm Technologies is building an ecosystem around our vast and innovative technology portfolio, large ecosystem of hardware, ODM/OEM, and software partners, along with business platforms, hyperscalers and connectivity providers. We added floLIVE to the Qualcomm Aware ecosystem because of its connectivity expertise and we're really glad we can scale with a global partner.

We have multiple networks with integrations into local providers all over the world as part of our global hyperlocal network, all centrally controlled and managed via an API that's fully exposed to Qualcomm Aware

www.flolive.com

How do you maximise your IoT revenue?

Our advisory service enables you to:

- understand the IoT value chain
- analyse key IoT sectors
- assess opportunities and threats from emerging technologies
- keep up to date with trends and best practice
- size the opportunity
- track other IoT players and benchmark your performance

analysys mason

analysysmason.com/IoT

How is the opportunity for module makers to sell integrated IoT connectivity maturing?

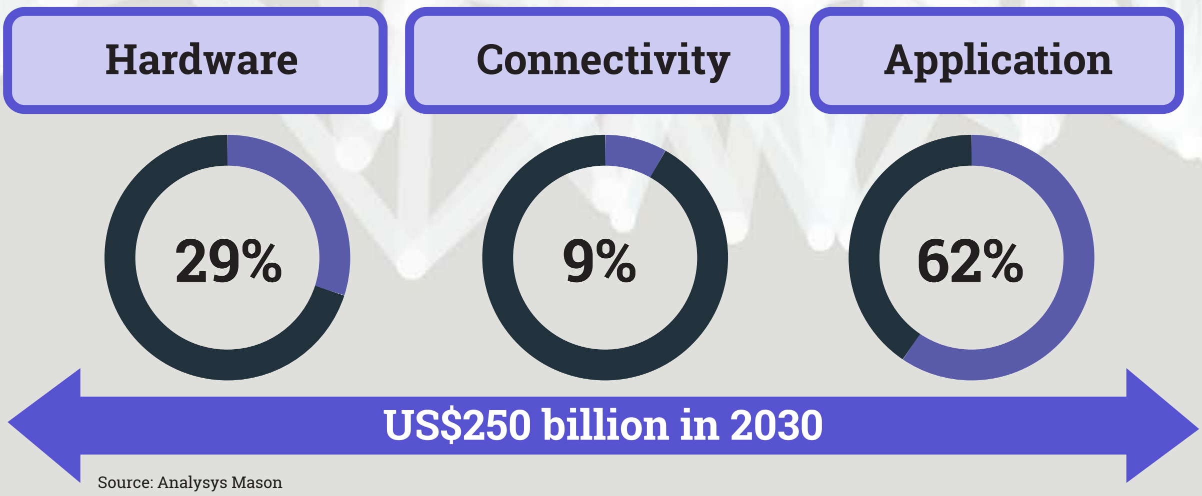
Report sponsor

How is the opportunity for module makers to sell integrated IoT connectivity maturing?

IoT is a relatively new technology: the market and IoT value chain are continuing to evolve and many IoT players are still figuring out their roles. Only a few module makers have attempted to sell IoT connectivity as a complementary offering to their core hardware proposition. This is despite the apparent advantages to module makers of providing an integrated solution, such as generating recurring revenue as opposed to a one-off sale, and a more direct relationship with their direct customers, original equipment manufacturers (OEMs), explain Ibraheem Kasujee, a senior analyst, and Tom Rebbeck, a partner, at Analysys Mason

Perhaps more importantly, there are signs of demand for an integrated solution from customers, which can also benefit from a streamlined procurement process and fewer issues with getting devices to work. However, as this report discusses, the opportunity will have its challenges, chief among them being how module firms can transform themselves into connectivity providers. Module makers that are interested in providing integrated connectivity need to think about the model of delivery that best fits their requirements in terms of risk, speed of deployment and level of control. ▶

Figure 1: Percentage of total cellular IoT value chain revenue by revenue component, worldwide, 2030



Source: Analysys Mason

Selling connectivity provides an opportunity for module makers to increase their addressable revenue

The IoT revenue opportunity is sizable (**Figure 1**): Analysys Mason's IoT forecast predicts the total value chain revenue worldwide from cellular IoT will increase from US$150 billion in 2022 to US$250 billion in 2030. Hardware will account for almost 30% of this revenue by 2030 but will grow at a CAGR of just 2% between 2022 and 2030. Connectivity will account for a lower share of the total revenue (9% in 2030) but will grow at a quicker rate than hardware (CAGR of 7%). The growth in connectivity revenue will be driven by strong growth in the automotive sector and deployments in sectors such as utilities, smart buildings and smart cities.

Most module makers have been reluctant to sell IoT connectivity and those that have, have had mixed results. Connectivity offers need to meet complex requirements. These include licensing and regulation, wholesale and roaming relationships, logistics for the SIM and subscription management, supporting their customers, adhering to data privacy acts and ensuring uniform performance globally. Some module makers may consider these requirements to be too far outside their areas of expertise.

However, as SIMs become smaller and the industry steadily moves towards embedded and integrated SIMs (eSIMs and iSIMs), connectivity will start to be integrated earlier in the IoT value chain. The introduction of eSIMs and iSIMs may lead module makers to reconsider the case for selling integrated connectivity, despite the concerns they may have about lacking expertise. The options to gain this expertise are outlined later in this report. ▶

Bundling connectivity and hardware together helps the module maker to have a more direct relationship with their OEM customers

Integrated connectivity could lead to better outcomes for module makers and end users

Module makers that integrate connectivity into their hardware products could benefit in the following ways.

- **Recurring revenue.** Selling modules typically generates one-off revenue. This can lead to swings in revenue from one quarter to another, or one year to another, depending on when modules are delivered. Selling connectivity adds a new source of revenue and one that is recurring. Connectivity contracts can be several years in length, providing a steady and reliable source of revenue that could improve the balance sheet of the module maker. Investors can be reassured by recurring revenue and may reward the firm with a higher valuation.

- **Greater stickiness.** Bundling connectivity and hardware together helps the module maker to have a more direct relationship with their OEM customers. The OEM customer has a streamlined relationship, dealing with one supplier rather than separate ones for hardware and connectivity: the efficiency gains from this may lead the customer to be more willing to stick with the module maker.

- **Options to provide other services.** Module makers may want to eventually provide other features linked to a subscription service, such as security. Connectivity would be a logical place to start and develop this business model for module makers, which they can then build on with other services.

Device manufacturers could also realise the following benefits from having integrated connectivity.

- **Recurring revenue.** OEMs can also benefit from new recurring revenues. With connectivity integrated with the hardware, the OEM can add the application component and offer an end-to-end solution. For instance, a tracker manufacturer could build a cloud-based application that controls and manages the fleet of tracked assets, with the ability to see the assets' location in real-time and apply geo-fencing and other rules. ▶

Module makers have been reluctant to offer connectivity because providing connectivity requires knowledge of several areas that are unfamiliar to module makers

- **Simpler procurement process.** The OEM can buy hardware and connectivity together without having to go through a separate procurement process for connectivity. This is particularly helpful if the connectivity provider can provide connectivity in multiple countries. The customer can go from having to deal with multiple connectivity contracts, plus procurement of modules, to having one contract for everything. This could reduce the total cost of ownership for the end customer.

- **One point of contact.** The OEM knows exactly who to go to if there are problems with the device. If there is an issue with the device or connectivity, the OEM knows exactly who to go to resolve it, avoiding cases where the customer has to go through two (or more) parties who may blame each other for being the cause of the problem.

- **Simplified logistics.** Logistics are made easier for the customer if the module is shipped to them with the SIM included and pre-connected. A single stock-keeping unit (SKU) provides an immediate cost saving to OEMs (in terms of logistics, storage, multiple part numbers, inventory management and so on).

- **Fewer connectivity and device issues.** If connectivity and hardware are integrated early in the value chain, it is likely that problems with the device – such as device provisioning or applying the correct configuration and network selection – will be reduced. The module vendor can ensure that connectivity works on all of its devices before they are shipped to the customer, rather than the customer trying to solve any problems later on in the process. An issue with a tiny proportion of the devices deployed, but which results in needing manual intervention for those faulty devices, can make the business case for the entire deployment void.

Module makers have several options for how to offer connectivity, each with pros and cons

Module makers have been reluctant to offer connectivity because providing connectivity requires knowledge of several areas that are unfamiliar to module makers. These areas include licensing, regulation, inventory management, billing, and sales and marketing. Module makers have a few options for gaining expertise in these areas (Figure 2). ▶

Figure 2: Options for module makers to gain capabilities to provide connectivity

	Build an MVNO organically	Buy an MVNO	Outsource to a partner
positives	Complete control	Quicker than building organically	Quck, simple process
positives	MVNO can be designed around needs of the business	More control than outsourcing to a partner	Keeps options open to later build/buy an MVNO
positives	Less risky than acquiring	Lots of MVNOs present in the market with necessary expertise	Less risk
negatives	Slow and complex	Expensive	Less control
negatives	Expensive	Entering a new, unfamiliar market	Less revenue accured
negatives	Entering a new, unfamiliar market	Risks with acquisitions (e.g. staff, platform integration)	Risk of choosing the wrong partner

Source: Analysys Mason

The option selected by the module vendor will depend on their priorities and appetite for risk. An acquisition is the riskiest option, because any acquisition comes with hazards such as integrating one company's systems with another's and retaining staff. Acquisitions have the advantage of being quicker than building organically and allow the module maker to gain expertise from the acquired firm rather than having to develop it itself. Building an MVNO is less risky than acquiring, and provides complete control, but is a slow, complex and potentially expensive process.

Outsourcing to a partner is the cheapest and least-risky option. The partner manages the connectivity aspects on behalf of the module maker. Connectivity partners can offer a single SKU to solve the inventory and logistics issues that are associated with connectivity and can provide support with meeting licensing and regulatory requirements. A partner can also handle aspects such as billing, sales and marketing on behalf of the module maker, if required. In addition, partnering does not block the option of buying or building an MVNO at a later date. The partnership model can be used as a first step to test the opportunity. However, outsourcing comes with the downsides of the module vendor having less control and having to share a proportion of revenue accrued.

If module makers are serious about providing integrated connectivity, they should consider the following:

- To enable integrated connectivity, the module maker should study the option of working alongside a global connectivity professional that will take full responsibility for all aspects of connectivity. The module maker will not have to deal with elements of connectivity that it is unfamiliar with directly but can still enjoy the benefits in terms of new revenue and customer stickiness.
- The ability to provide a single SKU is vital. Many connectivity providers rely on multiple SKUs (i.e. providing a different type of SIM for different countries/regions). Being able to provide a true single SKU will help to simplify logistics, inventory and cost issues.
- Any connectivity partner/acquisition target must be a well-established one, with proven experience and a global presence to give the module maker credibility. The partner must have credentials in enabling global connectivity and understand emerging technologies such as embedded universal integrated circuit card (eUICC) and iSIM. Financial stability is also an ▶

It is important to be flexible enough to support the ever-changing needs of the IoT ecosystem, such as flexible network configurations and business models

important trait to look for in a partner to ensure any relationship will be long-term.

- Customer service is critical when providing global connectivity for IoT. Module makers are unlikely to be able to offer the same depth of customer service relating to connectivity, compared to MNOs and MVNOs, so partnering or acquiring a connectivity provider that prioritises customer service is essential.
- It is important to be flexible enough to support the ever-changing needs of the IoT ecosystem, such as flexible network configurations and business models. This is a commitment that will provide challenges to a module maker if it seeks to go it alone. A provider which owns its own technology will have the means to support the module maker as requirements evolve.

The ever-changing IoT market provides an opportunity to approach connectivity in a different way

The adoption of eSIMs and iSIMs will change the IoT value chain, with connectivity being integrated much earlier in the process and the ability to off a single SKU becoming increasingly important. Chipset providers, SIM vendors and module makers must adapt to the new value chain and figure out the best way to maximise their roles.

This brings opportunities to think about connectivity in a different way to the status quo. IoT remains relatively immature and much more work is required to optimise the IoT experience for the end customer. IoT has failed to grow as quickly as previously expected, in part because it is overly complex (and therefore expensive). New business models and experimentation with integrating connectivity comes with risks, but could make IoT simpler and help the market to realise its potential.

Bermad adopts floLIVE's unique SIM technology with a single SKU for worldwide IoT coverage

Bermad is a world leader in water and flow management solutions. The company was established in 1965, so has more than 50 years of experience creating best-of-breed solutions that have been utilised worldwide. Looking for greater control over its own digital roadmap and the products within, Bermad launched its own product line of irrigation controllers, called Omega and was looking for a one-stop-shop solution for global IoT connectivity.

As a result of its global coverage, transparent and competitive pricing anywhere in the world, and a smart single stock-keeping unit (SKU) SIM solution, floLIVE checked all the boxes. Bermad can now attain cellular connectivity anywhere, and has achieved true business growth in IoT

Business impact of floLIVE

- A digital offering that's fully under its own control
- Coverage in 86 countries worldwide
- Single contract and bill for all global services
- Full visibility for expedited fault-resolution
- Attractive rates for customer data packages

"We wanted a product that was the most plug and play as possible"

Bermad launched a line of irrigation controllers with built-in data logging, based on narrowband-IoT (NB-IoT) cellular communications. As a global company with more than 86 countries to serve worldwide and subsidiaries around the globe, Bermad needed:

Transparent and stable costs: While the company could look to reduce the costs of communications to the cloud internally, the cost of data needed to be as low as possible, especially as the product would serve many countries and need to offer good return on investment (ROI) as a whole.

A single provider: Bermad couldn't afford to look for a tailor-made solution for each and every location, with a presence needed in countries from Israel and Spain, to Guatemala, China, India, New Zealand, the US and more.

Compliant connectivity: Each destination may have its own unique compliance regulations, roaming restrictions, or laws around data privacy. Bermad needed a solution that worked everywhere, without needing to worry about these details.

Worldwide cellular connectivity via a single SIM

"We wanted a product that was the most plug and play as possible," says Lior Doron, the digital solution manager at Bermad. "I can check locally in the lab headquarters all of my connectivity, and then send it worldwide, whether to India, China, Brazil or another country, and I know that it works. In the past I would have had to make time and resources for trials in the field, and this is no longer a consideration. This is a huge operational advantage - one SKU and global reach."

After testing floLIVE's solution against a competitor, Bermad chose floLIVE's global connectivity solution as the right choice for its first IoT product. floLIVE offered a unique ▶

alternative to multiple local connectivity providers in each region – one SIM card with a single SKU.

Until the device is set up, it will remain location and operator-agnostic. Once the device is active, it then connects to the right local network from floLIVE's international mobile subscriber identification (IMSI) library, the largest of its kind. Using floLIVE's unique SIM technology, the SIMs could be provisioned remotely over-the-air (OTA) giving Bermad ultimate control over its devices, anywhere in the world. This sidesteps issues such as compliance of local data internationally, or permanent roaming, as the device is always using local connectivity.

Reduced overhead and complexity

"With floLIVE, we feel that we've found a real partner in our IoT growth," adds Doron. "floLIVE has given us its own unique expertise and industry knowledge, and it never fails to provide active help and proactive guidance to support us when we need."

Benefits include:
Full control: Bermad regularly manufactures devices without knowing where the end destination will be. With floLIVE, this doesn't matter, as devices can be activated, provisioned and maintained OTA.

Flexibility: Bermad has a stock of floLIVE SIM cards, and can test locally, plus decide when to activate, deactivate and control them worldwide. With local SIMs, Bermad would have to go without testing altogether, opening up to risk. Logistically, this gives ultimate control.

Global coverage: With floLIVE's huge and growing IMSI library, Bermad can provision and manage devices with great performance, anywhere in the world with cellular connectivity.

Data visibility: It's easy to visualise the amount of data that is transferred through the SIM card, and get all the information related to connectivity and coverage at a glance from a single screen, making it much easier to troubleshoot remotely.

Reduced overhead: Managing a single partner relationship is far easier and comes with reduced costs and fault resolution times over trying to create relationships in multiple locations or for every stage of the solution.

Minimised complexity: A single partner allows for ease of use such as one bill at the end of each month, one contact to reach out to in case of issues, and even one time zone, language and culture.

A smart economic solution: Bermad's customers can benefit from economies of scale, receiving a more attractive rate for data packages, and passing on those benefits alongside reduced service costs to their own customers.

"With floLIVE, we feel that we've found a real partner in our IoT growth"

www.flolive.net

The ones we're watching for hyperscale IoT connectivity

The IoT Now team has created a new feature in which we select ones to watch from companies active in a specific sector of IoT. Our Ones to Watch are selected based on introduction of innovative new services or products, market progress and even because we have concerns about their strategies. This issue, our attention has turned to IoT connectivity and the companies in this article are those we believe are worth watching in the third and fourth quarters of 2023

Simplification of access to and management of IoT connectivity is a dynamic that has matured substantially during 2023

IoT Now Ones to Watch is not a ranking but a recognition of companies that we identify as poised to make significant progress, those working to transform IoT and those we see driving commercial traction. We hope you find our selections interesting and we look forward to continuing to track the entire IoT market place.

Simplification of access to and management of IoT connectivity is a dynamic that has matured substantially during 2023. One company we've noticed continuing to put forward global IoT connectivity is **Eseye**. The company's AnyNet+ embedded SIM (eSIM) offering coupled with its Infinity IoT platform is enabling IoT organisations to access optimal IoT connections without having to change SIM card. The promise of global IoT products with a single stock-keeping unit (SKU) is similarly enabled and made real with the company's global IoT SIMs which can access more than 700 networks in over 190 countries, covering remote and underground locations in addition.

