IoT Now: ISSN 2397-2793

Q2 2020 • VOLUME 10 • ISSUE 2

IoT NOW

HOW TO RUN AN IoT ENABLED BUSINESS

TALKING HEADS

Arm-based chips are the bedrock of the connected world and now Arm Pelion Device Management is powering IoT business transformation, says Charlene Marini

TRANSPORT
Telematics for a moving industry. See our Analyst Report at **www.iot-now.com**

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

CONNECTIVITY
How cellular technology is powering industrial IoT See our Analyst Report at **www.iot-now.com**

UTILITIES
Smart electricity metering's current state of play. Read our Analyst Report inside this issue

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

PLUS: **THE ENTERPRISE BUYERS' GUIDE - WHICH IoT PLATFORM 2020** • Will IoT show its strengths in the COVID crisis? • How Pelion Device Management is laying the foundations for Taiwan's smart city • Mavoco's Anton Cabrespina on the importance of single-source global IoT connectivity • Why the future of IoT connectivity is software-defined • Inside Aeris' project to help BBOXX provide clean energy to off-grid communities • How Apricity's LTE-M wireless water heater controllers are saving power usage • It's time to rethink streetlighting • Arm experts on how to stay ahead of the herd when it comes to device security • Latest news online at www.iot-now.com

CONTENTS

IN THIS ISSUE

Cover sponsor: Arm technology is at the heart of a computing and connectivity revolution that is transforming the way people live and businesses operate. Our advanced, energy-efficient processor designs have enabled intelligent computing in more than 150 billion chips and our technologies now securely power products from the sensor to the smartphone and the supercomputer. In combination with our IoT device, connectivity and data management platform, we are also enabling customers with powerful and actionable business insights that are generating new value from their connected devices and data. Together with 1,000+ technology partners we are at the forefront of designing, securing and managing all areas of compute from the chip to the cloud. **www.arm.com**

IoT has lots to offer for life on lock-down

Now is not the time for trumpeting or I-told-you-so but it is inescapable that, had IoT been just a few years further down the path of adoption and maturity, many of the risks associated with COVID-19 could have been reduced and some of the complexities simplified

Perhaps the most obvious area is the application of IoT technologies and services to the healthcare sector. Increased automation and improved tracking and traceability of patients, their health status and the medical resources available to them have evident advantages in the current crisis. In addition, moves towards remote, home-based healthcare has clear benefits in this climate of contagion.

Next is retail. This is also an area where the applications of IoT are multi-layered. We can easily see autonomous robots performing last mile deliveries from retailers of food and other products. These are already extensively trialled in markets across the globe but sadly have not made it into the mainstream in time for this outbreak.

Humans driving delivery vehicles puts them at risk as they come out of isolation to go to work and make deliveries. Similarly, in distribution centres and warehouses, the use of humans to pick products could be radically reduced in dark warehouses with these functions performed by robots.

We can go a step further and consider dark factories of fully automated production lines that only require minimised human interaction for maintenance and repair purposes.

Yet the benefits of IoT-enabled systems, processes, applications and services are not all confined to the future. Much of the quality of life on lock-down that we are experiencing has been enabled by the internet industry. Communications networks are enabling us to work, entertain ourselves and keep in contact with our friends and relatives. Unified communications tools that were the preserve of technology professionals and road warriors are now the housewife's choice.

Technologies that pre-date IoT such as tracking in logistics, are really proving their worth as people shop online and huge additional numbers of deliveries are made each day. That truck and van routing and tracking capability has never been more important for optimising over-stretched delivery systems.

Finally, in a time where people are at risk if they move location, the ability to perform analytics to enable predictive and remote maintenance of critical infrastructure is minimising the need for engineers to be on the move. Such systems enable only service-affecting work to be done and the delay of non-essential tasks.

These are just a few examples of what IoT is doing now to help combat the affects and impacts of the virus and a glimpse into what it can achieve in the near future. There is the real likelihood that greater possibilities for IoT will come out of this adversity as people recognise that IoT offers a means to reduce risk, improve quality of life and keep society better connected.

Enjoy the magazine – IoT has even given you something to read!

George Malim

Contributors in this issue of IoT Now

We are always proud to bring you the best writers and commentators in M2M and IoT. In this issue they include:

Levi Östling, IoT analyst, **Berg Insight**

Robin Duke-Woolley, chief executive, **Beecham Research**

Bill Ingle, senior analyst, **Beecham Research**

MANAGING EDITOR
George Malim
Tel: +44 (0) 1225 319566
g.malim@wkm-global.com

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

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

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

DESIGN
Jason Appleby
Ark Design Consultancy Ltd
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

DISTRIBUTION
UK Postings Ltd
Tel: +44 (0) 8456 444137

Printed in the UK by
The Magazine Printing Company
using only paper from FSC/PEFC suppliers
www.magprint.co.uk

weknow

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

IoT Now magazine covers worldwide developments in the Internet of Things (IoT), machine-to-machine (M2M) communications, connected consumer devices, smart buildings and services. To receive ALL 4 ISSUES per year of the printed magazine you need to subscribe. The price includes delivery to your chosen address worldwide. **BUY A 1-YEAR, 2-YEAR, or 3-YEAR SUBSCRIPTION**: **1 Year Normal price UK£60.00 NOW UK£51.00 for 4 issues** OR **2 Years NOW £102 (8 issues, save £18.00) SUBSCRIBE ONLINE**: **www.iot-now.com**

IoT connections to reach 83 billion by 2024

A new study from **Juniper Research** has found that the total number of IoT connections will reach 83 billion by 2024, rising from 35 billion connections in 2020. This represents a growth of 130% over the next four years. The research identified the industrial sector as a key driver of this growth. It forecast that this expansion will be driven by the increasing use of private networks that use cellular networks standards.

The new research found that the industrial sector, including manufacturing, retail and agriculture, will account for over 70% of all IoT connections by 2024. It anticipated that the emergence of cost-efficient private cellular networks would be a key driver of growth over the next four years, and expects that the recent increase in demand for private LTE networks will carry forward to private 5G networks as the cost of the technology decreases over the next two years.

The research forecast that the number of industrial IoT units in service will grow 180% over the next four years. “Industrial networks will need to scale rapidly as industrial IoT users adopt new technologies to expand the services available on their networks,” said research co-author, Sam Barker. “However, IoT platforms must ensure that the security processes can scale alongside this network growth.” ■

Device-to-cloud IoT platform services to hit US$18bn by 2026, says ABI

A new technology analysis report from **ABI Research** has projected revenue for device-to-cloud IoT platform services of US$18bn by 2026. IoT platform services now have drag and drop application development services, more sophisticated data and device management services, as well as managed security services. Software and services suppliers, a group that includes start-ups and cloud vendors, are expected to dominate revenue generation with nearly 67% of the total US$18 billion market. The supplier segment that has had the most impact on the competitive environment has been the cloud suppliers such as **Microsoft**, **AWS**, and others, which offer their own device-to-cloud IoT platform services. “Cloud services have become the centre of gravity for any IoT project,” said Dan Shey, the vice president of enabling platforms at the firm. ■

Liveable Cities selects Sierra Wireless LPWA solution for smart city applications

Sierra Wireless has announced that **Liveable Cities**, a division of Canada-based LED Roadway Lighting, has selected its low power wide area (LPWA) network solution to enable smart city applications.

Liveable Cities is using Sierra Wireless Ready-to-Connect HL78 modules for its SilQ Luminaire streetlight and the tool-less Sensor Platform (TSC) ANSI Controller, which can add radar, pollution and noise sensors to transform any streetlight into a network that provides data to cities to help them reduce pollution and keep citizens safe.

The Sierra Wireless LPWA solution connects sensors integrated in the Luminaire streetlight or TSP platform and securely transmits speed, pollution and noise data over cellular networks to Liveable Cities’ **SMARTLINX** cloud platform for analysis.

Ken Cartmill, vice president of product development, LED Roadway Lighting, said: “Municipalities are asking for solutions that will help them to make evidence-based decisions and measure the outcomes of their initiatives in real time. Using cellular was the best approach, and Sierra Wireless’ LPWA solution allowed us to get to market two to three months faster by streamlining our development and deployment process. Our customers can securely connect the TSP-Radar platform anywhere in the world.” ■

Alicia Asin, Libelium

Tutankhamun tomb turns to Libelium sensors to study cliff stability

IoT technology is preserving ancient Egyptian heritage under a geological research project to study cliff stability at Tutankhamun’s tomb.

A sensor platform developed by Spanish company, **Libelium**, has helped a team of geologists from York University in Canada and the University of Zurich in Switzerland to monitor the stability of the terrain over the tomb of the 18th dynasty of Pharaohs.

To measure the properties of the rock mass and the environmental conditions of the area, the researchers have developed a numerical model with different software and hardware tools, among which are Libelium sensors. The sensors include the platform of Libelium Plug & Sense Smart Agriculture Pro, a weather station, and a dendrometer, which is typically used to measure tree growth, modified to detect changes in fracture aperture.

“IoT technology can contribute to preserve historical and artistic heritage connecting the physical and the digital world through sensors that send the information to the internet and allow researchers to establish important conclusions for future conservation,” said Alicia Asin, the co-founder and chief executive of Libelium. ■

January and February 2020

It's free to be included in The Contract Hot List, which shows the companies announcing major contract wins, acquisitions or deployments. Email your contract details to us now, marked "Hot List" at **<j.cowan@wkm-global.com>**

Vendor/Partners	Client, Country	Product / Service (Duration & Value)	Awarded
City Fibre Council, UK	City of Wolverhampton	20-year contract agreed for full fibre network to connect council's public sector estate	2.20
CSG	Telstra, Asia-Pacific	Deal to provide billing and provisioning capabilities for Telstra Connected Car solution across the Asia-Pacific region	2.20
Geotab	General Motors, global	Integrated telematics system launched using the Geotab Integrated Soltuion to help General Motors meet all fleet connectivity requirements	1.20
IDEMIA	Fiat Chrysler Automobiles, global	Selection of IDEMIA's DAKOTA eSIM offering and subscriber management platform to enable lifetime connectivity choice for vehicles	2.20
IoTerop	Elvaco, Sweden	IoTerop's IOWA system selected by smart meter company to accelerate growth	1.20
Kerlink	UN Refugee Agency, global	Implementation of water management pilot project using Kerlink LoRaWAN gateways	2.20
Nokia	Telecom Argentina, Argentina	Nokia Worldwide IoT Network Grid (WING) chosen to enable telecoms operator to offer IoT services to enterprises across Latin America	2.20
Notion	Nationwide Insurance, USA	Provision of smart home monitoring technology to help alert customers via personal devices of water leaks, CO2 and smoke alarms and opening of doors or windows	2.20
Orange Business Services	Abu Dhabi Smart City Abu Dhabi	Development of bespoke app called IoT Cockpit through smart cities co-innovation programme	2.20
RealWear	Italgas, Italy	Italian gas distributor chooses RealWear intrinsically safe wearable device platform to help digitalise operations	2.20
Senet	Digital Matter, Australia	Partnership agreed to deliver LoRaWAN asset tracking and management solutions for developer of battery powered tracking devices and telematics software	1.20
ServiceMax	Smiths Detection, UK	Threat detection and screening technologies specialist selects ServiceMax to provide asset-centric field service management	2.20
Sierra Wireless	Electriq Power, USA	Deal agreed for home energy storage, management and monitoring company to take devices, network, services and software from Sierra Wireless	1.20
Sigfox	An Post, Ireland	Deal to use VT-IoT, Ireland's Sigfox 0G network provider's, tracking technology for parcels and ecommerce logistics	2.20
Spaceflight	Astrocast, global	New contract agreed for the launch of ten additional IoT nanosatellites	2.20
Swisscom and Telia	Sprint Curiosity IoT, Europe	New relationship agreed to expand Sprint Curiosity IoT across Europe	2.20
T-Mobile Austria and Ericsson	Stanley Black & Decker, global	T-Mobile Austria network and Ericsson IoT Accelerator selected by tool manufacturer's digital accelerator unit	2.20
Verizon	Honeywell, USA	Verizon Managed Connectivity LTE solutions selected to enable utilities to rapidly deploy LTE smart meters	1.20
Verizon	HERE Technologies, global	Verizon 5G and low latency mobile edge compute infrastructure combines with HERE Technologies' precise mapping to create new safety and navigation systems	1.20

Ericsson, T-Mobile Austria and Stanley Black & Decker speed IoT deployments

T-Mobile Austria's network, the **Ericsson** IoT accelerator for global connectivity and **Stanley Black & Decker**'s digital accelerator are collaborating to simplify and accelerate the global deployment of Stanley Black and Decker's connected equipment and services.

One example, already live in the field, is the Stanley Earth's farming project in India that is enabling farmers there to increase productivity and lower costs while offering a more sustainable alternative to an inefficient power grid or diesel-dependent water pumps for irrigation.