We believe this type of service removes one of the most significant barriers facing global, mass-scale IoT deployments – the need to manage global connectivity from multiple providers and the now-dying need to install plastic SIMs at the point of deployment.

This connectivity simplification is also in evidence in the hyperlocal globalised connectivity offered by **floLIVE**. In this issue, you can read our cover interview in which **Qualcomm** explains why it is collaborating with the company in support of its Qualcomm Aware offering. In essence, floLIVE has built and continues to add to its network of operator partners which combines to ensure ubiquitous connectivity can be made available to customers regardless of their location. Customers have one throat to choke and the complexity of managing a raft of providers is abstracted away from the customer organisation.

This enables the productisation of IoT on a global scale. We never believed that IoT organisations wanted to become connectivity experts and manage multiple carrier relationships so seeing the ability to embed connectivity into IoT devices that floLIVE, Eseye and others offer is a significant shift in mindset and capability for the industry.

The growing pains of IoT are having impacts on the connectivity sector in 2023. We have seen divestments of IoT businesses by **Twilio** and **Ericsson**, suggesting that larger parent companies see the fruits of IoT labours either being too distant or too expensive to compete for. The Twilio deal was relatively straightforward, seeing the divestment of its IoT business unit to **KORE Wireless** in return for around 11.5% of KORE in shares. This means Twilio still has skin in the IoT game but doesn't have to scale up its IoT unit to compete. On the flipside, KORE gains Twilio's IoT personnel – always in short supply – and its customer base.

We're interested and keeping a watching brief because KORE has announced its intention to become an IoT hyperscaler following the deal. We see the need for IoT connectivity to be treated and marketed in the same way as cloud resources ▶

so we're keen to see what KORE does next. Will there be more acquisitions to create greater scale or does it feel it now has a big enough platform to move to the next phase of its hyperscale ambitions?

In contrast, the **Aeris** acquisition of Ericsson looks to be a typical minnow swallows whale story with Aeris taking on the liabilities of large swathes of Ericsson's IoT activities including Ericsson IoT Accelerator. The big impact of this move in our view was the decision by Ericsson to back out of this part of IoT. Again, the rewards may look to be too distant or too small to justify continued investment and competition but Aeris evidently saw assuming the assets as a means to springboard its scale significantly.

This is not to discount Aeris' previously substantial IoT connectivity business but the IoT Now team has concerns regarding whether the company will be able to digest the Ericsson assets and combine both companies' strengths. The reason we're watching closely is so we can see whether Aeris can create compelling new products to serve mass-scale IoT that bring along Ericsson's customers alongside its own base.

Others have been growing through a series of more manageable acquisitions. **Wireless Logic**, for example, has acquired Singapore-based **Blu Wireless** and enterprise mobility, automotive and logistics MVNO **Webbing**. Typically acquisitive, Wireless Logic is pursuing growth with deals that expand its global footprint and its customer base in specific verticals. We find this interesting and therefore select the company as one to watch because we're keen to see how the acquisitions enable sector-specific global connectivity offerings to be created and sold.

That dynamic of consolidation alongside hyperscale preparation explains why IoT connectivity has given us plenty to look out for. A restructure of the IoT business at **Vodafone** has been reported and we foresee various mobile network operators changing or at least refining their approaches to the market to reflect changed needs and the arrival of embedded and integrated SIMs. These decouple operators' traditional SIM ownership from access to connectivity but this doesn't have to be a threat.

SIM innovations mean that operators, the connectivity providers mentioned earlier and potentially adjacent vendors such as IoT module providers are well-placed to position themselves as providers of IoT solutions or products that contain embedded connectivity. We have been waiting for the complexity of procuring IoT connectivity at scale and globally to be simplified and the first signs of this are now apparent.

Departure from the market by some large players has not left a vacuum to be filled, partly because device volumes are growing so rapidly but this does present an opportunity for aligned vendors to bring forward new propositions. This is why Aeris, Eseye, floLIVE, KORE Wireless, Vodafone and Wireless Logic are our inaugural IoT Now Ones to Watch for IoT connectivity.

The Aeris acquisition of Ericsson looks to be a typical minnow swallows whale story with Aeris taking on the liabilities of large swathes of Ericsson's IoT activities

Three top tips for IoT security

Companies designing and launching technology-based solutions must make security a priority, writes Simon Trend, the managing director of group services at Wireless Logic. The common perception is that IoT systems are complex and have enlarged attack surfaces because they include remote devices from different vendors. While there is some truth in that, it's important to remember that 74% of breaches involve a human element.* Cyberattacks will target weak links in the chain, and these could just as easily be in business processes or inadequate training as they could be in hardware or software systems

According to a report by SonicWall there were 57 million IoT malware attacks in the first half of 2022, an increase of 77%

IoT cybersecurity is gaining more attention, so we can expect legislation to increase in size and scope. Companies should prepare by adopting a 360-degree security approach, designing their solutions to defend, detect and react to incidents over the lifetime of devices. They must also rehearse their security measures, practising scenarios so they are in the best possible position should they have to put plans into action. For these reasons, these are my top three tips for IoT security:

1. Take a 360-degree security approach

According to a report by **SonicWall** there were 57 million IoT malware attacks in the first half of 2022, an increase of 77%. The security threat to the IoT is therefore very real, yet **Kaspersky** reports that 43% of businesses don't fully protect their IoT solutions. Over a third (35%) refer to a lack of staff or specific IoT security expertise and 40% cite difficulty in finding a suitable solution. Companies must protect their implementations by taking a holistic approach to IoT security that defends, whilst also detecting and reacting to breaches, should they occur. Security must be end-to-end and encompass processes and people as well as technology.

Defending an IoT solution means managing the cyberattack surface to prevent unauthorised access to devices, cloud infrastructure or data. If 360-degree security were to be viewed as a pie chart, defence measures would occupy the largest slice. Those measures encompass IoT SAFE, a SIM standard to uniquely identify devices for mutual authentication between devices and applications.

SPONSORED ARTICLE

Simon Trend
Wireless Logic

Defence also includes secure communication, resilience against outages, software updates, data security policies and compliance with market and industry regulations.

Astonishingly, it takes an average 212 days to detect a data breach, according to an IBM Security/Ponemon Institute report. To detect any anomalous activity or behaviour that could indicate a breach, such as a change in target URLs or data usage, companies must monitor their devices and analyse network traffic. Analytic capabilities, put in place at the solution design stage, ensure actionable insights in life.

Despite this, it is still essential that businesses prepare to react swiftly and comprehensively in the face of a security incident. Automated countermeasures can isolate security threats by, for example, quarantining and cleaning affected devices. Reactive measures also include reporting breaches and anomalies and applying corrective actions across systems.

2. Rehearse IoT security

Rehearsal is a critical weapon in the fight against data breaches and cyberattacks. It helps companies identify any weak points in the chain of security, plug gaps and react quickly should they have to put rehearsed plans into action.

There are a range of tools and methods to help. Digital twins, for example, through platforms such as **IoThink.com** can act as virtual representations of devices or processes and be used to model security threats. Simulations provide an ideal way of rehearsing firmware updates, revealing any false flags to address before go-live.

A range of companies offer workshops to rehearse 'what if?' scenarios specific to organisations and their IoT solutions, walking through all the steps needed to deal with such scenarios and providing valuable actionable insights along the way.

Companies must also prepare for potential ransomware attacks. These are increasingly common and can have devastating impact. Consider, ahead of time, the strategy and rehearse the reaction. There are decisions to be made, including around insurance, noting that this may cover only a ransom itself, not additional costs, such as those incurred resolving the issue, and losses to revenue and reputation.

3. Prepare for legislation

Device manufacturers and solutions providers must be aware of security legislation relevant to IoT and act to ensure compliance. They need an in depth understanding of the legislative landscape, particularly as IoT deployments are often international, global even.

It is likely they will need to take account of a range of existing and pending legislation, including the UK's Product Security and Telecommunications Infrastructure (PSTI) Act, the EU's Cyber Resilience Act, and the USA's IoT Cybersecurity Improvement Act (for devices used by federal government).

The PSTI (Product Security) regime is on the immediate horizon to regulate connected consumer products such as routers, webcams and connected fridges. It comes into effect on 29 April 2024 from when impacted products must be free of default passwords, have a vulnerability disclosure policy and be transparent about update support periods.

Internationally, legislation will vary from region to region, however existing industry standards offer a benchmark to help companies prepare. These include ETSI EN 303 645, IEC 62443 4-2 and ISO/SAE 21434. IoT solution designers can take a lead from these standards to meet cybersecurity challenges by, for example, allocating unique device identities, keeping security credentials private, authenticating devices on networks, keeping software up to date, reporting anomalies and threats, and quarantining affected devices.

The considerable damage a cybersecurity breach can do is, of course, more than sufficient motivation to make IoT solutions secure by design. The message therefore is don't wait, act now. The countdown to consumer legislation may be on already but even in the corporate space, tendering and procurement processes are likely to demand, if they don't already, certain cybersecurity maxims.

Fortunately, help is at hand for companies as they navigate the legislative landscape. Connected device security consultants **Copper Horse** manage an IoT security mapping site, this maps the different requirements and emerging standards.

IoT solutions that are secure, rehearsed and meet legislative requirements

IoT security and compliance cannot be an afterthought for device manufacturers and solutions providers. The only way to protect deployments is to build comprehensive defence, detection and reaction measures into solutions. Existing standards provide useful benchmarks to assess security measures against but, having designed with security and compliance in mind, companies must also rehearse and feed insights back into development cycles for continuous security improvement.

*Source https://www.verizon.com/business/resources/reports/dbir/

www.wirelesslogic.com

IoT verticals need specific capabilities, the market's not horizontal anymore

With volumes starting to take-off in everything from electric cars to healthcare, the IoT conversation has moved on from future-gazing into real, commercial-scale deployments, with the frequency of new launches increasing. Key enablers of the move to the mainstream are ubiquitous connectivity enabled by embedded SIMs (eSIM), Onur Kasaba, the director of sales at Tele2 IoT, tells Matt Hatton, the founding partner of Transforma Insights

Onur Kasaba
Tele2IoT

MH: How do you see the IoT market at the moment? What have been some of the interesting trends you've witnessed?

OK: The IoT market is a very interesting one. Since I've been involved, back when it was machine-to-machine and data collection, everyone was always saying that it was on the verge of explosion. There were a lot of 3-5 year predictions of billions of devices, which never happened. We're more realistic at Tele2 IoT and believe in taking the market one step at a time. We're quite happy with how IoT is growing, and in our humble opinion it's growing quite quickly, with a few areas growing particularly fast, such as healthcare.

Healthcare continues to be more and more connected. In healthcare, IoT is an essential tool, not an add on. With aging populations we're already seeing that in-home care is increasingly important. Most governments are facing care-giver shortages, making taking care of patients, who often have comorbidities while remaining in their homes, challenging. Care for the elderly and

SPONSORED INTERVIEW

most vulnerable is crucial and in demand and we are already there in terms of delivering it.

Another big one is electric vehicle (EV) charging. The EV revolution is picking up. Regulatory bodies are pushing for evolution in the charging infrastructure. That's the biggest challenge. We're seeing ambitious plans in most countries. And we shouldn't forget private EV charging, which is also increasingly important. Many entrepreneurs are seeing an opportunity there.

And closely related to EV is the automotive sector. With the EV revolution it becomes much easier to build cars. It looks more and more like the mobile phone industry. You just need to optimise the synchronisation of electric motors. Because it's much simpler than internal combustion cars, the automotive landscape is changing. Before, we at Tele2 IoT were getting tenders from the usual car maker suspects in Italy, Germany and beyond. Everyone was trying to get a piece of that business. Today, there are a lot more EV car makers, so it's easier for suppliers to get a piece of it, hence why Tele2 IoT is getting more involved.

MH: We're coming up on a year with Tele2 IoT pushing strongly into the European market. How are things going?

OK: At Tele2 IoT, we have hired local resources in France, Italy, Germany and Spain, and we continue to expand. We think the market still has untapped potential, particularly in Southern Europe. There are more IoT devices there than in Northern Europe because of big adoption of applications like insurance telematics and track and trace, and there are quite a few established players in this area. This has pushed Tele2 IoT to understand the developer needs of those regions for the use of new technology. We want to be the thought leader in that area. There are some strong incumbents, but not necessarily in the newer IoT technologies.

Our core ambition is to democratise IoT. We have fearlessly enabled embedded universal integrated circuit cards and embedded SIM (eUICC/eSIM) capabilities, which are a key tool for doing this. We're not worried about customers leaving us. Our focus is on delivering improved services such that customers won't even think about it. Combine eUICC/eSIM with the needs that we see in Southern Europe, and it works very well. In our experience, the DNA of a Nordic business culture fits well with Southern Europe, particularly in terms of the transparency of our offering.

MH: Why do you think eUICC/eSIM has resonated so well?

OK: Customers can avoid the lock-in effect with eUICC. The result is that they no longer need to do quite the amount of due diligence that they previously had to, because they have the ability to switch. The result is that with eUICC, customer acquisition is easier because they have the peace of mind to switch if needed. It's very transparent in the customer contract that they are allowed to leave if they want. ▶

We're super happy with how things are going with Control Center. It's enabling different tiers for different use cases and industries, which has been very useful

MH: In terms of new technology, is it just eUICC?

OK: We've also seen success with new products in the security area in partnership with **Cisco** and **Equinix**. Cisco IoT Control Center as a platform is well ahead of the competition. It has always had the most comprehensive set of features among connectivity management platforms (CMPs). And it has been flexible in adapting its roadmap to the needs of Tele2 IoT.

We're super happy with how things are going with Control Center. It's enabling different tiers for different use cases and industries, which has been very useful. There's always been the question in every provider's head: should I stick with just one CMP or use several? But Cisco is delivering well, and our partnership is doing well. This has been true particularly in terms of security features, analytics, and anomaly detection. It's not so easy for others to develop it.

Cloud Interconnect is a product that has attracted a lot of interest. End-to-end IoT security is typically handled by VPNs and APNs. But VPN is a cumbersome approach. And the likes of **Amazon Web Services** keep changing parameters for delivering data into the cloud. So we created Cloud Interconnect, together with our partner Equinix, providing a simple integration to deliver data securely into the cloud without touching the internet.

If we couple the new growth sectors with the new technology the result is very good. When society decides to invest in new technology it wants to do everything fresh. For instance for electric vehicles, it's to create something from scratch using all the newly available technologies. And it makes life much easier, deploying more secure and scalable technologies, which they can do with Tele2 IoT as long as they use one of top 30 cloud vendors.

MH: What about on-prem?

OK: We also have an on-prem version for private interconnect. We can bring a fibre connection to their premises, and we have several clients doing that already.

MH: Have there been any surprises or unexpected developments that have helped you steer your course or adjust it?

OK: We've been investing in automotive, as I mentioned, but the main surprise was that it is the smaller car makers who are selling more, such as **MG**. That's quite surprising for IoT and for all society. Maybe the big car manufacturers will have problems competing.

Verticals are becoming real verticals. It used to be that one IoT solution was provided to everyone. But now it needs more customisation. For instance, the reliability needs of agriculture and healthcare are not the same. They used to be much the same but demands of different sectors have evolved differently. Automotive might demand more security, with cybersecurity protection. But it will be less critical in other sectors. Also, the hardware requirements are different for each one. Utilities for instance require more specialisation.

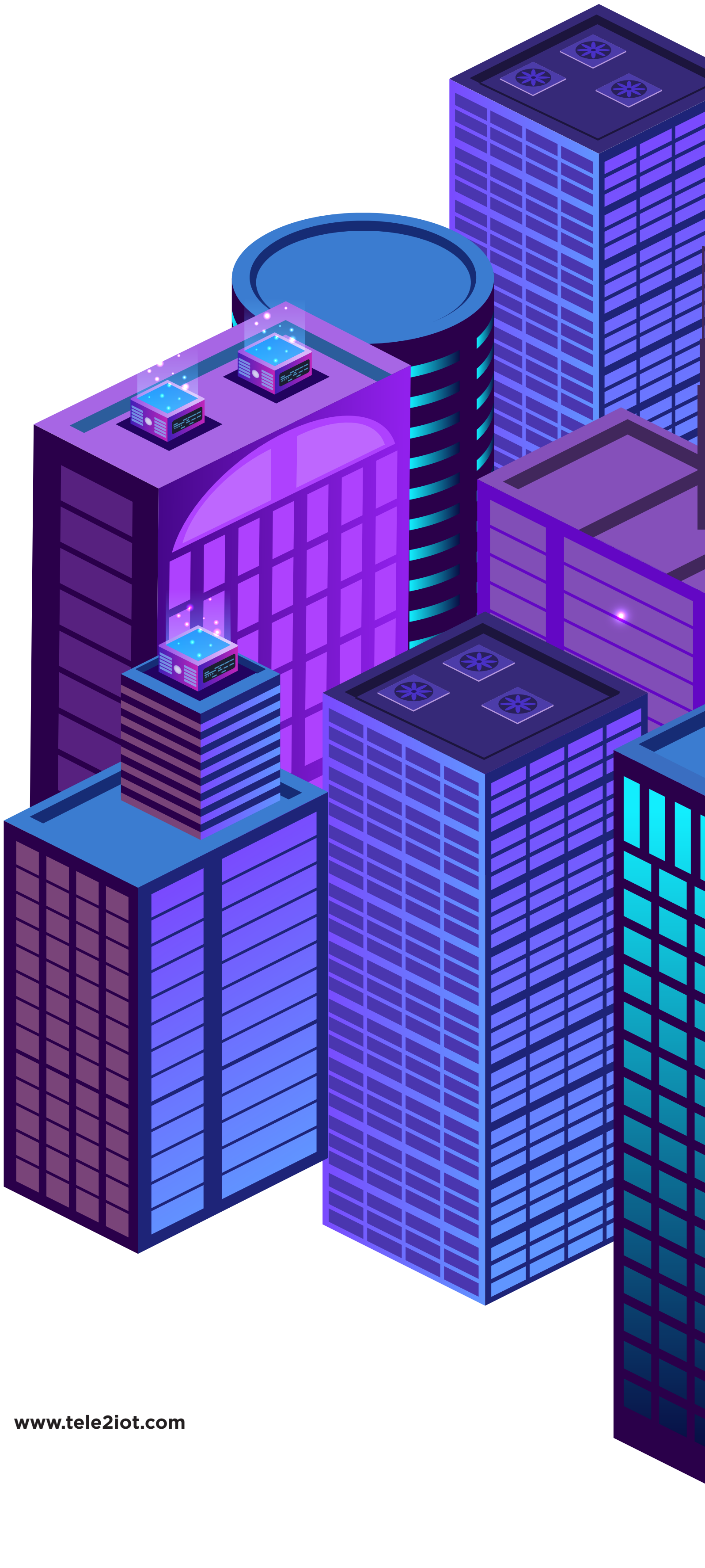
It's not just about knowing the sector, it's also about providing the technology that's more relevant, and building up more competence there. It's critical to be able to differentiate, for instance, in terms of reliability.