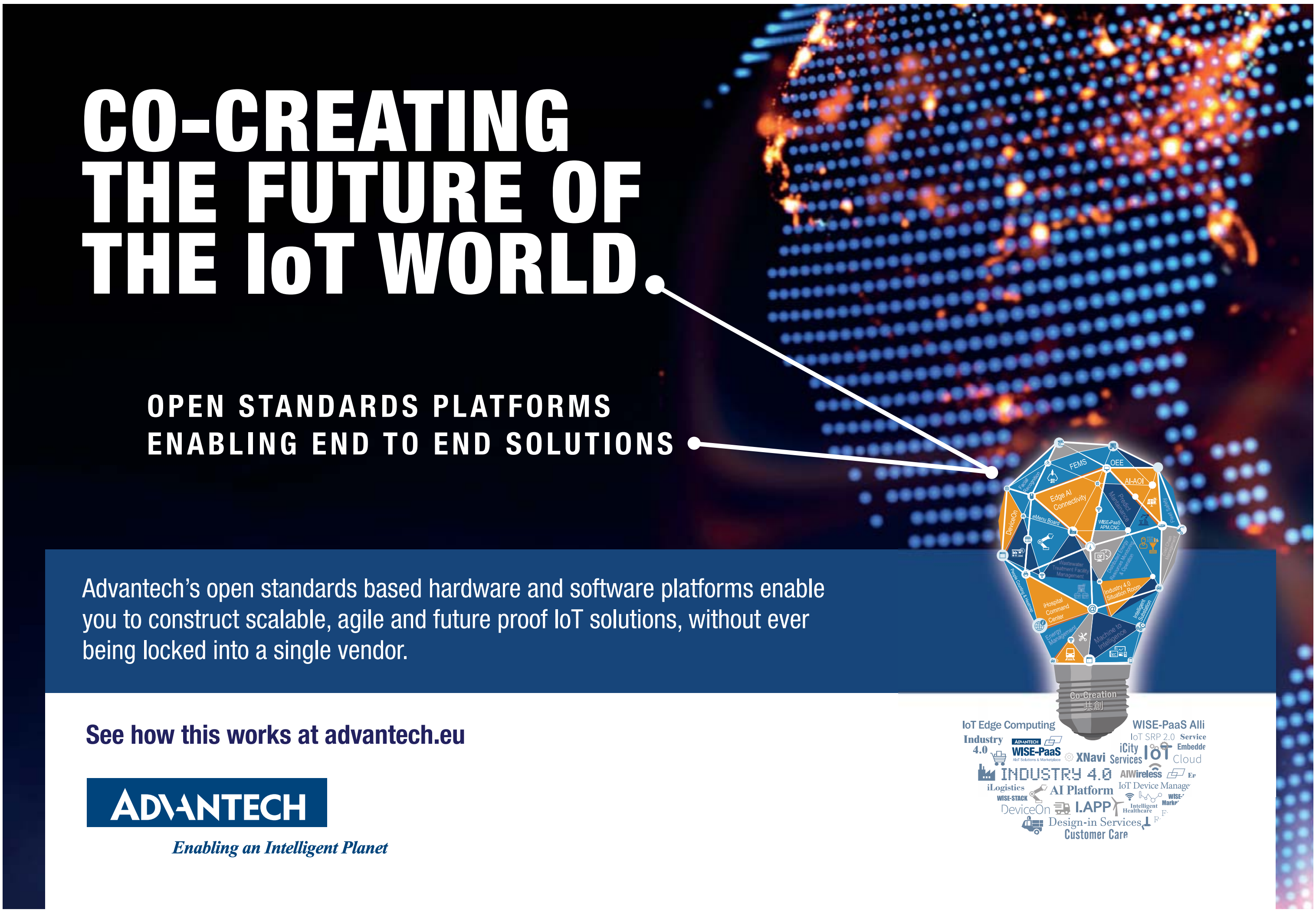
The five horsepower model of the NADI Smart Solar Pump is capable of delivering 100,000 litres of water a day, enabling farmers to manage groundwater resources better and irrigate more than five acres of land throughout the year for higher crop yields – all with the control from their mobile phone. In addition to improving the livelihoods of rural farmers, the smart, connected solar water pumps also have a positive impact on the environment due to low water and energy consumption.

Maria Zesch, T-Mobile Austria

Other Stanley Black & Decker use cases include connecting high-end heavy excavators for predictive maintenance, tracking and productivity monitoring, and connected security infrastructure for software updates, intruder detection and alerts, and appropriate responses.

Mike Keogh, president of Stanley-X, said: "We utilise cellular IoT along with renewable energy to expand workable areas for farms, simplify compliance to regulations, conserve natural resources, decrease dependency on fossil fuel, and increase revenue opportunities for farmers. We're proud to offer improvements to the quality of life of farmers while improving the environment."

Maria Zesch, the chief commercial officer for business and digitalisation at T-Mobile Austria, added: "Stanley Black & Decker demonstrates what an innovative company can achieve by combining its products with connectivity to have a positive and sustainable impact productivity and income of farmers. As an operator, we are delighted to help them use the connectivity and coverage to meet the needs of the local market and their project." ■



Haltian closes US$9.8m funding round to accelerate its growing IoT business

New investment worth €9 million in IoT and product development company, **Haltian**, is set to help accelerate the company's Internet of Things (IoT) business, enabling it to upscale and supporting development in international markets.

Now Haltian, which is headquartered in Oulu, Finland, expects rapid global growth in its IoT business and is focusing on selected business verticals including: smart facilities, smart washrooms and smart factories. The successful funding round was closed with Finnish venture capital company **Inventure**, employment pension company **Ilmarinen**, venture capital fund **Nordic Option** and a group of private investors through investment service **SijoittajaPRO**, including **Head Invest**.

"This funding round confirms that our strategy to focus on the selected IoT segments has proven to be the right one," said Pasi Leipala, the chief executive of Haltian. "We will now continue to further grow our business and develop the Thingsee IoT solution platform by improving our existing products, creating some new products and strengthening our presence in international markets as well. The message from the investors and customers has been extremely positive, and we feel very confident in going forward with our plans."

Ilmarinen's senior portfolio manager Ilja Ripatti, added that Ilmarinen is pleased to participate in Haltian's growth and become a shareholder in the company. "The market opportunity is vast, and the company has shown to be able to produce high quality solutions for large customers in interesting niche areas." ■

IoT agency SharpEnd wins investment from Guala Closures to scale connected packaging

SharpEnd has signed a strategic partnership with **Guala Closures Group**, a manufacturer of closures for spirits and wine, and a specialist in connected bottle caps.