MH: Any other areas where you have seen some development?

OK: Apart from the ones I've already mentioned, aviation is becoming more and more important, as well as maritime.

In aviation we see aircraft doing more in terms of collecting and offloading data. It's becoming mandatory to drop data when you land. This has led to the emergence of a strong need for connectivity. So, we're seeing a surge in interest from aviation companies. It used to be that we would see enquiries once every five years, but now it's several per quarter. And then there are also demands in adjacent areas such as luggage and on-site tracking. This expands the opportunity into a bigger initiative, involving mobile private networks (MPN), probably 5G, for airports, for accurate indoor and outdoor location. Tele2 IoT is getting into this in home markets. But MPN is new, and there's a lag in adoption. ▶

Sustainability is probably the number one topic in the house at Tele2, not just IoT but driven by the group leadership



Looking briefly at maritime, we work with customers across the spectrum, meaning everything from sleek luxury electric speedboats to autonomous public electric ferries powered by 5G and IoT to cargo vessels reducing fuel consumption and optimising routes. It's an area that is diversified and growing.

Also, the emergence of **Starlink** is very relevant to the aviation and maritime sectors. It's an enabler rather than a competitor and is changing the game a little bit. Its emergence as important in IoT has also been surprising. Tele2 IoT is certainly looking at collaborating with satellite operators.

MH: What about sustainability – Tele2 is number one on the Financial Times' Climate Leaders 2023, and Transforma Insights noted in our CSP IoT Peer Benchmarking Report that Tele2 has a company-wide vision to lead on sustainability – why is this important and how does the IoT unit contribute?

OK: Sustainability is probably the number one topic in the house at Tele2, not just IoT but driven by the group leadership. We're trying to be most sustainable company. It's nice to work in a company striving to be the best. By now we don't really need to touch on the need for sustainability, but we should emphasise how IoT in particular is a catalyst for enabling sustainability. At Tele2 we know the carbon emissions that our own business creates, and we have done a lot of work to minimise them. For instance by reducing the SIM size by half. But it's also about how IoT is being used to manage resources.

For instance, we see wars driving food shortages and the need for more effective supply chains. Who would have thought a war in Ukraine would affect a child in Uganda? It shows how integrated we are. The dream for us is to connect food production. Historically the economics of it weren't there, but the emergence of more cost-effective technologies, and the growing criticality of supply chains, has resulted in a spike in interest. Again, as with aviation, if we had one agriculture lead per year a few years ago, now it's several per month. The economic viability of using IoT is growing, as is the use of other technologies, such as machine learning.

From securing delivery of foodstuffs through to producing more food using new scientific methodologies, the use of technology is growing. We've noted that the Netherlands is particularly good at the latter. There's a reason why it's the second biggest food exporter in the world, and it's down to technology.

www.tele2iot.com

SMART CITIES SECTION SPONSOR:

libelium

Holistic, data-fueled, IoT-enabled capabilities drive smart cities beyond their challenges

Alicia Asin Perez is the chief executive of Libelium, which provides an IoT platform that incorporates sensors to monitor various metrics from air quality to noise and moisture and then delivers real-time smart applications to enable positive outcomes. In smart cities, this could involve using navigation systems to reduce emissions from private vehicles and promoting public or shared transport or, for example, using geographic information systems (GIS) to identify and control highly-polluted areas. Here, she tells George Malim, the managing editor of IoT Now, how smart city initiatives are maturing to adopt a more holistic approach in which data from multiple sources can be combined to deliver significant improvements for citizens

George Malim: IoT is powering changes across society but there are substantial challenges to overcome as projects scale up. Libelium describes its mission as 'behind the change, beyond the challenge'. How does this inform your vision of the future?

Alicia Asin Perez: We defined our 'behind the change, beyond the challenge' direction a year ago because we consider that IoT is a revolutionary technology that has changed our society a lot. We have the potential now to collect and monitor data on lots of things that we couldn't do before and this puts us in a strong position behind the change. We can, for example, monitor water consumption, how much pollution is in a city, how many cars come in and out and how much parking there is. IoT has enabled monitoring of all of these things and combined this can create significant advances in sustainability and improved citizen quality of life.

When it comes to taking IoT beyond the challenge that it faces today, there is plenty of work to do. We know what's possible and what can be done with technology but, so what? Talking about technology is easy but it's dreaming, it's technology for the sake of technology. Going beyond the challenge means taking technology and ensuring it enables sustainability.

When it comes to taking IoT beyond the challenge that it faces today, there is plenty of work to do

This important in our own business. We don't want to impact climate change by creating large volumes of additional devices or increasing power consumption that's not offset by the benefits we enable so we help customers by going beyond simply monitoring smart cities to enable rich insights and positive outcomes. ▶

SPONSORED INTERVIEW

SMART CITIES SECTION SPONSOR:

libelium

Alicia Asin Perez
Libelium

We help customers move on from just monitoring metrics such as pollution levels to using data to achieve real goals, such as a reduction in particulates, for example

GM: One example in which smart cities are delivering proven benefits to citizens is in initiatives to improve air quality. How has Libelium worked in this area and what technologies are being deployed to reduce CO2 and other emissions in cities and companies?

AAP: We help customers move on from just monitoring metrics such as pollution levels to using data to achieve real goals, such as a reduction in particulates, for example. In Saudi Arabia at the Saudi government's new NEOM smart city, we're helping to monitor pollution levels. This is how we're behind the change as we monitor pollution levels and combine that with other data such as traffic flows, weather information and much more. We apply artificial intelligence (AI) to combine data from multiple sources and this means we can support far richer data.

At NEOM, for example, we can define if air pollution is from desert sand that has blown into the city or from construction machinery that is generating pollution. There's not much we can do about the desert sand but the information can be used to minimise the risks for citizens. However, for construction machinery pollution or cargo ship pollution in the harbour, you can put policies in place and require operators to reduce their environmental impacts.

In Cartagena, a city in Spain, we've helped in the implementation of a low emissions zone (LEZ). This is a controversial topic because, although people want cleaner air they also struggle with the restrictions that LEZs impose being not very convenient for their lives. Thanks to Libelium's technology and our experiences elsewhere we have been able to advise the city on where the biggest problems and the greatest sources of pollutants are. This has enabled the least restrictive zone in the whole of Spain to be implemented.

The city has used data to tightly target the areas of most impact and reinforced public transport in areas where bigger capacity is needed because of reduced need to use cars. In addition, the city has used the data to identify where to introduce new green areas to improve the lives of citizens. In the past, projects like this were only about monitoring for one condition, such as CO2 levels but to achieve improved air quality is a much more complex problem. Particles in the air, for example, are even more problematic than percentage of gases so we take the whole picture now. In the early days of IoT, we'd have monitored levels of just one gas.

GM: How is the smart cities sector adopting AI in its daily operations? ▶

SMART CITIES SECTION SPONSOR:

libelium

GM: Real results are needed in order for companies and smart cities to demonstrate compliance with tightening regulations. Are you seeing IoT platforms being utilised to report directly to authorities for compliance purposes?

AAP: Yes, we are seeing this but not as much today as we will see in the very near future. In some cases there are environmental directives where cities can access specific funding if they demonstrate they have a problem with pollution. If they can't show the problem exists with real data, they can't get the funding but if they can show the scale of the issues they face, they have the right to ask the government for funding.

We're also seeing IoT platforms being utilised in the business-to-business arena. Companies are increasingly concerned about environmental, sustainability and governance (ESG) issues and their green credentials and reputation. By gathering data they can demonstrate that they are making improvements and doing this better than previously. This has the potential to go beyond greenwashing and deliver real results.

Most ESG rating companies are just putting out information based on forms being filled in and interviews with companies but, if you say you're reducing your CO2 emissions at your factory, you should be able to demonstrate that with real data. Similarly, if you're a chemicals company you should be able to show that you are emitting lower levels of water pollution year-on-year.

The technology behind this is robust and well-established. We think that in future IoT will power more rational ESG reporting and help put an end to greenwashing by replacing it with real metrics that show a company's performance.

AAP: One thing we're offering to cities is a map that presents a heatmap of pollution levels that can also forecast the evolution of the heatmap. This means cities can see what the future looks like if they do nothing. They can also understand what the impact of making an area traffic-free for one or two hours might be or they can model how to incentivise people to change their behaviour with free or reduced price public transport.

AI is a powerful tool for enabling simulation of multiple possibilities for the future and we see it as an important enabler of holistic smart city planning, operations and visions of the future.

GM: We're seeing data-driven decisions being taken to drive improved sustainability in cities but this isn't just about technology adoption. Ideologies and politics also swirl around smart city initiatives and can hamper progress. How can ideology and politics reconcile with the technology to enable maximised benefits to be achieved?

SMART CITIES SECTION SPONSOR:

libelium

AAP: I think smart cities are very, very immature in this sense. Unfortunately, we are not living in the golden age of our democracies and a lot of politics is now conducted on social networks with politicians elected on the basis of that activity. City mayors and managers should be less focused on ideology and give more attention to the operations of their cities. Key performance indicators should be used to monitor the performance of the city to provide real data to fight back against fake news.

It's easy to say in an election that the city is a mess and a change is needed but is it really? IoT is able to gather and present data that reveals what pollution levels were before the current administration, detail what action has been taken and what the results have been. These can be seen month-by-month so citizens can ask the questions of their leaders that drive progress.

If we implement and insist on data as part of our culture and educate people to ask about the data around every piece of news, we'd have a much better democracy.

GM: What is Libelium's role here and how do you help smart cities benefit citizens?

AAP: Libelium has been making a huge change over the years. We started as a hardware enabling company with the accuracy of sensors as our focus. Now that's not enough, we've become a solutions company with a specific focus on sustainability supported with AI and our data capabilities.

That enables us to provide cities with consulting and advice to address the huge problems they face. With the speed of advances in technology, I sometimes feel overwhelmed so I can imagine how every manager might feel. We can be the sherpa that helps them climb to the top.

We've been here for 17 years and that's unusual in the IoT sector. Our path of starting with data quality and making sure sensor data is truly accurate and data quality is not violated along the rest of value chain, means the data can be trusted and acted upon. Transforming cities relies on the raw materials that fuel decision-making and that's always about accurate data.

However, the data doesn't exist or create value in isolation. Interoperability in smart cities is essential. Ten years ago, cities were addressing smart city initiatives in siloes for activities such as air pollution, irrigation, transport but now the approach is to have the whole platform to digitalise all of the services of the city. That enriches the data set so, if the focus is on improving air quality, traffic data can contribute.

This allows a city to make more parking spaces available so fewer cars circulate looking for parking spaces and emitting CO_2. It's the same with irrigation, while Libelium is known for our air quality projects, we also work with water utilities and for a range of different issues. In Asia, for example, dust and particles are the biggest pollutants while in Europe, it's noise. We are replicating projects we've deployed to address air pollution for noise as well. In New York City, for example, we're piloting a noise monitoring project.

The trend though is towards adoption of a holistic approach that addresses multiple issues with a single technological foundation. In the city of Las Rosas, near Madrid in Spain, we have data on the return on investment the city has achieved. The project has seen a 32% reduction in supervision and maintenance activities, air pollution reduced by 14%, street noise reduced by 17% and operating cost and data integration costs reduced by 21% because of grouping all the services in the same software platform.

Those are compelling numbers that are attractive to city budgets but the real value is in the improved quality of life and improvements to the society they live in that citizens experience. This is why I am proud that Libelium is able to be behind the change and able to take our smart city customers beyond the challenges they face.

Libelium has been making a huge change over the years. We started as a hardware enabling company with the accuracy of sensors as our focus

www.libelium.com

SMART CITIES SECTION SPONSOR:

libelium

How to unlock the potential of smart cities

Smart cities present an exciting new arena in which the lives of citizens can be improved and the environmental impact of our lives can be minimised. Exclusively for IoT Now, Juniper Research has prepared a report that explores the smart cities arena

As part of its Sustainability & IoT Market Intelligence Centre, Juniper Research covers the smart cities market extensively. Over the last three decades, smart cities have evolved from an abstract concept to a technology-based and inclusive spatial concept; emphasising environmental considerations. The 'digital' element referring to the technology has now gained an underlying enabler role. As such, a smart city is a city that utilises technology and technological deployments to effectively meet inhabitants' needs, improve their experience, and engage them without compromising on basic considerations like data integrity and privacy protection. Therefore, an important element of smart cities is about efficient governance through empowerment of local administrators, who, in turn, are enabled to devise policies for enhancing citizens' quality of life. However, getting the most out of smart cities as a concept has proven tricky, with different cities taking different strategies. As such, there is no single path to building a successful smart city, with many different routes available.

Definitions and scope

Juniper Research defines a smart city as follows:

'A smart city is a place where traditional networks and services are made more efficient through the use of digital solutions for the benefit of its inhabitants and business. It means smarter urban transport networks, upgraded water supply and waste disposal facilities, and more efficient ways to light and heat buildings.'

This practical and goal-oriented view ultimately focuses on areas where industry applications can have visible contributions to both collective and individual lives, for instance, in regard to energy supply.

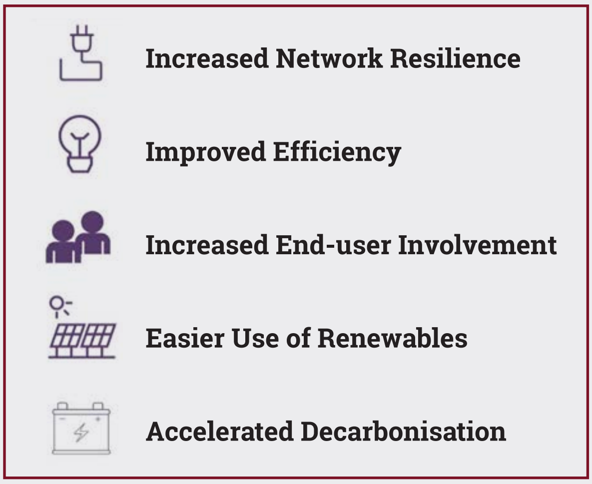
Components and segments of a smart city that allude to underlying technologies are numerous, stated as below.

- **Smart buildings:** Smart buildings refer to where buildings use information and communications technology-based systems, services and technology for optimisation of the facility's performance and operations to create a comfortable environment and improve sustainability. These systems and services often involve IoT devices and solutions, such as sensors, which are utilised to generate data to measure power and air quality, energy and resource consumption, as well as occupancy, and to predict maintenance needs to achieve efficiency. Collectively, they contribute to the lowering of energy and operational costs and enable inhabitants to make informed decisions about changes or improvements they may want to undertake for buildings their own consumption habits. Smart buildings differ from connected buildings, with the former referring to building operations connected to, and run, and/or managed by IT networks. On the other hand, smart buildings produce insights from the data collected, often enriched by artificial intelligence and machine learning (AI/ML), and feed them into platforms for responsive and highly configurable solutions.
- **Smart grid:** Smart grids can be broadly defined as an electricity supply network that uses digital communications technology to detect and react to local changes in usage, leveraging analytics and smart metering, and including elements such as microgeneration. Like smart buildings, smart grid leverages IoT and adapts to changing supply and demand patterns by ensuring communication throughout the value chain without overly relying on separate operators, as well as through data collection and analysis. It acts as an integrated management mechanism to coordinate demand and supply and oversee efficient and sustainable energy distribution. More importantly, since it is a foundational system, it lays the basis for the efficient functioning of all other smart city components, such as smart lighting, buildings and interrelated systems such as EV charging.
- **Smart lighting:** Smart lighting is one of the earliest applications of smart cities, where analytics and sensors are utilised to optimise how lighting is used; ▶

SMART CITIES SECTION SPONSOR:

libelium

Figure 1: Smart grid benefits
Source: Juniper Research



helping reduce emissions compared to traditional lighting systems. With the help of sensors, pedestrian traffic is monitored and adapted to traffic and control systems, which also allows remote diagnostics and visualisation. Smart lighting also has a role in ensuring public safety. Adoption of smart lighting technologies has also paved the way for the use of other sensors leveraging poles for uses in air quality monitoring and parking, Wi-Fi connectivity, EV charging, and more. In this sense, smart lighting is a precursor to smart city solutions employed.

- **Smart traffic management and parking:** These concepts involve the use of digital technologies to manage vehicular traffic for the purpose of driving efficiencies, reducing congestion, and/or minimising harmful emissions. Smart traffic management holds a great potential to reduce greenhouse gas (GHG) emissions by optimising the traffic flow, especially when complemented or supported by other mobility solutions such as congestion surcharges and carpooling/ride hailing. They also contribute to the prevention of accidents and improve road safety. Likewise, smart parking solutions aim to reduce fuel and time consumption caused by parking efforts and optimise these activities through data collected by parking management systems (PMS) that include sensor-based solutions.

- **MaaS:** Mobility as-a-Service (MaaS) is a type of service which enables users to plan, book, and pay for multiple types of urban mobility services through a joint digital channel. The channel is often a platform that collates different transport modes, as well as parking facilities to deliver the most efficient and seamless route to journeys. MaaS has gained in popularity within the last decade, thanks to increased adoption of local governments and transit authorities/agencies worldwide of the mobility platform solutions, to provide unified approaches to transport that encompasses products and services in interconnected industries such as digital ticketing and mobile payments. MaaS, concurrent to smart city developments, is an area that continues to grow and increasingly adapts alternative modes of transport such as ride sharing/carpooling.

Key trends and drivers

The key trends and drivers influencing the development of smart cities market are multi-fold; reflecting the component layers of deployments and objectives behind initiatives. These are explained in detail below.

Environmental concerns

Increasing environmental considerations and consciousness, and a move towards net zero have accelerated smart city developments in recent years. The driving force of environmental concerns is inevitably linked to decarbonisation/net zero goals, as well as the generation and use of renewable energy targets set by governments, international coalitions, and regulatory bodies. In terms of smart cities, these objectives are and continue to be mirrored most immediately and visibly in efforts to render transport and buildings carbon neutral, and many local authorities have made environmental objectives a strategic pillar for their smart city deployments.

At the international level, the Paris Agreement's tenets of carbon neutrality rest on the premise to limit global warming to 1.5°C. Therefore, GHG emissions must peak before 2025 at the latest and decline 43% by 2030. In order to achieve this goal, the parties to the agreement have adopted national policies and strategies for 2030; albeit with mixed success to date. Therefore, the COP27 cover decision in 2022 requests agreement parties to revisit and strengthen the 2030 targets in their countries, to align with the temperature goal by the end of 2023; taking into account different national circumstances. Other broader strategies involve climate neutrality and resilience with varying emphasis on facilitating measures such as the use of renewables in the energy mix, which is tied to smart grid deployments.

The European Union (EU) aims to be climate neutral by 2050, which was the objective at the heart of the European Green Deal Industrial Plan, in line with the pledges of the Paris Agreement. The European Commission (EC) has been paying particular attention to smart cities and enabling technologies by innovation partnerships and initiatives such as Smart Cities Marketplace, which consists of numerous communities and initiatives to help shape the market for smart cities in Europe. The Marketplace's cross-cutting operation areas include sustainable urban mobility, sustainable districts and built environment and integrated infrastructures, and processes in energy, information and communication technologies and transport. ▶

SMART CITIES SECTION SPONSOR:

libelium

Throughout Europe, all member states (with the exception of Poland) have also set their own initiatives; focusing on achieving net zero targets. For instance, Germany's Climate Action Plan 2050 stated the reduction of sector-specific emissions as part of the concept of Energiewende, 'Energy Transition'. This concept refers to the country's planned transition to a low-carbon economy, and in line with this broader transition, Germany has pledged to cover 65% of the energy consumption via renewables by 2030. This was further bolstered by the EEG (Renewables Energy Act) 2021 that set the new target for increased production and use of renewable energy. In April 2022, following the war on Ukraine, the Act set a new target of achieving 80% of renewable energy by 2030; entering into force on 1 July 2022. Germany's particular focus on renewables necessitates bolstered smart grid deployments, and will be an area to watch for future smart city applications in German cities.

The US government also aims for net-zero emissions by 2050. The Inflation Reduction Act proposes a US Green Deal which will channel US$370 million towards green energy projects. More importantly from the standpoint of smart cities, the Act provides funding to bolster urban sustainability, improve home energy efficiency, and mitigate pollution across the country; incentivising both state and city authorities to deploy carbon-neutrality initiatives. Therefore, the Act is expected to expedite deployment of smart city solutions, particularly in terms of transport and building improvements. For example, the Act aims to accelerate local pledges for decarbonisation of buildings by providing funds. This complements cities' own climate initiatives, such as Boston's new building performance standard, and Washington DC and Seattle's new building electrification codes that will phase out fossil fuels from buildings.

The UK government has a similar goal with its new Net Zero Strategy published in March 2023. In this document, previous net zero targets of carbon neutrality by 2050 are echoed; albeit with somewhat more tangible policy initiatives, around, for instance, Zero Emission Vehicle (ZEV) mandates. The ZEV mandate will support delivery of the phase out of the sale of new petrol and diesel cars and vans from 2030 and ensure that all new cars and vans are zero emissions at the tailpipe from 2035. This is aimed at driving adoption and deployment of ZEVs, as well as increasing investment in their manufacturing, supply chains, and enabling infrastructure. The strategy also includes propositions to reduce buildings emissions, which are responsible for around one third of GHG emissions across the country; mentioning the possible adoption of clean heat technologies such as heat pumps and incentives around boiler upgrades. Future Homes and Future Building Standards will also be drafted in 2023 and legislated in 2024, with both planned to be implemented in 2025. As such, an area for smart city deployment focus is transport, more specifically, ZEV-related solutions (including EV charging infrastructure) in the short term.

A global superpower and home to numerous well-documented smart cities in the world, China aims to transform its power generation mix towards 90% from renewable sources including nuclear power and achieve net-zero by 2060, as President Xi Jinping pledged in September 2020 and confirmed in March 2022. However, diverging from the aforementioned net zero targets, carbon neutrality only covers carbon dioxide emissions, but no other greenhouse gases. In terms of smart city deployments, the LTS (Mid-Century Long-Term Low Greenhouse Gas Emission Development Strategy), accepted in October 2021, sets out mid-term targets, including the following:

- Implement green building standards in 100% of new buildings by 2025
- Achieve around 40% market share of vehicles sold for new energy vehicles, including EVs (NEVs)
- Strive to reduce carbon emission from the transportation sector by more than 10% in 2030 compared with 2020 and achieve more than 30% reduction compared with 2020 by 2050

Therefore, China's industry targets reflect the general trends of emphasising green buildings and transportation, which are already partly manifested in the country's smart city deployments. For instance, two of the country's smart cities, Shanghai and Shenzhen, have made strides in utilising big data and analytics in deployment of smart transportation solutions to reduce congestion and thereby, GHG emissions.

Highlighted environmental considerations in smart city initiatives are also linked to grassroots movements as climate consciousness among inhabitants rises to the fore. Observed mainly in the changing transport choices, environmental concerns increasingly correlate to cost of living and energy efficiency considerations. The same holds true for local authorities looking to reduce energy costs and optimise solutions.

Technological developments

Modern smart city deployments are intertwined with IoT connections and solutions. IoT use cases are mostly linked to smart city-related ones, along with a few others expected to increase consistently (ie, lighting, building automation). ▶

SMART CITIES SECTION SPONSOR:

libelium

Enhanced by the growing and ubiquitous connectivity and data processing capabilities, advancement of IoT industrial applications has been a game changer for smart cities. Edge computing is a good example. As a concept, it refers to a distributed information technology architecture in which client data is processed at the periphery of the network; as close to the originating source as possible. This entails moving data partially from data centres closer to the data source, as well as enabling computing and storage at the same point as the data source at the network edge; alleviating the pressures on data centres when transferring massive amounts of information. In addition, the data processed via edge computing can be sent to real-time analytics platforms; enabling the foundations of central server applications. The integration of edge computing into sensor networks enabled the use of AI powered video technology, and led cameras to becoming part of the sensor network itself. This is part of the phenomenon which is referred to as Edge AI that helps to provide real-time insights; thanks to AI's self-training and continuous learning capabilities supported by edge computing's local data processing and analysis. Edge AI also claims to respond to the several challenges involving localisation of data processing, network connectivity/capability, data sovereignty and security. Offline data processing capabilities and local data analysis for enhanced privacy are the two solutions these technologies present for capability and data security problems.

Connectivity and capability are closely interwoven with limitations of networks and data resources, which current 5G deployments aim to largely address. Successful 5G deployments are expected to facilitate automation capabilities by resolving network and capability limitations, to be achieved via critical IoT and mobile and mass IoT deployments. The latter already exists within current 4G networks, while the former refers to time-critical IoT applications which currently use the ultra-reliable low-latency communication (URLLC) standard that will be introduced with more advanced 5G deployments. Automation IoT is another layer to be built on critical IoT and enable integration of 5G systems with real-time Ethernet and time-sensitive networking (TSN) used in wired industrial automation networks. Critical IoT's use cases are numerous and cut across industries such as transportation and automotive, creating the potential for significant benefits for smart city applications.

Besides autonomous technologies, and interwoven with data collection and processing, the concept of digital twinning is becoming increasingly popular in smart city deployments. This approach enables duplication of entire cities, infrastructures, buildings, and other assets as digital representations. Accessing the digital twin online, or through a software, allows users to test and plan deployments based on real-time data, and thereby gives local authorities a comprehensive understanding of smart city data and operations, particularly for effective management and maintenance of infrastructure assets. This is achieved through various technologies (ie, AI-powered sensors) and solutions, such as geospatial data, and data imaging/mapping. Changes or inconsistencies in usage of systems can be viewed, automatically detected or projected, based on real-time data and AI-powered analysis.

The role of AI has been visible in several areas of smart city applications:

- Applications in Smart Grid: AI-powered digital technologies and sensors allow all devices and assets within the grid to communicate better, predict grid imbalance and improve automated switching. These applications also improve security of the grid and improve demand-side energy management.

- Applications in Smart Buildings: AI-powered building applications allow for better communication with smart grids and increase their participation in distributed energy sources through data-driven analytics. At the granular level, these applications lead to better automation capabilities to reduce energy use.

- Applications in Smart Lighting: As will be analysed in depth in the next chapter, AI enabled smart lighting solutions advance applications to go beyond lighting and evolve to smart poles.

- Applications in Smart Urban Mobility: Besides future uses of AVs, current applications of AI in urban mobility include operations management, intelligent digital ticketing, and customer analytics for public transport. As discussed briefly, AI also assists in multi-modal journey planning in urban settings.

Tying all these applications together is a smart city data platform as was conceptualised by large tech companies. A smart data platform is an open, secure, and city-wide platform, with a data warehouse (in-house or on cloud) to store, manage, and report smart city data from IoT sensors and other open data sources, about energy, population, traffic, buildings, and infrastructure. Coupled with dashboards and powered by AI and analytics, the platform allows the government to manage and optimise the city's system for the benefit of businesses and inhabitants. ▶

SMART CITIES SECTION SPONSOR:

libelium

Key challenges

Despite largely being top-down initiatives, smart city deployments are not without their practical challenges. These can be explained under two main strands.

Cost

Rolling out a smart city is a costly task with national and local authorities allocating a considerable amount of budget and other resources to realise deployments. The same obstacle also holds true for incremental solution roll-outs; albeit in lesser scale. For the former, design requirements along with sustainable construction practices can not only be not costly, but also require specific technical skills and expertise which may not be readily available in local governments' disposal. Therefore, greenfield roll-outs depend largely on the capabilities of the contracted or procured products and services. To bridge the gap in the lack of administrative expertise and high technical requirements, both national and local governments often opt for large tech vendors with proven experience and know-how for deployment, which can drive up the costs even further. As a recent example of a smart city, Masdar in Abu Dhabi was estimated to cost around US$20 billion. Although it can be argued that the revenue to be made from a smart city will surpass budget spend and the return on investment (ROI) will be achieved in the longer term, along with the value added to the environment and citizen life quality, initial costs are simply too large to be ignored. The temporary pause or halt of similar projects due to the COVID-19 pandemic revealed that short-term cost considerations outweigh the perceived future benefits of such investments.

Conversely, while cost can be inconducive to large-scale smart city deployments, it can also enable smaller transitions to smart solutions by local governments. This is exacerbated by the current energy prices and the macroeconomic outlook, which can provide a further incentive to think about city-wide cost-saving measures. Simpler solutions, such as switching to smart lighting and prioritising smart grid applications (in particular, smart metering) for energy efficiency, are longer-term investments contributing to the fabric of smart city deployments.

The built environment

To accelerate transition to smart cities, a considerable amount of renovation and construction will be required in a similar fashion to achieve transition to net zero. From this point of view, the built environment can be a hindering factor in smart city deployments. In fact, attempts of achieving smart transitions through retrofits are costly, and need to be subsidised both for the public sector and individuals. Nevertheless, there are solutions to retrofit applications such as LoRa, which provides gateways to implementation. The real challenge is conducting retrofitting at scale, and thereby, local governments often opt to repurpose existing built areas or make incremental changes to improve or facilitate future transitions.

On the other hand, greenfield deployments are where smart cities are built from the ground up, with high environmental/eco standards and connectedness embedded in their designs. Since they are built from scratch, these cities meet urban sustainability considerations and fulfil the '15-minute city' requirements. Yet, they are largely testbeds; benefitting the local authorities for future deployments, and met with less enthusiasm by inhabitants as they are functional dwellings. In such deployments, national and local authorities aim to explore smart energy, transportation, utilities, as well as state-of-the-art R&D, education, and innovation initiatives.

A greenfield smart city project is currently underway in Egypt, named ACUD. ACUD stands for Administrative Capital for Urban Development, a state-owned company, and is a new smart city that is being developed approximately 60 kilometres (37.3 miles) east of Cairo; dubbed as the New Administrative Capital City (New Cairo). The city is envisioned to reach up to 7 million inhabitants in the next 10 years, and to have around 2.5 million IoT devices and the largest certified tiered data centre in Africa. Egypt's New Administrative Capital will allow the users to benefit from an end to-end online cycle for procuring, activating, and paying for utilities, Internet, and data centre services for enterprise subscribers. First announced in 2015 by the Egyptian government, this smart city seeks to lessen the burden on Cairo in terms of population growth, and constitutes the first of the 14 planned smart cities across the country.

This, along with other greenfield projects, poses an interesting question to smart city development, namely, the feasibility of building such cities from scratch as opposed to retrofitting and/or repurposing. Greenfield projects have so far been met with mixed reception since these cities are usually purpose built, namely, to act as hubs to economic development and business activity, often supported by R&D and educational institutions. Masdar in Abu Dhabi and Songdo in South Korea are examples of such deployments. ▶

SMART CITIES SECTION SPONSOR:

libelium

The Juniper Research Smart Cities Ranking

Smart City Ranking Methodology

Juniper Research collated extensive information about the smart city developments around the world to create the Juniper Research Worldwide Smart City Ranking. We incorporated the following elements into the ranking process:

- Degree of smart transportation and infrastructure present including assisted parking, MaaS, EV infrastructure
- Degree of smart energy and lighting deployed including smart street lighting, smart metering and grid
- Degree of smart city management including data platforms to assemble, analyse and display the status of the city for both city management and inhabitants
- Degree of urban connectivity including municipal Wi-Fi, urban network deployment and emergency response communication technology

The results

Juniper Research found that Shanghai is the leading smart city in 2023, ranked first for the second year in a row.

The top 5 smart cities ranked by Juniper Research are:
- Shanghai
- New York
- Toronto
- Seoul
- Shenzhen

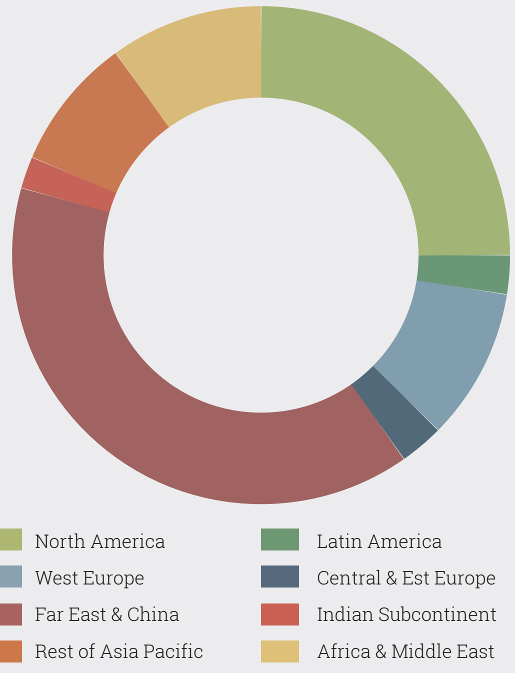
The ranking of 50 world cities is based on an evaluation of many different smart city aspects, covering transportation and infrastructure, energy and lighting, city management and technology, and urban connectivity. Shanghai is leading due to its Suishenban Citizen Cloud, which provides access for over 1,000 different services for city residents, as well as its strong deployment of 5G, and its use of innovative technologies including digital twins. The leading cities in this ranking have all rolled out services that are effectively harnessing data and connectivity to improve citizen experiences.