The deal consists of the initial acquisition of 20% of shares of SharpEnd by Guala Closures for an undisclosed sum, with potential for further capital injections in the company. Guala Closures will remain a minority investor while Cameron Worth, SharpEnd's founder and current sole shareholder, will retain the majority of the company's shares. Guala Closures is a pioneer in connected closures with its NeSTGATE proprietary technology, enabling industrial use in supply chain management as well as consumer engagement programmes.

Founded in 2015 Internet of Things (IoT) agency, SharpEnd is known for being a pioneering creative technology partner with an appetite to push the boundaries of consumer engagement with a global client list including **AB-InBev**, **PepsiCo**, **Nestle**, **Unilever** and **Pernod Ricard**. This partnership enables SharpEnd to continue this journey and accelerate its growth strategy through Guala Closures' backing.

SharpEnd and Guala Closures already have a consolidated relationship based on their work together on NFC enabled closures. Most recently, they partnered with Californian wine brand **Boen**, the first United States wine brand to deploy NeSTGATE NFC technology. By simply tapping the cap with their smartphones, consumers are taken to an interactive farmhouse with a range of content experiences.

Guala Closures' investment in a strategic partner follows its intent to provide turnkey solutions to customers by becoming a technology integrator of connected packaging solutions. SharpEnd will scale up the development of its IoT software platform to be implemented by GCL's clients, extending to supply chain management, stock management, theft prevention and ultimately product security, anti-tampering and forgery prevention.

Paolo Ferrari, Guala Closures group chief marketing officer and M&A director, said: "SharpEnd's expertise will allow us to accelerate our Internet of Closures strategy development to help our clients provide better brand experiences to their consumers via the most advanced digital marketing solutions, turning data into valuable consumer insights." ■

Guala Closures specialises in connected bottle caps

Telenor, Sony and Ericsson team up to develop smart IoT healthcare devices

Mats Lundquist, Telenor Connexion

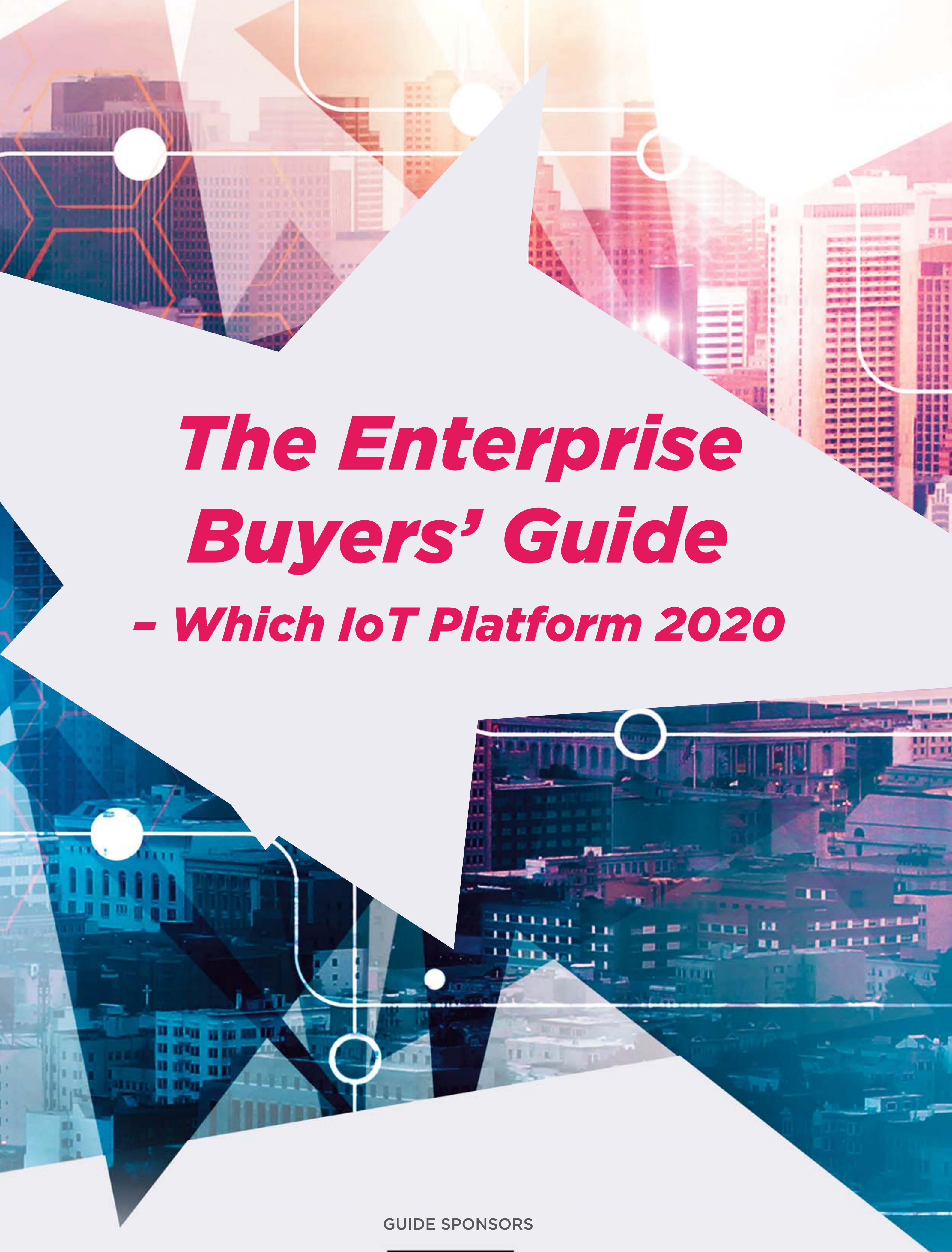
Using **Telenor Connexion**'s network, the **Ericsson** IoT accelerator for global connectivity, and **Sony Network Communications Europe**'s smart IoT services, the three companies are collaborating to enhance real-time location and tracking solutions for different sectors.

Ericsson IoT accelerator is the company's IoT connectivity and device management platform, providing enterprises with a unified solution that manages IoT operations of any scale, using worldwide mobile network infrastructure. More than 35 service providers, spanning more than 100 countries, are currently part of the Ericsson IoT accelerator ecosystem. The service currently enables reliable, scalable, and secure connectivity management of IoT devices to more than 5000 enterprises globally. With more than 50 million devices onboarded on to the platform including over three million eSIMs, the Ericsson IoT accelerator is a truly global platform.

Sony Network Communications Europe focuses on connectivity solutions and offers IoT cellular platforms such as Visilion and mSafety, providing cellular connectivity and wearable tracking devices.

Anders Stromberg, director, head of wearable platform department at Sony Network Communications Europe, said: "As the use of cellular technology matures, this can have a positive impact on the future of mobile health services and the safety and welfare of end-users."