Shanghai has taken a joined-up approach to data; building not only a robust and all encompassing data platform, but also the connectivity to underpin every aspect of this. This joined-up approach is the biggest takeaway for rival cities wanting to emulate Shanghai's success, and should be a part of any smart city initiative to ensure success. View our infographic with further information on our top 5 cities here.

Market forecast summary

- Cost savings from smart city deployments are forecast to reach US$249 billion by 2028 globally, from US$96 billion in 2023; representing growth of 158%
- Cost savings represent the monetary impacts of reduced energy usage and emissions from the deployment of smart grid, smart traffic management and smart street lighting
- These massive savings are a major driver of smart city deployments, and will equate to almost three times the spend on smart city software and hardware by 2028; showing a clear path to return on investment for cities

Figure 2: Total Cost Savings from Smart City Deployments in 2028 ($m): $249 Billion
Source: Juniper Research



About Juniper Research

Juniper Research delivers market sizing and forecasting intelligence, competitive analysis, and strategic assessment to the world's leading innovators; enabling them to recognise today's shifting markets and seize tomorrow's opportunities.

www.juniperresearch.com

SMART CITIES SECTION SPONSOR:

libelium

Smartness is needed to build the smart cities of the future

Now that the idea of smart cities has been around for a while, Antony Savvas looks at the latest developments

> ***"Most projects have not lived up to the hype. Promised improvements in public services, economic development and citizens' lives remain largely theoretical"***

In the last century, both Walt Disney and Henry Ford attempted to build smart cities in Florida and Brazil's Amazon Rainforest, respectively. They used a combination of social engineering and new technology to promote healthier communities, and increased production.

Both industrialists failed. Disney's ill health, and subsequent death, led to his Experimental Prototype Community of Tomorrow (EPCOT) project being turned into an Orlando theme park, that is still operating. Disney's plan to limit living in the smart city for a maximum of nine months, to stop any community building roots - and developing its own democratic control - may have proved to be a major obstacle to his plans however.

Ford built his Fordlândia tyre rubber town. But Ford's ideas around abstinence among his workers – alcohol, tobacco, women and even football were banned – provoked riots against his social control, and the end of that community project too.

Acceptance

Now, the idea of smart cities has been widely accepted, although doubts still exist in some quarters around elements of them, including digital surveillance and the existence of digital credits for only those who fully comply.

Axis Communications, a player in network video, released research bringing attention to the many benefits afforded by the modern smart city, but it found almost two-thirds (63%) of people thought the way connected devices collect data about their behaviour was "creepy".

These same people must be convinced of the benefits, and assured of the safety of data collected, to enable smart city waste reduction, better public transport services, and lighting and heating efficiencies, for instance, says Axis.
In the face of accelerating climate disasters and global health emergencies, however, cities are digitally transforming to become smart in the face of adversity.

Consulting and technology services firm **Cognizant** identifies collaboration as the key to becoming future-ready, with strong ecosystems of local government, infrastructure providers and integrators being essential.

The firm says cities around the world have long been experimenting with technology to become smart through initiatives such as using sensors to improve traffic management, and applying artificial intelligence (AI) solutions to increase energy efficiency, "but with varying degrees of success".

"Most projects have not lived up to the hype. Promised improvements in public services, economic development and citizens' lives remain largely theoretical," says Cognizant. ▶

SMART CITIES SECTION SPONSOR:

libelium

Imperatives

Based on its research among 200 city officials across six global regions, along with a survey of 2,000 citizens from 20 cities, Cognizant identifies six key smart city imperatives officials need to consider.

These are:

- **Develop three-point ecosystems to support and execute on the future-ready city vision:** These ecosystems span local governments, infrastructure providers (telcos) and integrators (tech partners).
- **Design ecosystems with the right dynamics:** Mutually beneficial relationships between all ecosystem partners encourages innovation and makes successful initiatives more sustainable.
- **Create individual solutions with a shared foundation in mind:** A clear vision must guide all.
- **Embolden tech choices:** Embracing technology such as automation, AI, electric vehicles, mobile tech, cloud, digital twins – all enhanced by 5G – is essential.
- **Share data by default:** Data needs to flow not just within local governments, but often across jurisdictional borders.
- **Take privacy concerns to heart:** Concern about cyber security and the potential for citizen surveillance is widespread and must be addressed.

An important aspect is urban sandboxes, says Cognizant. These are safe spaces for experimental efforts that can safely fail without substantial negative impacts, but which could also lead to outstanding results. "This requires a mindset shift, but it could pay off handsomely," the company says.

Activity

There is obviously a lot of smart city activity out there, as **Kaleido Intelligence** has found smart city data usage will increase globally by over 140% between 2023 and 2027.

Kaleido says smart cities have recently been put back onto governments' agendas, following increased drives for municipal sustainability. It expects smart city initiatives to "intensify" in the future, with cellular IoT connections growing at a CAGR (compound annual growth rate) of 17.9% between 2022 and 2027.

"Smart traffic management in many ways represents a nexus for smart city applications," says Kaleido's James Moar. "Traffic routing decisions can be based on air quality data and smart parking availability. However, care must be taken to abide by data privacy legislation and other relevant laws, that require an intelligent network to direct data purely on a need-to-know basis."

Projects

Nick Maynard of **Juniper Research**, says: "Creating an effective smart city strategy means more than just looking at technical design, it means developing a comprehensive approach that actively solves challenges that citizens face in their lives."

The EVEREST Project, funded by the Horizon 2020 European Union programme, promises to "revolutionise" municipality traffic control with its AI processing platform. Developed by project partners **Sygic** and **IT4Innovations**, the Smart City Traffic Computation Platform will soon be available for city lab testing.

The platform collects and processes traffic data and navigates drivers in a way aligned with city policies, ensuring balanced road loads, reduced emissions, and enhanced safety for drivers and residents.

In another project, **Minima** and **Inferrix**, specialists in blockchain and IoT infrastructure, have joined forces to spearhead innovation in IoT connectivity and asset management for smart buildings.

Minima's decentralised mobile native blockchain technology will be integrated with Inferrix's IoT edge products, including wireless sensors, controllers, and intelligent gateways designed for smart buildings and sustainability.

The goal is to provide secure and efficient communication between all sensors, and the protection of mission-critical data, such as within hospitals. With hospital campus operations, the partners aim to track medical equipment to ensure it is in the right place at the right time, using continuous blockchain updates.

They also plan to enhance the visitor experience by optimising parking allocation, with the help of non-fungible tokens (NFTs) generated and distributed by the parking booking system.

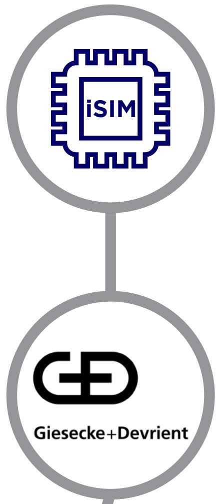
Orange Business Services has also just signed a deal with the King Abdullah Financial District Development & Management Company in Riyadh, Saudi Arabia, to design, build and run a smart city platform in the country's prime business district. Orange will iseAI and data analytics, and will provide a range of system integration services through orchestrating its partner ecosystem around the project.

The smart cities market is evolving, and its technology reach is certainly wide and varied. ■

The goal is to provide secure and efficient communication between all sensors, and the protection of mission-critical data, such as within hospitals

What is an iSIM?

An integrated SIM is the next stage in SIM solution technology. Traditional SIM cards are removable chips set into plastic surrounds, and eSIMs are dedicated embedded chips on your device's circuit board, but an iSIM is different



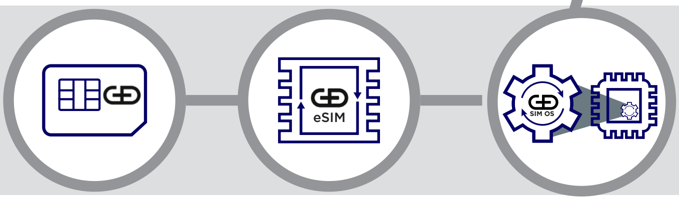
An iSIM is an isolated hardware component or tamper-resistant element (TRE) that is physically incorporated into a device's system on chip (SOC), a single chip which contains CPUs, memory, and in some cases even wireless transceivers, and is the heart of many connected devices. This means that security-critical code and data are still processed in an independent secure hardware unit, but at a much smaller size than an eSIM. So, you retain the security advantages of a smart card chip while saving space on the device's circuit board.

The iSIM has the potential to completely revolutionise the connected IoT device and technology market. Smaller, cost-efficient, and with more flexibility and sustainability, it offers substantial efficiencies and improvements over previous generations of SIMs. **Giesecke+Devrient (G+D)** commercially deployed the world's first secure iSIM solution successfully in 2021.

SIM evolution towards an all-in-one connectivity solution

Reduction of:
- Cost
- Size
- Power consumption
- Process complexity
- Plastic / waste...

Increase of:
- Service
- Sustainability
- Flexibility
- Functionality



Classical SIM card
- Pluggable SIM card
- Dedicated smart card controller
- Typically, fixed and preconfigured MNO / connectivity profile
- Form factors: Mini SIM, Micro SIM, Nano SIM
- G+D provides hardware and smart card operating system (OS)

Embedded SIM (eSIM)
- Solderable surface-mounted device (SMD)
- Dedicated smart card controller
- Supports flexible connectivity management via remote SIM provisioning (RSP)
- Form factors: MFF2, VQFN-32
- G+D provides hardware, smart card OS and RSP

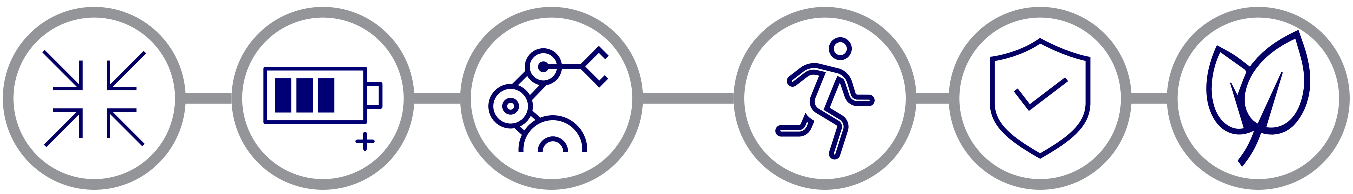
Integrated SIM (iSIM)
- Tamper-resistant element (TRE) implemented within a system on chip (SOC)
- All-in-one connectivity solution
- No additional footprint required
- No specific form factor
- Supports flexible connectivity management via RSP
- Secure production concept for IoT available
- G+D provides smart card OS and RSP

Benefits of the iSIM

Reduced footprint
Embedded into the device's hardware, the iSIM allows for smaller, lighter devices that are less expensive to produce.

Power optimisation
Lower power requirements means that batteries will last longer and IoT devices will benefit from more efficiency.

More efficient production
Integrating the iSIM as part of the baseband module can streamline production and operation processes.



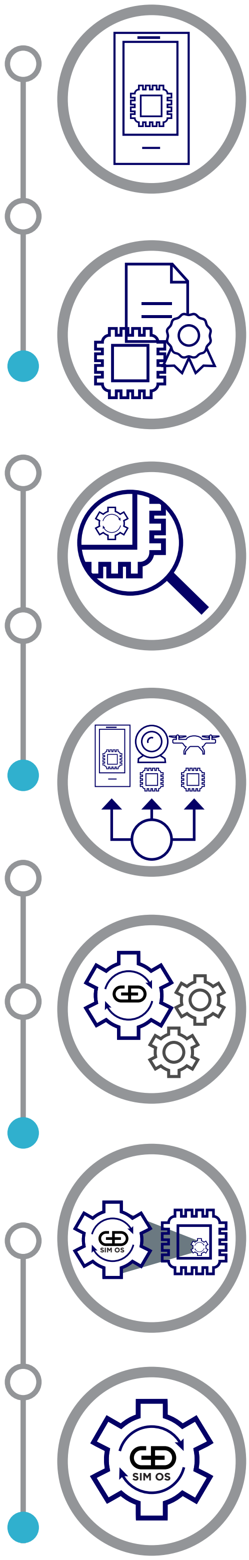
Reduced cost and time to market
Provides a generic and easy-to-integrate solution for all IoT verticals as well as a smaller chip with less material, which leads to cost reduction.

Security
Powered by G+D's trusted SIM OS, the isolated, tamper-resistant hardware is as secure as other high-end SIM solutions.

Sustainability
No extra housing or plastic, reduced power consumption and a much smaller size makes this a 'green' SIM solution for the IoT.

SPONSORED ARTICLE

Taking the lead in integrated SIM technology



Developing trusted, tamper-resistant hardware

Challenge	Fact	Action
In order for the market to adopt new standards, a high level of security is essential. G+D together with its partners deployed a solution where the security is as strong as with traditional SIM cards, for the software as well as the underlying hardware.	G+D, mobile network operators (MNOs) and other technology partners have worked together to integrate the SIM into the modem chipset. This paves the way for the next generation of secure IoT connectivity especially for narrowband-IoT (NB-IoT) and cellular low power wide area networks (LPWANs).	Although the iSIM doesn't rely on a standard hardware format, a set of design principles that are commonly agreed upon are adopted to ensure that the device remains resistant to physical tampering.

Ensure secure data preparation and provisioning

Challenge	Fact	Action
New integrated technologies, require a trusted and secure environment. To be successful, the entire process and supply chain must be secure and protected so that data can be safely generated and processed, and service can be successfully delivered.	We are committed to the secure personalisation of eSIM in consumer devices, phones, and tablets. The same applies to the iSIM for IoT devices. G+D successfully commercialised the world's first secure iSIM solution in 2021.	To ensure secure data preparation and provisioning, close collaboration across the entire ecosystem is needed. Chipset manufacturers establish Root of Trust – the physical foundation for security in a system-on-chip environment. A secure and efficient process for SIM OS download and personalisation is established.

Guarantee interoperability within the eSIM ecosystem

Challenge	Fact	Action
Interoperability is crucial to the ongoing success of iSIM. Developing common standards to both hardware and software will ensure that devices work smoothly with one another.	The eSIM ecosystem has rapidly matured into a globally trusted, secure foundation for IoT connectivity. This maturity has been aided by G+D's commitment to industry standardisation, proven interoperability and application in the field.	With security certifications and robust testing protocols in place, we have developed partnerships with industry-leading certification and testing labs. Interoperability is not just a goal – it's our standard.

Integrate and manage lifecycles

Challenge	Fact	Action
Integrating and migrating secure SIM OS on multiple chipsets, is complex and requires a high level of specialised expertise. The SIM OS loading and updating with in-factory or in the field is equally complex with challenges across supply chain, processes and security.	G+D believes that standardisation is the key to worldwide commercial success for the iSIM. We are working on several initiatives to define lifecycle management for integrated solutions concerning both operating systems and profile updates.	G+D's remote SIM management solution, allows to remotely provision devices with SIM profiles to adapt to necessary network requirements, customer choice of MNO, and local demands.

The future of integrated SIM

iSIM is a very exciting technology with massive amounts of potential, especially for the IoT. G+D prides itself on being at the forefront when it comes to bringing this to market together with our industrial partners.

If you are looking to access the benefits of evolving SIM technology now, we can help. G+D is the trusted market leader in eSIM solutions, with more than one billion eSIM devices enabled by G+D worldwide. Alongside enabling a complete eSIM solution for you today, our G+D expertise and market position means we're ideally placed to help you prepare for the future of connectivity, with iSIM at the forefront of that conversation. It is now available.

New Transforma Insights study identifies Connected-by-Design as the optimum approach for IoT

The diversity of IoT applications and the criticality of connectivity mean that the optimum way of building an IoT solution is by applying principles of Connected-by-Design. That was the key finding of a July 2023 report by Transforma Insights, sponsored by Eseye, entitled 'Connected-by-Design: Optimising Device-to-Cloud Connectivity'. This article, written by Matt Hatton, the founding partner of Transforma Insights, explores the reasons why 'Connected-by-Design' is so important

A second dimension of complexity comes from the diversity of the elements involved in an IoT solution

Each IoT use case has unique deployment characteristics. Applying a single universal moniker, in the form of IoT, belies the diversity of the space. Each has different technical requirements, commercial models, deployment environments and other sensitivities. IoT is just a convenient umbrella term for an incredibly varied set of use cases. This is especially true of the connectivity requirements, where each use case will be working under different and quite pronounced constraints, requiring particular specific capabilities.

An electricity smart meter deployment, for instance, does not need to give much consideration to power consumption given that it has ready access to mains power. Similarly it does not require much bandwidth or latency, and it's largely insensitive to unreliable connectivity. However, it will ideally work for 15-20 years without a requirement to be replaced or upgraded and devices will often be located in inaccessible places often underground. Furthermore, it will require relatively high levels of security. Contrast this with a connected heart rate monitor, which will have strict requirements for performance and reliability, or a simple asset tracker where low price and power consumption will be the key attributes for deployments of millions of highly distributed devices.

Each use case works under its own constraints and sensitivities, all of which will dictate the decisions to be made over the approach to building its technology stack, including price sensitivity (both device and ongoing connectivity), power-saving, data speeds, latency, availability, mobility, durability, space and security. These sensitivities are most prominently manifest in the choices made over which connectivity technologies and protocols are selected for the IoT implementation.

The distributed nature of IoT makes connectivity the most critical element

A second dimension of complexity comes from the diversity of the elements involved in an IoT solution. If we think of the entirety of an Internet of Things use case, the 'full stack' that might need to be considered by a developer, it comprises eight principal layers: sensors and actuators, operating systems and containers, compute and storage, applications and data, business and process integration, security, management, and connectivity.

Because IoT is, by nature, a distributed system, including end devices, edge compute (at various locations) and cloud compute, the connectivity aspect, which stitches it all together, is the most critical. IoT deployments will incorporate increasingly sophisticated compute tools, including such approaches as containers and Kubernetes, as well as the widespread use of artificial intelligence and machine learning (AI/ML). Connectivity must manage the interplay of all these elements.

IoT needs optimised and cross-optimised technologies

Developing an effective IoT solution should, as a minimum, draw upon a range of protocols, technologies and architectures that are optimised for IoT and coping with the various constraints of power, processing, memory and many more. Across the stack there are capabilities that have been developed with the constrained needs of IoT in mind. This includes ▶

elements such as the device (incorporating things like system-on-chip, and embedded SIM), operating system (such as embedded OSs such as FreeRTOS, RIOT, TinyOS and Zephyr), protocols (such as message queuing telemetry transport (MQTT) and constrained application protocol (CoAP)), and network technologies (for instance NB-IoT, Wi-Fi HaLow or LoRaWAN).

Further to this, it's not just a case of selecting the 'best' technologies, but about picking the right combination and cross-optimising them to ensure that each is able to compensate for challenges in other areas. The rewards of adopting a cross-optimised type of approach will be significant, providing a competitive advantage in terms of lower costs and/or superior functionality.

A Connected-by-Design approach is also needed

Cross-optimisation of the various elements is not enough. Optimising a deployment to take advantage of the appropriate functions and architectures, from containers to GPUs to edge compute, will become very challenging. It is increasingly unwise to build and deploy a solution and then seek to optimise in production. Such an approach will likely see a developer boxed into a corner by some of their technology decisions, for instance relating to power consumption, ability to implement security patches, costs, bandwidth, lifespan of technologies, and numerous others. What is required is a systematic approach to building an optimal solution which is Connected-by-Design.

Address connectivity flexibility and optimisation up front

The prevailing approach today is to design, build and deploy the application, monitor its performance and adjust elements of the architecture based on how it is performing. This increases the time and cost of getting to an efficient design and deployment. Developers should not wait until an IoT solution is deployed, or it will be too late. They need to address connectivity flexibility and optimisation up front, when designing the solution.

Many readers will be familiar with the concept of Secure-by-Design, whereby considerations of security are at the forefront of a product design process, permeating the whole development process. This provides a far superior framework than attempting to overlay security at the end of the development process. The same thing applies to connectivity in the context of IoT. It is fundamental to the proposition, acting as the glue that binds the various elements of the stack, and there are many potential pitfalls. This means that it cannot be simply bolted onto the solution after it has been built and/or deployed. It must permeate the design process. Hence Connected-by-Design.

The prevailing approach today is to design, build and deploy the application, monitor its performance and adjust elements of the architecture based on how it is performing

About the report

This article is based on the recently published Transition Topic Position Paper 'Connected-by-Design: Optimising Device-to-Cloud Connectivity' from Transforma Insights, sponsored by Eseye. The report examines the transition occurring in the way Internet of Things solutions are developed. The IoT is moving from a one-size-fits-all approach built on technologies that were not developed with the constraints of IoT in mind, to a 'Connected-by-Design' approach, reflecting the unique requirements of each IoT use case, complexity of the mix of components, and where careful consideration is given to how all the elements are optimised, particularly connectivity.

Introducing the Vision Stack and why your company needs it for IoT success

New VP Research in North America, Dr Brad Canham, shares some of the highlights of an innovative new research stream from Transforma Insights focussed on how technology vendors and adopters might best position themselves for success. This article explores one such topic, that of the Vision Stack, a practical tool for harnessing all aspects of organisational knowledge in order to expedite value creation

Much of the focus of technology commentators, including industry analysts, is typically on the emergence of new technologies, regulations or external commercial dynamics and how those external triggers will have an impact on the competitive landscape. Not enough emphasis is given to the internal workings of technology organisations, both vendors and adopters, and how they can adapt their operations to best embrace innovation and succeed in their chosen market. This article highlights one such key area identified by **Transforma Insights** in its recent report 'The Vision Stack: navigating complexity with knowledge' (September, 2023), and its applicability in the Internet of Things.

What is the Vision Stack?

A core characteristic of the use of IoT and digital transformation is the acceleration of innovative technologies and their penetration of all aspects of operations. In turn, the practice of innovating in organisations is not limited to R&D departments. Today, innovation happens constantly at all levels in an organisation. Traditionally, organisations organise around resources, like time, money, and people, and use a methodology like Agile or Lean to optimise innovation processes. In short, traditionally resources served as an input, a method served as a process, and the innovation was the output. By comparison, The Vision Stack is generative. It utilises the existing expertise and knowledge in organisations to adapt to the constant flow of innovation opportunities, and create innovations more quickly.

The Vision Stack is a practical tool that uses knowledge-creation to expedite value-creation in intricate adaptive systems such as IoT. Because knowledge in organisations is created by people, a knowledge-creation approach acknowledges that the objective facts of management cannot be separated from the subjective experience and expertise of human beings in organisations. Moreover, especially in complex technology environments, quickly ▶

Dr Brad Canham
Transforma Insights

identifying and exploiting high impact opportunities is an ongoing challenge. In dynamic markets, organisational clarity, speed, and alignment with the value a market is seeking are key differences between success and failure. The Vision Stack helps organisations achieve the latter by further leveraging an existing organisational resource, knowledge, from a new perspective.

The Vision Stack comprises five layers, relating to the different aspects of organisational knowledge under the acronym TEMPA (techne, episteme, metis, phronesis and arete):

- **Craft knowledge (or Techne)**, involves the application of mathematical and scientific knowledge to achieve a final result that reliably works (techne1), such as a Bluetooth connection. A variation of techne which enhances the odds of achieving a working result better than chance alone (techne2). An enterprise salesperson, for example, selling a packet inspection box to a prospect. Within the IoT, techne1 expertise ensures the proper integration of sensors, communication protocols, and data security measures, resulting in functioning and dependable connected devices, while techne2 is exemplified by experts who can strategically configure IoT devices to improve the odds of reliable data transmission and network interactions. A data sheet capturing speeds and feeds of a product on page 1 would be an example of techne1, and a use case on page 2 would be an example of techne2.

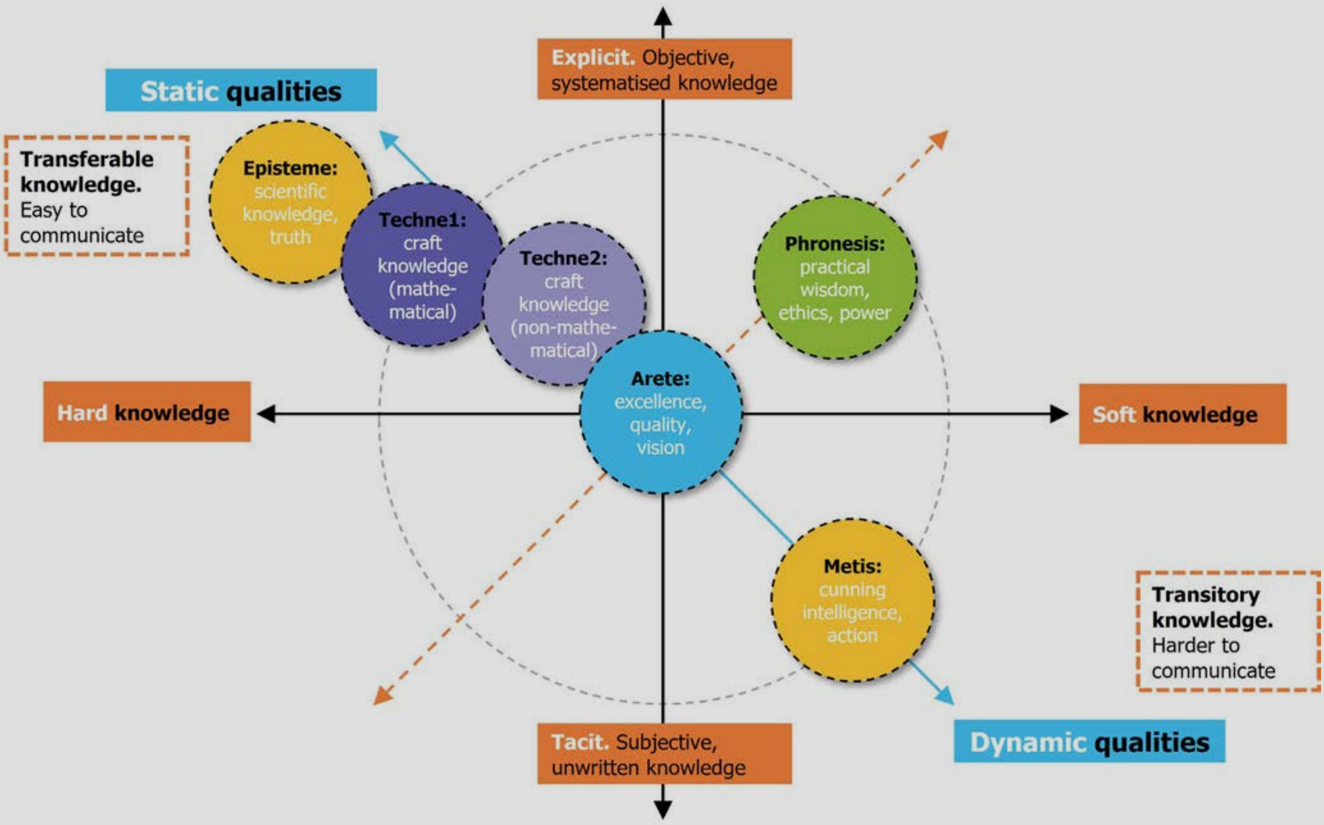
- **Scientific knowledge (or Episteme)** embodies a certain, intellectually anchored understanding, exemplified by simple mathematical truths such as 2 + 2 = 4. In the domain of IoT, episteme guides the scientific understanding of communication protocols, data security, and network architectures. Experts with epistemic knowledge ensure that IoT networks operate seamlessly and securely, preventing data breaches and enabling efficient device interactions. A patent which shows the algorithm for increasing the sensitivity of a Wi-Fi router antenna configuration is an example of episteme.

- **Cunning intelligence (or Metis)** incorporates the subjective, unwritten knowledge within an organisation. In the IoT landscape, metis manifests in the ability to swiftly adapt to unexpected challenges in network connectivity, data integrity, and device interactions. Perhaps more prominently it relates to a common social process where technology insiders conjecture together by ▶

In dynamic markets, organisational clarity, speed, and alignment with the value a market is seeking are key differences between success and failure

The Vision Stack: discrete modes of knowledge as interrelated "stack"

Source: Transforma Insights, 2023



The Vision Stack is especially relevant within innovative organisations navigating constant innovations

drawing from all the other forms of knowledge. They do so to stay up to speed with fast-moving market dynamics, company relationships, and to identify innovation opportunities.

- **Practical wisdom (or Phronesis)** is key to navigating IoT complexities, ensuring practical and ethical considerations are central. It applies practical wisdom, factoring in societal and technological considerations like climate change, diversity, justice, and fairness. Experts with phronetic insight navigate the intricate web of data collection, usage, and consent, ensuring that technology deployments prioritize individual rights and well-being. The current discussion about placing a pause on AI is an example of phronesis's reflexive expertise: "We can build AI, but if we do who wins and who loses?"
- **Excellence (or Arete)** is the pursuit of excellence across each of the aforementioned areas. It thrives within mission-driven organisations in both static and dynamic forms. For example, a static form of excellence would be an Agile method that constantly coordinates virtual teams around software development sprints. A dynamic form of excellence could include a Monday morning meeting where "the best idea wins' regardless of title or power.

  However, in many organisations there is a bias favouring measurable outcomes, static excellence, which sidelines the qualitative and more dynamic aspects of excellence, risking a restricted understanding of arete.

The Vision Stack enables leaders to assess circumstances at work at various levels, such as individuals, teams, projects, departments, organisations, vertical markets, and fields, incorporating both the explicit objective forms of knowledge (e.g. episteme and techne) or the tacit forms, such as metis and phronesis.

How can the Vision Stack be used?

The Vision Stack is especially relevant within innovative organisations navigating constant innovations. For example, in an IoT landscape, episteme encompasses the scientific understanding of IoT technologies, while techne involves the technical competencies to construct and manage IoT networks. Metis is a form of expertise used manoeuvre the intricacies of ever-changing IoT stacks, ecosystem levels, technology partners and niche use cases. Phronesis guides practical considerations of deploying IoT solutions, like building trust with partners, accounting for contextualisation, security, privacy and societal considerations. Arete in IoT describes the process of locking in static excellence, and then ▶

pushing forward with dynamic excellence initiatives, which encompasses technological innovation and ethical implementation.

Technology companies tend to overly favour technical knowledge. Hard-earned expertise and experience which provides aha moments, short-cuts, conjectural insights, and a 'feel' for the market get lost. Furthermore, 'if you can't measure it, you can't change it' is a common maxim in technology. Not the least because of the vast array of raw data, information, and metrics available. But, data is not knowledge, and information isn't navigation. Solely paying attention to metrics and ignoring more qualitative learnings can result in slowed innovation and missed opportunities.

To realise the fully market opportunity, technology vendors and adopters must consider how the organisation harnesses organisational knowledge as a whole. They should consider practical mechanisms for the sharing of tacit knowledge, including daily/weekly stand-ups, skunkworks projects, and sales input to product development.

How does the Vision Stack apply? A practical example in IoT

Consider the scenario of an IoT gateway firm, where a sales leader's social influence secured a meeting with a Fortune 500 industrial conglomerate. Despite the conglomerate's limited prior engagement with the IoT firm's offerings, the sales leader discerned a new narrative. It revolved around early discussions involving the conglomerate's foray into digital transformation.

The sales leader perceived a convergence of market indicators and pursued the conglomerate based on a 'hunch'. While other enterprises were also in the IoT firm's pipeline, this conglomerate 'felt' distinctive to the sales leader. Driven by tacit expertise and an inherent understanding of the situation, the sales leader marshalled company resources and leveraged her social capital to champion the pursuit of this deal. In essence, the available explicit data suggested that the conglomerate was an unpromising prospect. However, the sales leader's tacit insights pointed to an opportunity in the making.

In time, the sales leader's instinctive expertise was validated. The initially hesitant conglomerate partnered with the IoT gateway firm, eventually procured thousands of units. The conglomerate furthered the partnership and led a funding round with the IoT gateway firm. This narrative underscores how tacit expertise often serves as the origination point for exponential scaling as well as pivoting.

Rather than succumbing to the tunnel vision of explicit data, characterized by metrics such as weekly sales calls and revenue figures, a more holistic approach emerged. Prioritizing the fusion of explicit and tacit knowledge preserved the knowledge-creation to value-creation process. The fusion also scaled the relationship to higher levels in the broader IoT ecosystem. This ecosystem bridged hierarchical divides, engendering a culture of dynamic teamwork fuelled by ideas and collective expertise.

A different way of thinking

We are conscious that this article does not fit the usual mould of contributions to IoT Now, which tend to examine the implications of a highly impactful new technological or commercial change. Transforma Insights analysts regularly contribute such articles, including several in this issue! However, we also think that it is critical that organisations and leaders in the technology field have support around the internal, 'feel for the game' considerations dominating their thinking. How do I converge hard metrics with my soft signals to drive innovation? How do I fill my sales pipeline? Which trade shows are the best for us to attend? How do I bring all our expertise to bear when reacting to constantly changing market conditions? And so forth. In this article we offer the Vision Stack as a tool and perspective on how additional forms of knowledge and expertise play a key role in the success of innovative organisations. Such initiatives are just as important as understanding the technology landscape, and one where at least one analyst firm is looking to assist. ■

To realise the fully market opportunity, technology vendors and adopters must consider how the organisation harnesses organisational knowledge as a whole

www.transformainsights.com

TRANSFORMA INSIGHTS

Global Advisors on IoT, AI and Digital Transformation

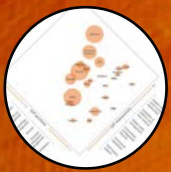
Transforma Insights can increase your revenue, reduce your costs, and limit your exposure to risk

How?

We're glad you asked...

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

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



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

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

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

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

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

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

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

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

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

transformainsights.com enquiries@transformainsights.com @transformatweet

Best practice for delivering IoT connectivity

Report sponsor

BOSCH

Invented for life

Best practice for delivering IoT connectivity

The last decade has seen a rapid evolution in the way that IoT devices are connected and supported. In this light report Transforma Insights examines the key developments in delivering cellular-based IoT, how they translate (or should translate) into evolving demands from enterprises, and what connectivity providers, and others in the ecosystem, need to do to deliver them

The IoT connectivity space is going through a period of pronounced change. The tools used to deliver connectivity, the commercial models surrounding it, and the regulatory environment are undergoing a period of quite rapid evolution. In this section we identify some of the key critical changes that might affect how enterprise IoT solutions might be supported.