Mats Lundquist, the chief executive of Telenor Connexion, added: "We are proud to be a long term partner of forward-thinking companies like Sony Network Communications Europe and to support their business growth and future IoT products and services." ■



The Enterprise Buyers' Guide – Which IoT Platform 2020

GUIDE SPONSORS

arm

flo. LIVE

MAVOCO

The Enterprise Buyers' Guide – Which IoT Platform 2020

If you are planning on connecting more than a single IoT device you will need an IoT platform but there are well over 600 available IoT platforms. Even as the largest players increase their market share, start-ups continue to emerge faster than existing start-ups are acquired or go out of business. Meanwhile, stalwarts continue to continue. They have years of experience, especially in whatever vertical sector they began in and those they may have expanded into over the years, writes Bill Ingle, a senior analyst at Beecham Research

With so many platforms to choose from and platform benchmarking services uncommon, diligence is required.

All IoT platforms enable some kind of remote monitoring application, but as IoT has grown so have the kinds of devices being monitored and related applications. Various platforms may be specialised for particular devices, functions, applications and vertical industries.

Data analytics, edge processing and edge analytics have become more prominent – many IoT platforms now take this into account.

Is a platform provider viable as a business? Few would choose a provider that might go out of business after an IoT project investment, but platform providers may originate from successful custom IoT projects. If your project is similar to one of those projects and the provider, however small, is clearly succeeding – they may not need vast numbers of customers – their platform is worth considering.

Time has proven that purchasing an IoT platform - whether as a one-time purchase or as a software as a service (SaaS) package - beats the alternative: Tasking your in-house development team with creating one. Doing this has often led to IoT project failure. Some customisation will inevitably be required, but that's a much smaller challenge.

What are your business goals? How will your IoT project and chosen IoT platform make them achievable? Do platforms specialised for your industry and/or applications exist? If not, does a provider work closely with appropriate partners?

Elements of an IoT solution

For any IoT solution involving connected devices, there are three key elements that must be managed:

1. **The connected device** with sensors measuring temperature, location or some other parameter. Also an asset such as a vehicle that has many sensors – the edge devices. Device management may include device identity in the network, provisioning for use of the network and secure over-the-air update of device firmware. These are part of device management.

2. **The connection** from the device to a server to which the data is transmitted for processing. The connection may be short-range or long-range, wired or wireless, or a combination. The server may be at the network edge or in the cloud or in both. Areas that may need managing are connectivity options, coverage, network protocol support and billing or usage. These are part of connectivity management.

3. **The data generated** needs to be stored, processed – sometimes in real-time – either on its own or in combination with other data to create results. Additional areas that need managing include workflow handling, visualisation, orchestration and data analytics. These are part of data management, which may happen at the edge or in the cloud depending on the particular application requirements.

In addition, an application is required to make specific use of the data created. All of this must be carried out securely so that the device itself and anything using the data, such as a controller, is not compromised. Security needs to bind together all the other elements so that potential attack surfaces are minimised.

These elements are illustrated in **Figure 1**, where they form a stack that sits above

beecham research

Shaping the IoT future

the sensors, devices and gateways at the network edge and network infrastructure.

These are also the main elements of an IoT platform, a software middleware suite that facilitates secure monitoring, control and analysis of device and sensor behavior in the field. It provides an enabling layer between connected devices/sensors and user applications.

IoT platforms have been created for the express purpose of reducing the time and cost of getting new IoT solutions built and implemented. An IoT platform takes advantage of the fact that the majority of what is needed in IoT solutions is the same and does not need to be redeveloped for every application. In theory, at least 80% of IoT solutions are made from common parts, and can be made available through an IoT platform. The platform then also provides the means for customising and configuring the solution – the other 20% – for a specific application.

Experience has shown, however, that platforms with a narrow market focus require less customisation – say 10%, with more horizontal platforms – those offered for multiple sectors and applications – requiring more customisation – say 30%.

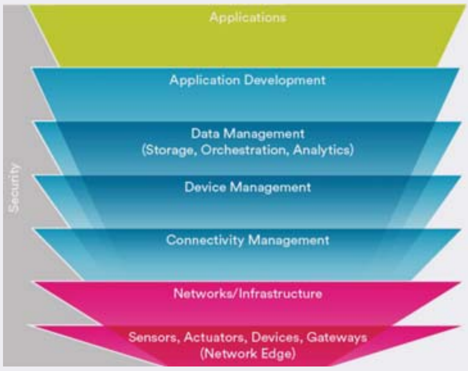


Figure 1: Elements of an IoT Solution

©2020 Beecham Research

IoT needs a secure management platform to cover everything from silicon to insight

As networks transform, new devices come to market and data is ingested from new sources, Robin Duke-Woolley, the chief executive of Beecham Research, interviews Charlene Marini, the vice president and general manager of devices in the IoT Platform business unit at Arm. Deriving the full value and benefit of trillions of IoT devices will require a platform for data, connectivity and device management that brings together a large ecosystem of developers in a secure yet simple to use way, she says

Robin Duke-Woolley: Arm has traditionally had an extensive ecosystem. How has this been adapted to address the opportunities of IoT?

Charlene Marini: We are targeting the scale of IoT. Our investments in processor design, software and services are focused on how we enable the Arm ecosystem of chipmakers, developers and original equipment manufacturers (OEMs), as well as enterprises and consumers to derive the most value from the wave of connected devices coming. Along with our device management capability – enabling secure control and data access – we also provide connectivity as part of an overall intelligent connected device platform. We have focused our investments on how to enable the broadest range of devices; heterogeneous networks and systems, and how organisations can obtain insights from the harvested data. Today, we have more than 1,000 customers and 150 ecosystem partners. That includes silicon suppliers, device suppliers, system integrators, application providers, as well as a robust and growing developer ecosystem of more than 425,000 third party developers. The bulk of these partners are in embedded design, but there's also a growing emphasis on cloud applications. ▶

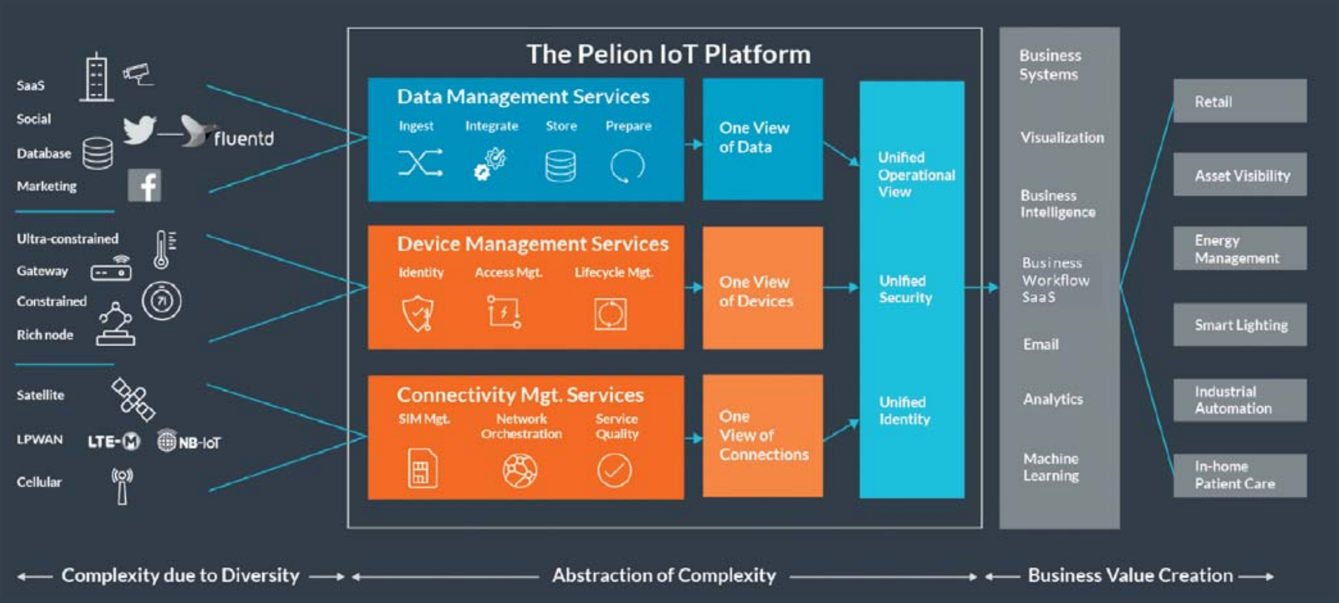


Figure 1: Pelion abstracts complexity to deliver insightful data

Device management brings the capability to manage firmware and application updates together with insights into how devices are performing

RD-W: Where does Arm aim to add new value for your customers?

CM: Figure 1 shows where we are in terms of the value we provide to our customers. The three services of Connectivity Management, Device Management and Data Management are the product lines within Arm Pelion and revolving around that centre is the device ecosystem and our activities to enable a vast range of secure, intelligent devices.

Device management brings the capability to manage firmware and application updates together with insights into how devices are performing. From a visibility perspective, knowing what's on your network, the firmware and the devices, is the basic level of understanding that's needed. Then you need to know how your devices are operating – normal or a potential problem? The third level of need is the ability to take actions based on your observations; you must be able to act at a device fleet-wide level as well as on individual devices.

In addition to value gained at the operational level is the benefit of value-added services. Robust device management allows you to add new applications; features and functionality securely to a device in the field, and apply new policies for enhanced functionality through the application. These are the two main areas adding value in the market today: holistic operational integrity and the building and adding of services which enhance the value of our customers' products.

RD-W: The Pelion IoT Platform also includes a Data Management component. Can you say more about your data management capability?

CM: One of the things that is very attractive to our customers is our data capability, both the quantity and velocity of data that we can ingest and process. To give an analogy, similar to connectivity and device management, a lot of value in data management is in how you can abstract insights from heterogeneity. You are likely to have multiple sources of data, all with individual characteristics in terms of velocity, how the data is organised, and so forth. Fundamentally, the data management service we offer enables broad data ingestion from different types of devices and the ability to mix that data with other types of enterprise data. We believe in most IoT use cases, device data will need to be combined with other data to get to the core insights, so enabling easy ingestion and understanding across different data types is essential.

RD-W: What other types of data do you mean?

CM: If we take a factory use case; that data might come in the form of system records, or weather data, it might even be supply chain data being fed into the factory system. If we take more of a consumer view; that data might be social media or data from other properties that the brand or consumer device manufacturer offers.

What we give our customers is a very sound data management platform capable of ingesting any type of data for their algorithms, to store that data and present it consistently to different types of tools they want to deploy. We have some tools that we integrate with, but there are also other tools, and partners, that our customers might work with on the pure analytics front. Enabling the broadest array of tooling and analytics is really important for all of our customers. ▶

> *There are usually multiple workflow outcomes that our customers are trying to achieve so having off-the-shelf plug-ins for those capabilities is essential for integration*

RD-W: Can you name some of those tools?

CM: One is Treasure Boxes which enable our customers to use pre-formed analytic models, or they can create their own. It is offered by Treasure Data, the enterprise data management company that Arm acquired in 2018. We also offer tools such as Jupyter Notebooks which are a standard open source way for data scientists to collect and organise their library of models.

RD-W: Apart from the enablement of data analytics and the processing of the data, what else does Arm provide?

CM: The other important aspect is enabling multiple different outputs from data. There are usually multiple workflow outcomes that our customers are trying to achieve so having off-the-shelf plug-ins for those capabilities is essential for integration. If you think of email, it might, for example, be an alert system. You want to make sure you can generate those automated emails. It might be things like CRM, different business intelligence tools, or visualisation tools. We provide plug-ins for those and ways to modify those plug-ins that enable those integrations more easily.

RD-W: Those are rules-based alarms that send out alerts when a threshold has been reached?

CM: Yes. It is important that our services are generally applicable. We tend to focus on enabling use cases end-to-end and currently target areas such as retail, utilities, industrial automation and energy management, including metering. For all of these, we've made further specific investments.

RD-W: Are those four the leading sectors for Arm?

CM: In addition to those, we work in smart lighting and smart spaces – touching smart buildings and smart cities. This is about how you gain insight from spaces. We have been focused more on indoor spaces to date, but the technology is just as applicable to outdoor.

RD-W: Is this in-building lighting management only?

CM: We have found that there is a strong need for more occupancy and environmental management. We are working with Prolojik around lighting management. We are also enabling workspace insights through our Space Analytics solution. This includes providing insights and understanding around occupancy, coworking, or office space - such as where people tend to congregate. That may be because the lighting is better in some places, or it may be due to other environmental factors. What often happens is that companies install one type of sensor capability for their primary use case. For office buildings, many deployments start with lighting as part of an energy management strategy. But the lighting that was installed had other sensors as well, such as occupancy sensors used to determine whether a light should be on or off. From this latent capability, you can then gather other useful data for your building planning. You might find five conference rooms are hardly ever used so those low occupancy rooms may not all be needed. That is where you start to get derivative value from the data. So smart lighting might be the initial IoT motivation, but it becomes clear how the data being gathered can also be used to create new insights.