The first development relates to the arrival of a set of technologies that are optimised for more effectively supporting IoT. The most notable of these is probably the arrival of a set of low power wide area (LPWA) technologies that are designed to support relatively low bandwidth applications (less than 1Mbit/s, and often much less), coupled with low power consumption allowing devices to last for months or even years in the field, and a low price point. The most notable cellular additions here are narrowband-IoT (NB-IoT) and LTE-M. These technologies are the medium-term replacement for 2G and 3G networks, and with superior capabilities, that are being switched off around the world.

A number of other technologies have also become available that are also optimised for deployments in more constrained environments, i.e. where there is a lack of access to power, processing or connectivity. For instance, IoT optimised protocols such as message queueing telemetry transport (MQTT), constrained application protocol (CoAP) and Lightweight M2M (LwM2M) are increasingly widely used. Similarly, embedded operating systems such as Free RTOS, TinyOS or Zephyr, reduce the requirements for processing and memory on the device. ▶

One of the key facets of the arrival of the IoT optimised technologies noted above, is that they are also highly constrained, meaning that it's necessary to ensure that they are cross-optimised with each other to make sure that devices, connectivity, protocols and applications all work well together. This is one reason why we see hardware makers increasingly successful in bundling hardware and connectivity: one cross-optimised solution with a single vendor to deal with in the event of any problems.

The other major technology development is embedded SIM (eSIM). Until 2016 devices relied on removable SIM cards for authenticating devices. Since then eSIM (a ruggedised soldered chip) has become increasingly the norm, with integrated SIM (iSIM), which virtualises the SIM entirely as an element on another processor, to follow. With this change of form factor can the need to change the profile remotely, using a technique called Remote SIM Provisioning (RSP). Today there are two standards (known as M2M and consumer) with a third (IoT) being standardised currently. The availability of eSIM creates new dynamics in how connectivity can be provided and by whom. According to Transforma Insights, by 2032, 40% of new cellular IoT shipments will be eSIM-capable.

The advent of eSIM focuses attention on another major change ongoing in how IoT connectivity is delivered, particularly for multi-country IoT deployments.

Historically connectivity providers used roaming, either based on their own roaming agreements or those of partners. Alternatives included proprietary 'multi-IMSI' approaches. However, roaming has become less viable, partly due to regulation, and partly because host networks have been less willing to accept roaming IoT devices on their networks. The need to be conscious of regulatory issues of all types has also increased dramatically in recent years.

We should also note that the delivery of IoT connectivity is not immune from the growing importance of artificial intelligence. It has two major implications. Firstly it can be harnessed for more effectively delivering IoT connectivity services, for instance in analytics and optimisation. Secondly the requirement to embed AI within applications will have knock-on effects on the architecting of IoT solutions. Whereas historically the intelligence of an application might have resided on the customer's server or hosted in the cloud, increasingly the intelligence will be distributed so as to reduce the latency of the application and more efficiently manage data. This creates implications for edge computing, and the need to manage payloads at various points on the network whether that be at the edge device, the network edge, or in the cloud.

Turning to the more commercial aspects of IoT we also note a number of significant trends that influence how

IoT connectivity is delivered. Most notably there is a clear dynamic of price erosion, manifest in what Transforma Insights refers to as '$1 IoT', whereby many devices may generate less than US$1 of revenue per year. This doesn't apply to all connections, but it is likely to apply to a large volume, particularly of the LPWA connections. This trend triggers connectivity providers to make numerous changes to their propositions to do two things: bolster revenue and reduce cost. In the former case this results in the addition of new services offerings, which in many cases are sorely in demand by enterprise customers that need more of a tailored service. In the latter case it drives a desire to be more 'hyperscale', delivering connectivity with low touch, highly scalable platforms and processes.

7 key requirements of enterprise IoT connectivity users

In general, enterprise demand for the features and functionality of their IoT connectivity solutions have always been quite consistent: secure, reliable, compliant, low cost connectivity that is easily managed and highly scalable. However, with increasing price pressures, more regulation, emerging technologies and new commercial dynamics, those needs are constantly in flux. This section provides an overview of the key requirements that Transforma Insights hears from enterprises regarding IoT connectivity, whether they are triggered by evolving changes in the industry, or not.

Reliability

The prime consideration above all others with IoT connectivity is: does it work? Network outages are unacceptable and enterprises need to give careful consideration to which mechanisms are being used by connectivity providers to support their deployments. This necessitates some potentially tough questions with providers over exactly how they plan to deliver connectivity services such as sponsored roaming, multi-IMSI, or eSIM localisation. Further to this, the cross-optimisation topic noted in the previous section should deliver more effective solutions with fewer faults, as well as simpler fault resolution, because the different elements of the solution have been developed with consideration of the capabilities and limitations of the others.

Reputation and brand

In the Transforma Insights Enterprise IoT connectivity survey published in November 2022, the number one factor influencing enterprises over vendor choice for IoT connectivity was "reputation/brand". The category combines a broad range of considerations, but there is little doubt that enterprises should give very careful consideration to whether a connectivity provider is a trusted long-term partner. Most enterprise IoT deployments will involve a long-term relationship that typically involves mission-critical applications. Enterprises should look at factors such as ownership ▶

structure and major backers, the use of standards, and established credentials with major adopters. Similarly the ability to back-out of a relationship if things go wrong, which would usually be associated with the use of eSIM.

Security

This topic has always been one of the top two considerations and concerns for IoT adopters. The security threats associated with IoT are growing: there are more use cases, with bigger scale and more mission-critical than ever before, making IoT an increasingly appealing target for bad actors. Even without that growing scale, the security landscape for IoT was already something of a headache with a complex array of stakeholders, a diverse set of devices, and a general lack of embedded security development skills. Add to this the fact that IoT is making more use of constrained devices with potentially less capability to support security features.

Coverage

With cellular IoT connectivity, there is no escaping network coverage as a significant consideration. However, the degree to which coverage is important will depend very much on the application. Some devices will be located in hard-to-reach places, while others will be constantly moving. The question for enterprises is: will I get the right coverage for the application at an appropriate price point. Some connectivity providers may be able to support connectivity over a single network in a market, and others using multiple networks. The use of eSIM for localisation may be the best approach. But in some cases the ability to roam onto multiple networks will give a superior experience. Cellular connectivity solutions are also increasingly integrating non-terrestrial networks (NTNs), i.e. via satellite, so these offerings may hold some potential.

Price

We have already mentioned that price for IoT connectivity is seeing some erosion. This will always be a prime consideration for enterprise customers. However, the most important thing to consider is: low price at what cost? A low headline rate often belies a service that is not delivered in a compliant way. Or where there will be subsequent overage charges once the real volume of data generated by the application becomes apparent.

Compliance

Regulations affecting IoT have expanded significantly in recent years. This has increased the degree to which enterprises need to be aware of compliance-related topics. This is particularly important for some countries that have more challenging regulatory regimes, e.g. Brazil for permanent mobile roaming, China for data sovereignty, Europe for data, or the US for device security and certification. ▶

Support

For most enterprises, IoT is not core business. As a result, it is normal for enterprises to require a high degree of hand-holding as they go through the process of developing and rolling out their IoT solutions. Most need an additional service layer on top of the technology building blocks which helps them to understand which are the most appropriate technologies for them to use, what the roadmap looks like, how to deploy them and more.

A checklist for what connectivity providers and others in the ecosystem need to deliver

The evolution in technology and commercial models, as well as changing demands from customers, as outlined in the sections above, should flow through into a refined set of capabilities from IoT connectivity providers, MNOs and MVNOs.

In this section we provide a checklist of some of the key facets of what those providers should deliver, both technical functions, such as features of a connectivity management platform, and services.

SIM management - The baseline functionality of IoT connectivity, involving managing the SIM, specifically activation, deactivation, suspension, APIs and some billing functions.

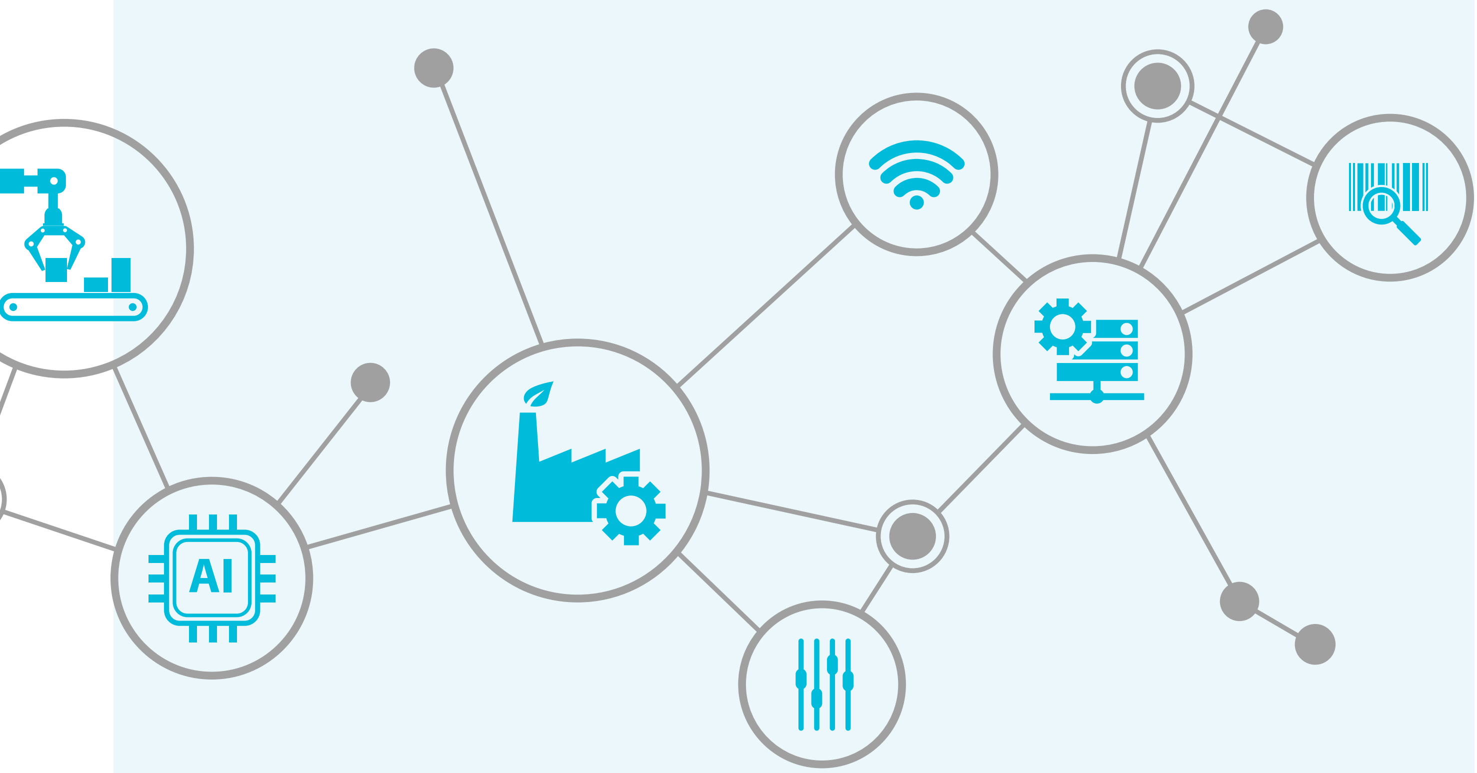
Abstraction - Many enterprise customers have multiple relationships with connectivity providers. They will want a single pane of glass to enterprise customers to manage all their connections.

Localisation - Supporting connectivity in any geography, either through eSIM subscription management or through some other viable alternative to provide compliant comprehensive coverage.

Analytics - A range of analytics and automation of connectivity functions based on network data, including related to network selection, security, anomaly detection, root-cause analysis, churn reduction, bill prediction and many more. This is likely to make increasing use of AI. To be fully optimised, this must be real-time.

Control - Complex global device deployments demand greater policy control and management of data flows. It is increasingly common practice for connectivity providers to operate their own core network and associated infrastructure for the purpose of providing greater transparency, more real-time capabilities and higher levels of security.

Compliance - Connectivity vendors need to be able to provides some level of guarantee to the enterprise about the end-to-end compliance of its deployment, for instance related to permanent roaming, data sovereignty or device security. ▶



A device-to-cloud (and edge) experience - IoT is about connecting devices to the cloud to enable (bidirectional) data flows. As a result, an IoT connectivity offering must incorporate serious considerations of (and features related to) delivering that full stack. This includes cloud connectors for seamless integration into AWS, Azure and others, orchestration of payloads, and the integration of hardware into the proposition.

Devices - Further to the device-to-cloud topic, IoT connectivity providers are increasingly adding in device-related capabilities, as a way to avoid the potential pitfalls of simply bolting on a connectivity provider to an already built device. Capabilities include hardware integration and optimisation, device management, troubleshooting, and warehousing and fulfilment.

Security - A range of capabilities including end-point, network (such as private APNs, network diagnostics and troubleshooting, device locking, device quarantining), transport (such as IoT SAFE and transport layer security), cloud/data, and application security. Additionally end-to-end security including secure-by-design, policy management, vendor compliance, and anomaly detection across the other layers.

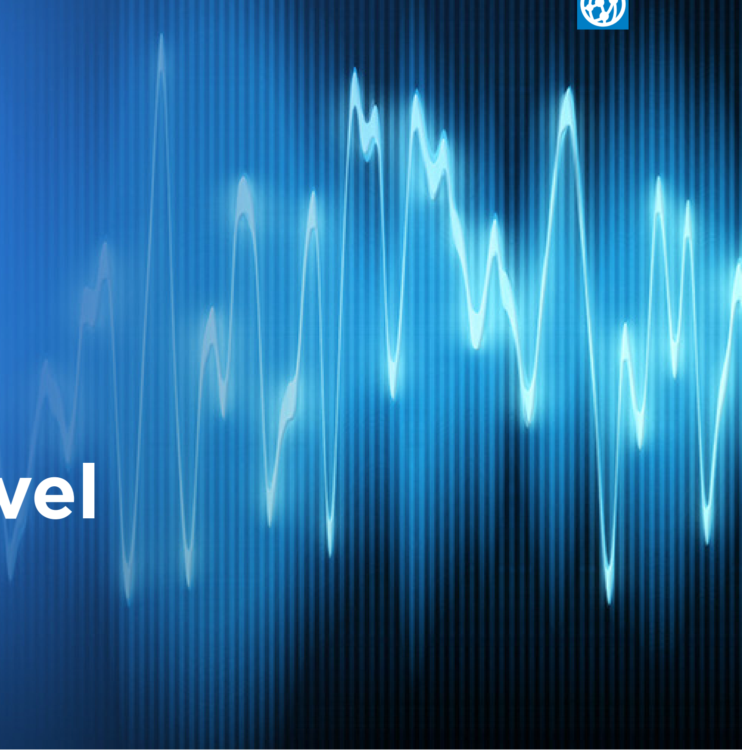
Hyperscale platforms and processes - The price of connectivity is declining and in order to support that, particularly for low-cost LPWA connections, IoT connectivity providers need a set of capabilities and processes in place that can deliver connectivity in a low-cost scalable way. This includes cost-effective connectivity management platform with low touch onboarding of devices.

Speed and agility - Time to market is an increasingly important issue for enterprises deploying IoT. Operators will need to provide a connectivity solution that is deployable in a matter of weeks. Connectivity providers also need to be sure that they can react to changing market dynamics, including regulation, requiring new features, reports or technologies, delivered in a timely way.

SLAs - IoT is often deployed for mission-critical use cases. Enterprises will demand strict SLAs, particularly over up-time and fault resolution time. The ability to offer SLAs will depend largely on the CMP vendor's end-to-end control of the proposition.

Superior customer support - Comprehensive 24x7, follow the sun, support is a must-have for IoT connectivity providers. As is online self-care. Also customer success managers to act as the voice of the customer within the organisation, reflecting the fact that IoT is not a product-based transaction, but a managed service.

A customised/contextualised approach - IoT is not best delivered as an off-the-shelf product. All customer requirements are different and require some degree of customisation, or at least contextualisation, i.e. delivering a connectivity offering that is the most appropriate for the customer's circumstances. This requires enhanced pre-sales support and a consultative sales approach to really understand their needs.

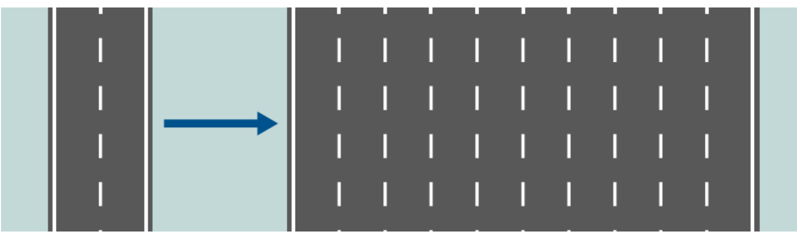


Is 5G mmWave technology paving the way for next-level connectivity?

In a digital age defined by rapid advancements, the horizon of connectivity is expanding like never before. In the early stages of the 5G rollout, most countries tried to promote its deployment based on 5G Sub-6GHz. This is because it can build upon the experience and technology from the 4G era, offering the advantages of wide coverage and relatively faster speeds. It is very suitable for rapid initial deployment, assisting consumers and businesses in quickly experiencing the convenience of 5G

With the continuous enrichment of outdoor multimedia and entertainment content, the demand for 5G networks is shifting from traditional mobile devices such as smartphones and computers to a pursuit of higher internet speeds for industrial automation, healthcare, intelligent transportation, and augmented and virtual reality (AR/VR) experiences. This leads wireless carriers to focus on how to deliver services that upgrade the current mobile network experience, especially in densely populated, economically thriving urban areas where entertainment lifestyles are rapidly evolving. In terms of network coverage in suburban areas, there is a need to consider how to provide higher-quality network services for users in these regions.

Decoding 5G mmWave's significance



Source: GSMA-5G-mmWave-Factsheet-Unlocking-the-Full-Potential-of-5G.pdf

5G mmWave— an innovation that operates within the millimetre wavelength spectrum and serves as the bedrock of 5G technology. It contains some significant features:

1. **Enhanced speed:** mmWave, introduced as the NR frequency range 2 (24-52 GHz) (FR2) in the 3GPP specifications, is considered the rising star to unleash the 10 Gigabit (Gbps) speed limits in 5G. And according to the latest news reported in July 2023, Nokia said it has achieved sustained average downlink speeds of over 2 Gbps using mmWave spectrum and 5G fixed wireless access (FWA) over a distance of 10.86 kilometres.

2. **Low latency:** mmWave technology features such as short wavelengths, beamforming, large bandwidth, and support for real-time applications make it well-suited for achieving ultra-low latency.

3. **Elevated capacity:** Utilising the wide frequency band available in the mmWave spectrum, and the unique short wavelengths, mmWave has the potential to provide up to 1000MHz bandwidth, which will bring users an unprecedented high-speed experience.

4. **Millimetre wave antennas** are smaller and equipment is lighter, which makes deployment more convenient.

These collective attributes come together to empower 5G mmWave with seamless functionality, especially in densely populated environments such as dense residential areas, dense business districts, bustling airports, dynamic stadiums, and vibrant music theatres. In these high-traffic arenas, where the need for rapid internet is tremendous, 5G mmWave performs exceptionally, delivering an internet experience with seamless connectivity. ▶

SPONSORED ARTICLE

Furthermore, FWA emerges as a pivotal use case for 5G millimetre wave technology, catering to both residential and commercial settings. This technology finds utility in offering high-speed wireless internet connectivity for homes and office buildings, enriching the communication landscape.

For instance, in the pioneering 5G deployment undertaken by the United States, a strategic emphasis has been placed on mmWave networks. Geographical considerations play a pivotal role in the mmWave deployment strategy. With most highly populated American cities concentrated along the east and west coasts, as well as select southern states, network operators prioritise the establishment of robust infrastructure in these densely populated zones. The inherent advantages of mmWave help users to have a fast-speed and stable internet connection.

Furthermore, in India, urban landscapes are characterised by a dense population, resulting in a heightened requirement for seamless high-speed and low-latency data connectivity. In this context, the capabilities offered by mmWave technology become particularly pertinent. Its capacity to deliver elevated data rates and accommodate substantial data loads aligns exceptionally well with the data-intensive needs of urban dwellers in the country while balancing the deployment cost.

Therefore, mmWave emerges as the feasible solution to cater to the evolving demands of the modern connectivity landscape. With its remarkable combination of high speed, low latency, and elevated capacity, mmWave is poised to revolutionise connectivity, particularly in densely populated urban areas and suburban regions.

Unveiling the future

The 5G mmWave system boasts abundant frequency resources and a substantial bandwidth, offering a solution to the global shortage of mid-to-low frequency spectrum resources. Mid-band is perfect for 5G rollout in wide areas and high-band offers large capacity for precise areas. When combined with Sub-6GHz tech, it covers the entire country with 5G.

Due to their shorter wavelengths, mmWave corresponds to frequencies of 30-300 GHz. This frequency is considered quite high in the electromagnetic spectrum. Higher frequencies result in faster signal transmission speeds and greater storage capacity. This way, it can reach data speeds over several Gbps in certain places.

FWA devices work together effectively by combining the 5G Sub-6GHz frequency range with mmWave technology. 5G Sub-6GHz fulfills the role of genuine high-speed transmission to make up for the flaws of 5G mmWave requiring a high cost of transmission in a wider range. Using the 5G mmWave system allows for the deployment of a greater number of antenna arrays within the same area, concentrating beamforming energy. Employing transmission technology in short-distance and low-interference scenarios ensures superior network stability and higher transmission speeds. Ultimately, this empowers both households and businesses with FWA services and cost-effective deployments.

Choose Fibocom's 5G mmWave Solution

Fibocom's FG190W 5G mmWave and Sub-6GHz module supports up to 1,000MHz bandwidth in the mmWave frequency range and NR 10CA for downlink. It also supports up to 300MHz bandwidth in NR Sub-6GHz and NR 5CA for downlink, achieving a maximum downlink peak of 10Gbps. The module is built with an LGA package, supporting flexible custom development needs.

Multiple reserved interfaces empower the ODU to connect external omnidirectional, directional, and mmWave antennas. These antennas penetrate signals more effectively and environmental changes while maintaining alignment, ensuring network link availability. With the support of dual connectivity simultaneously, 5G Sub-6GHz and 5G mmWave, the module can receive and transmit wireless signals even in complex environments, enabling unrestricted 5G signal utilisation.

The 5G mmWave system boasts abundant frequency resources and a substantial bandwidth, offering a solution to the global shortage of mid-to-low frequency spectrum resources

The solution can be implemented through Open CPU development architecture, allowing flexible choices based on customer requirements. Meanwhile, the Open CPU approach reduces the physical size of terminal products, increases integration, and lowers overall costs and energy consumption. Diverse development architecture options provide convenience, fostering the adoption and application of 5G FWA technology.

In a world that thrives on innovation, 5G mmWave emerges as the beacon guiding us toward a new era of connectivity. As a leading global wireless module and solution provider, Fibocom's journey through its potential takes on added significance, illustrating the transformative power that mmWave technology holds in redefining the global landscape.

www.fibocom.com

The regulatory stack for IoT-enabled digital transformation

The telecommunications space has long been a highly regulated environment, including aspects relating to the radio performance of devices, allocations of spectrum for cellular networks, universal service obligations, and so on. But in recent years, regulators around the world have upped their game and a slew of new regulations that apply more widely to digital transformation initiatives have been announced, reports Transforma Insights

Requirements such as secure by design will be increasingly commonplace for IoT devices

This article focuses on new emerging regulations in the fields of cellular connectivity, the Internet of Things (IoT), and artificial intelligence (AI). What follows is not a detailed review of such regulations, simply a summary of some of the more interesting and impactful aspects. Some of the regulations referred to are still in a planning stage and have yet to be implemented.

Cellular connectivity

Focusing initially on (cellular) mobile private networks (MPNs), it may be the case in a certain market that spectrum has been set aside for the operation of MPNs, but this is not the case in all markets. In markets where spectrum has not been set aside for MPNs it may, or may not, be possible for any potential end-user adopter of MPNs to lease spectrum from an incumbent cellular operator.

International roaming of cellular IoT connections is allowed in many markets but banned in some. In some territories where international roaming of cellular IoT connections is allowed, fair use policies apply so that effectively overseas players cannot use international roaming as a back door to gain market entry and compete with domestic providers. Even in markets where fair use restrictions do not apply, then it may be necessary for an overseas IoT provider to register with a local regulator and potentially join a licenced dispute resolution scheme before offering services. A number of countries around the world stipulate that any entity offering IoT services in a country must first establish a locally registered operating company.

Embedded SIM (eSIM) technologies that allow cellular connections to localise onto domestic networks do circumvent many of the restrictions associated with international roaming, and the eSIM concept has been broadly welcomed around the world, but in certain markets there are restrictions associated with the use of eSIM. For instance, in China the servers supporting eSIM must themselves be located in China.

Internet of Things

Regulatory considerations do not end once the challenge of simply connecting a device has been overcome. A range of new IoT-domain regulations are at various stages of development and implementation around the world.

Requirements such as secure by design will be increasingly commonplace for IoT devices. A key consideration of many such emerging regulations is the management of passwords which often must be user-configured (so that users cannot simply adopt a default password) or that default passwords must be unique. Other restrictions apply to the management of any IoT security vulnerabilities that are identified, with support for software updating to patch such vulnerabilities mandated in some markets, alongside certain reporting requirements.

New regulations are also expected to apply to the management of data associated with IoT devices. Variously these might apply restrictions to the modification or destruction of data; unless such modification or destruction is requested by end-users and in which case other regulations might mandate that the end-user's requirements are complied with. Other regulations apply to data that might be stored on end-user devices, stipulating that permission is sought (and received) for such an approach.

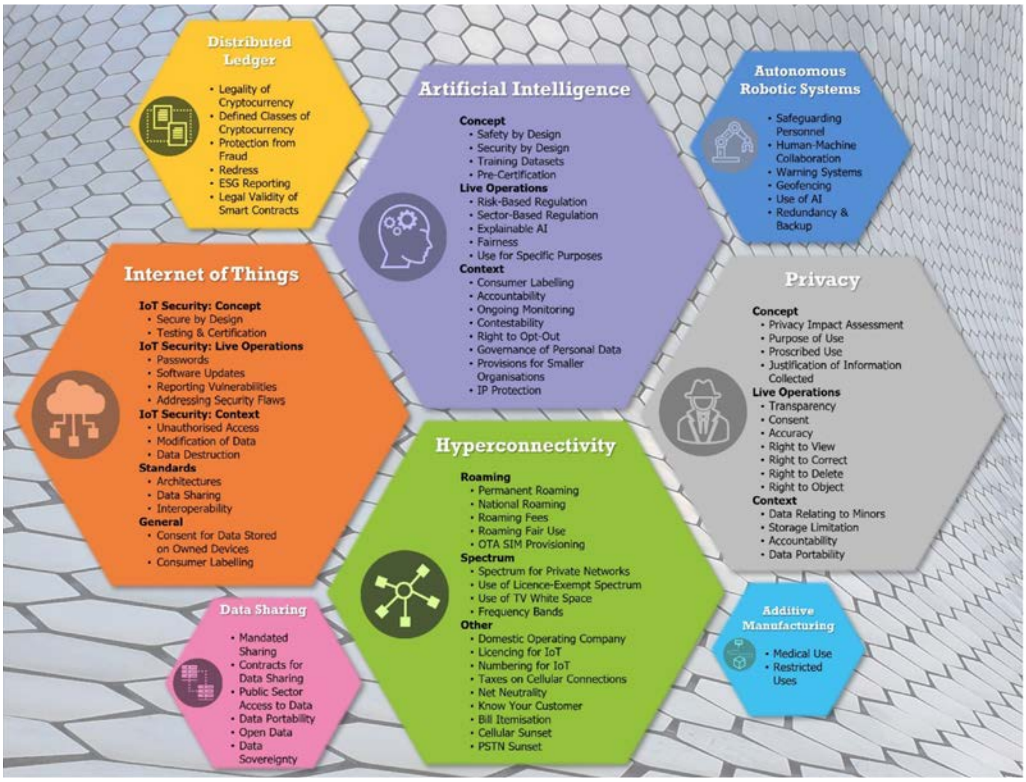
Meanwhile, the (proposed) European Data Act seeks to make more data available for use by more parties. For instance, stipulating that all information that a device OEM has about a particular IoT device should be made available to the owner of that device so that he, in turn, can provide it to third parties. The aim of the Act is to facilitate a competitive market in aftermarket services.

Artificial intelligence

Meanwhile, incoming regulations that would relate to AI have been garnering headlines recently. Probably the most high-profile of ►

SPONSORED ARTICLE

Figure 1: The DNA of Regulations [Source: Transforma Insights, 2023]



Interestingly, the USA's 'Blueprint for an AI Bill of Rights' includes provisions for consumers to be able to 'opt out' of AI-enabled processes on request

these is the EU's proposed 'AI Act' although many countries around the world have similar initiatives.

At the core of many such proposals is the (arguably unachievable) concept of 'fairness' of AI outputs, but many such regulations extend to include sector- and risk-based regulations. The concepts of 'safety by design' and 'security by design' feature often, with some regulators seeking to stipulate pre-certification for higher-risk applications, and with different approaches to ongoing reporting and monitoring. Other considerations relate to the 'explainability' of AI outputs and consumer labelling for AI or other techniques to ensure that consumers are aware that they are interacting with AI generated content.

Interestingly, the USA's 'Blueprint for an AI Bill of Rights' includes provisions for consumers to be able to 'opt out' of AI-enabled processes on request. Proposed regulations in many parts of the world include provisions relating to the right of a consumer to contest the results of AI-enabled processes.

Sector regulations

And, of course, layered on top of these considerations are a potentially wide range of vertical- and application-specific regulations, many of which may vary by country. For instance, HIPAA (Health Insurance Portability and Accountability Act) healthcare regulations in the USA. Healthcare in general can be a particularly challenging field, and in some cases a digitally transformed version of a process associated with a medical treatment may precipitate a need for a new approvals cycle. For instance, if a physical signature to validate a process was specified as part of the initial approval process.

Conclusions

The direction of travel for regulations associated with digital transformation is clear: in future there will be more of them, applying to more aspects of any potential digitally transformative solution, and the detail of regulations is likely to continue to vary across different countries around the world.

Accordingly, it is becoming increasingly important for end-user adopters of digitally transformative technologies, and for vendors of such solutions, to pay close attention to regulatory developments. As a general rule-of-thumb, the 'closer' that a digitally transformative solution gets to impacting a consumer, then the more regulations are likely to apply. But many regulations will apply for all kinds of digitally transformative solutions, even if they are buried deep inside the workings of an organisation.

In a recent report, Transforma Insights has identified the 'DNA of Regulations', as illustrated in **Figure 1**. The DNA of Regulations is a list of themes that commonly feature in a range of regulations as they apply to digital transformation around the world. An associated Regulatory Database provides a summary of, and links to, regulations that apply to any of these identified themes in a range of individual countries. ■

Our pick of IoT industry's upcoming events

SEPTEMBER

AI Hardware & Edge AI Summit
https://www.iot-now.com/event/ai-hardware-edge-ai-summit/

DTW23 – Ignite
https://www.iot-now.com/event/dtw23-ignite/

Chief Data & Analytics Officer – Government
https://www.iot-now.com/event/chief-data-analytics-officer-government/

SIDO Lyon
https://www.iot-now.com/event/sido-lyon-2/

The Things Conference 2023 Amsterdam
https://www.iot-now.com/event/the-things-conference-2023-amsterdam/

Quantum Business Europe 2023
https://www.iot-now.com/event/quantum-business-europe-2023/

IoT Tech Expo Europe
https://www.iot-now.com/event/iot-tech-expo-europe-2/

Digital Transformation Week Europe
https://www.iot-now.com/event/digital-transformation-week-europe-2/

AI & Big Data Expo Europe
https://www.iot-now.com/event/ai-big-data-expo-europe/

Cyber Security & Cloud Europe
https://www.iot-now.com/event/cyber-security-cloud-europe/

MWC Las Vegas 2023
https://www.iot-now.com/event/mwc-las-vegas-2023/

OCTOBER

AI in Healthcare Summit
https://www.iot-now.com/event/ai-in-healthcare-summit/

Supply Chain Europe 2023
https://www.iot-now.com/event/supply-chain-europe-2023/

Network X 2023
https://www.iot-now.com/event/network-x-2023/

NOVEMBER

Enlite Europe 2023
https://www.iot-now.com/event/enlite-europe-2023/

London EV Show
https://www.iot-now.com/event/london-ev-show/

Smart Cities Connect
https://www.iot-now.com/event/smart-cities-connect/

IoT Tech Expo Global
https://www.iot-now.com/event/iot-tech-expo-global-2/

Digital Transformation Week Global
https://www.iot-now.com/event/digital-transformation-week-global-2/

Cyber Security & Cloud Global
https://www.iot-now.com/event/cyber-security-cloud-global/

DECEMBER

GIANT Health Event
https://www.iot-now.com/event/giant-health-event/

GIANT's Mental Health Tech Show
https://www.iot-now.com/event/giants-mental-health-tech-show/

GIANT's Women's Health Tech Show
https://www.iot-now.com/event/giants-womens-health-tech-show/

GIANT's Future Hospital Show
https://www.iot-now.com/event/giants-future-hospital-show/

GIANT's UK National ICS Congress
https://www.iot-now.com/event/giants-uk-national-ics-congress/

Chief Data & Analytics Officer – APEX West
https://www.iot-now.com/event/chief-data-analytics-officer-apex-west/

SIDO Paris
https://www.iot-now.com/event/sido-paris-2/

LoRaWAN® Briefing for System Integrators and Solution Providers

LoRa® is the leading LPWAN technology for IoT.

So if you are a System Integrator or Solution Provider operating in the Smart Buildings, Smart Cities and/or Smart Utilities sectors, this briefing is for you!

Just how significant is LoRaWAN for the **Smart Buildings, Smart Cities** and **Smart Utilities** sectors in the IoT market?

Use Indoors

Operates in sub-1GHz band and avoids interference issues

Penetrates walls and infrastructure

Long Range

Designed for sending small amounts of data over very long distances

Low Cost

Low deployment cost, low management cost, low sensor cost

Typically just one gateway per business property also means quick to deploy

Dowload this new report for FREE at
www.lpwaninfo.com

LoRa Alliance®

beecham research
Shaping the IoT future

Everyone hates toys without batteries.

That's hardware without connectivity.

Hey, OEMs, don't slow down play time!

Boost your revenues and make every day game day by adding connectivity to your offering.

Connect with us to learn more about how an all-in-one solution could work for you.

info@flolive.net | www.flolive.net

flo. LIVE