RD-W: When we talk about other kinds of sensors, can you indicate what sort of connectivity you are thinking about?

CM: Connectivity varies a lot by use case as well. Broadly, with low power wireless and cellular we are seeing increasing interest around movable applications. That is a very interesting area for us. We think that is going to continue to gain momentum over the next year. The second area is mesh, especially with utilities for some spaces applications. Thirdly, we are also seeing demand for higher data rate cellular for backhaul in these applications. As people build out their sensor capabilities and sensor network in a building or field, higher data rate 4G cellular is the gateway for backhaul.

RD-W: So how would you summarise what Arm is offering for IoT solutions?

CM: The main thing for us is providing the ability to deal with complex heterogeneous data environments and enabling IoT deployments that are easily-scalable. The fact is that organisations' IoT networks are going to be different, the devices making up those networks are also going to be different, and the variety of data that must be ingested, aggregated and understood will be very different. We think this is where Arm adds significant value. We have unique device understanding, with 160 billion Arm-based chips shipped over the last 30 years. We also have world class secure device management, connectivity and data expertise. That combination of knowledge puts us in a great position as we understand the device universe, what will be possible in the future, and how to manage and get value from the resultant data.

Charlene Marini, Arm

For me, this is the most exciting time for the IoT – companies are moving quickly from research and planning into early and, for some use cases, extensive deployments. The question is whether everyone will succeed in realizing the benefit of intelligent, connected devices? It's a question we're going to help answer in as many ways as possible as we know the IoT is absolutely not about one size fits all. ■

www.arm.com

The IoT platforms to watch in 2020

Monitoring the well over 600 IoT platforms in existence, including new entrants and those that fade away or are acquired even as the overall number continues to increase, is not a trivial pursuit, reports Beecham Research

Not all platforms are the same; they can be differentiated in a number of ways. They may be specialised for particular functions, for specific vertical industry sectors and/or for specific applications. They may be offered by very large corporations with massive resources or by start-ups created after a successful IoT project. They may be offered by firms in business since the days of M2M, having gained years of experience.

The very large companies offering platforms continue to gain market share. Most of them initially acquired smaller players and gradually expanded their offerings, especially as data analytics and digital transformation acquired an increased emphasis. Some are also the major cloud providers.

These include **AWS**, **Microsoft**, **Google**, **IBM**, **Oracle**, **SAP**, **Siemens**, **HPE** and others. Here are two quick sketches to describe how approaches differ:

AWS IoT offerings continue to multiply, with its **IoT Core** managed cloud platform central to AWS and designed to work with the company overall. A year ago, AWS IoT was focused on connected home and industrial IoT solutions. It has since added a commercial area, which includes traffic monitoring, public safety and health monitoring. AWS IoT divides its services into analytics services, connectivity and control services, and device software. AWS IoT Greengrass extends AWS to edge devices enabling edge processing.

New features continue to accrue to Microsoft's **Azure IoT** as well, reflecting the US$5bn investment announced in 2018. **Azure IoT Hub**, the company says: "provides a cloud-hosted solution backend to connect virtually any device. Extend your solution from the cloud to the edge with per-device authentication, built-in device management, and scaled provisioning." **Azure IoT Edge** is built on Azure IoT Hub and runs on edge devices. Microsoft offers a full range of analytics services. **Azure stream analytics** is specifically designed for "real-time data stream processing from millions of IoT devices," the company states. Focus areas for Azure IoT include discrete and process manufacturing, energy, healthcare, retail and transportation and logistics. ▶

Just a few of the hundreds of newer and/or lesser known IoT platforms described by their makers:

AssetWolf Cloud-based IoT platform: "facilitates fast prototyping for designers and developers. It allows you to connect a device to the cloud and quickly develop an application, with data analysis, event/alarm triggers, user-privilege access control and more."

Axonize: "Based on six breakthrough technologies, our no-code solution is unlike any other on the IoT market."

Blynk: "A hardware-agnostic IoT platform with white-label mobile apps, private clouds, device management, data analytics, and machine learning."

CENTERSIGHT: "Use the CENTERSIGHT IoT platform to make use of edge computing, infinitely scalable middleware and tailored apps to provide an unsurpassed user experience."

Initial State – IoT Platform for Data Visualisations: "Stream data from your device and services to beautiful cloud-based data visualisations. "

Altizon – Datonis Industrial IoT Platform: "Cloud based industrial IoT platform that connects your machines, your people and your processes to drive digital transformation."

Other platforms to watch

SoftBank's **Arm** announced its **Pelion IoT platform** after acquiring **Stream Technologies** for connectivity expertise and **Treasure Data** for data analytics capability. As a result, Pelion offers a combination of connectivity management, device management and data management – a full IoT stack – with the ability to choose which services are needed for a particular requirement. Focus areas include smart buildings, utilities, telecoms, retail and logistics.

Cisco's IoT Control Center is said to have more than 100 million M2M/IoT connections, its worldwide customers including major telecoms and original equipment manufacturers (OEMs). **Cisco Kinetic**, a second IoT platform, is focused on connecting devices and acquiring and using data from them for business outcomes in multiple industry sectors.

IoT Control Center is a connectivity management platform that competes with **Ericsson's IoT Accelerator**. Note another developing player in this platform area: **Mavoco**, with its Connectivity Management Platform (CMP), primarily working with network operators. See also the **FloLIVE** Global Connectivity Management Platform.

Cellular module, gateway and router supplier **Sierra Wireless' AirVantage** platform, part of the Sierra Wireless Cloud and Connectivity Portfolio, continues to evolve and now offers a range of optional micro services that can be selected to meet particular customer needs. This is complemented by **Octave**, an edge-to-cloud solution for connecting industrial assets and acting on data extracted from them.

Another major IoT cellular module manufacturer, **Telit**, offers **OneEdge**, an edge-focused software system that provides device management, connectivity management, and application enablement features all based around the cellular module itself.

PTC's Thingworx Industrial Enablement IoT platform offers multiple connectivity options, application development tools, analytics, and digital twins and AR capabilities. PTC's strategic partnership with **Rockwell Automation** strengthens this platform's position in industrial IoT. ■

Pelion Device Management lays the foundation for Taiwan's Smart City

When the City of Taipei put its smart lighting solution out to tender, industrial and embedded systems developer AAEON turned to Arm for a solution that not only met the brief, but offered a sustainable solution that can be adapted to scale for the future

City officials were looking for a reduction in energy costs, infrastructure life cycle cost and greater control over their utilities by deploying IoT nodes to 4,000 lampposts that would sense ambient light levels and attenuate output to reduce energy consumption.

A stringent security specification combined with the burden of developing its own real-time operating system (RTOS) and IoT platform led AAEON to look for partners who could reduce its time to market and offer a solution that could be easily replicated in other South Asian cities.

Working with the Pelion IoT platform resulted in reduced complexity and time taken to design, deploy and manage a city's device estate. The AAEON lighting node allows facilities managers to control Taipei's IoT-enabled lighting infrastructure from the Pelion Device Management platform by simply plugging into a NEMA socket controller that is found on most streetlights, enabling remote administered applications that instruct lampposts to power up, attenuate, or switch off lights during off-peak hours.

"Mbed OS and Pelion IoT Platform provided us with a simple route to delivering the city's digital transformation," says Kevin Ting, the senior manager in the design manufacturing service at AAEON Technology. "We particularly liked how the IoT Operating System (IoT OS) can be ported across different Arm microcontrollers and different product families by using readily available libraries. Isolated security in-kernel and secure communication channels over the internet offered peace of mind for Taipei's essential infrastructure."

City-wide cost reductions

The Taipei taxpayer benefited from far more than just lower energy bills. The life cycle cost of each lamppost is reduced by relaying live insights that can reduce downtime through preventative maintenance and eradicating the bureaucracy of reporting and processing a failed light.

"Repair costs for a failed light can amount to twice the cost of the light itself by the time you factor in a night shift of engineers, public liability insurance, and the disruption caused by road closures," adds Ting. "Thankfully the insights provided by Pelion minimise all these factors by optimising predictive maintenance planning that pinpoints failures on a closed street before they happen, dramatically reducing repeat visits to the same location." ▶

SPONSORED CASE STUDY

Company-wide cost reductions

AAEON was quick to divest the burden of developing a secure RTOS and IoT platform and identified Arm's Mbed OS and Pelion IoT Platform as its preferred choice to help its team deploy 4,000 nodes far sooner than developing their own proprietary solution.

AAEON utilised a range of Arm-based solutions including:

- A Cortex M-based STM32F429IEH6 chipset for the MCU
- Ublox SARA-N410 NB-IoT communication modules
- Mbed OS version 5.11.5
- Pelion Device Management Platform Toolchain including Secure Device Access and Mbed Compiler

Pelion Device Management acted as the single dashboard that takes care of all ongoing city-wide management, allowing remote firmware updates to be administered from a central location and Pelion's Secure Device Access (SDA) functionality that grants third party facility managers and engineers access at a specific time with the ability to read device data without the option to corrupt or overwrite it.

A Bright Future for Taipei

AAEON is already using Arm Cortex-based processors to help facilitate Taipei's smart city vision, whilst administering additional functionality and frictionless software updates thanks to the Pelion IoT Platform.

Pelion's streamlined provisioning process will help deploy an additional 25,000 IoT devices across the city by the end of 2020, forming the backbone of the city's IoT infrastructure and enabling additional features including:

Data-driven Insights

- Live weather conditions
- Air quality
- Noise conditions
- Live traffic updates
- Digital signage
- Provisioning access to public networks

Features

- Free Wi-Fi
- USB/wireless charging
- UPS battery backup
- Interactive touchscreen displaying insights
- Digital signage
- Emergency intercom and video call

"Partnering with Arm has meant we've reached market far sooner than expected, offered additional functionality that helps generate new revenues for AAEON that can be repeated in cities around the world," says Ting.

www.pelion.com/iot-device-management

> ***AAEON was quick to divest the burden of developing a secure RTOS and IoT platform and identified Arm's Mbed OS and Pelion IoT Platform***

IoT demands a single-source global connectivity solution for global customers

As volumes of IoT connected devices start to increase, the challenges of global connectivity require a connectivity management platform to handle the scale of connection numbers and sheer disparity in requirements from mobile operator to mobile operator and country to country. Here, Robin Duke-Woolley, the chief executive of Beecham Research, speaks to Anton Cabrespina, the chief commercial officer and founder of Mavoco, to understand how communications management platforms are underpinning the next wave of IoT growth

Anton Cabrespina, Mavoco

Robin Duke-Woolley: How did Mavoco get started in IoT?

Anton Cabrespina: Originally we were called Machine and Voice Communication, which was shortened to Mavoco. The company was founded in 2010 and started doing what we do now in 2014. We started developing the software then and also in parallel founded a service provider – a mobile virtual network operator (MVNO) for IoT – to sell the IoT platform and connectivity services to enterprise users. Our main market is now IoT connectivity management platform (CMP) services to mobile network operators (MNOs). This took a little while to go through the various approvals for each MNO. The platform became commercially available in the fourth quarter of 2015. First implementations with MNOs came in 2018, which are provided through our network infrastructure partner.

RD-W: So what is your vision for the IoT market?

AC: We believe that we are still in the early days of IoT and that there will be huge steps forward. Also that when you connect anything, the value of that thing increases massively. That was true for PCs and it's true for connected devices. Looking into how this is evolving, we see several major trends.

There is a big international aspect. The telecoms market is structured in a local way. Most of the telecoms business is for personal communications and the primary aspect of that is for people to use mobile phones in their own country. IoT, on the other hand, is primarily an international business.

Dealing with SIMs internationally is complex for companies and will become even more so with 5G. Most devices will come with connectivity already embedded from the factory. This has a major impact on local MNOs. If you are a large international device manufacturer, you cannot deal with the complexity of working with many MNO partners. You need to have a global solution for global customers from a single source. This is a key driver for the future. This is not just about the connectivity itself, it is the connectivity management which is also very fragmented. An industrial company cannot afford to manage many platforms. They need to manage from a centralised platform and this is what we have invested in from the beginning.

RD-W: How do you see user needs evolving?

AC: At first, companies that took up IoT needed to do so as part of their product offering. For example, a tracker unit needs to be connected in order to carry out its function. The growing trend is that industrial companies are now using IoT to monitor, support and improve how their products are being used beyond those that need IoT for the product to exist. There are several reasons for this.

One is that they want to know how the service is being used so they can improve it – they can customise it. They can more efficiently adapt it to how their consumers are using it. Also, they want to change their business model, to go from where ▶

SPONSORED INTERVIEW

they just sell the product to selling a service – a move from capex to opex.

In moving from sale to subscription, they do not have the tools for that. They need be able to onboard the customers, manage the lifecycle, define how services are being charged, create products that are based on usage, bill for them and so on. That's a lot they do not have right now. Our CMP is already capable of doing all this and we are evolving it further.

RD-W: Are there other issues that your CMP can help manage?

AC: Yes. For example, in Brazil there is this permanent roaming issue. It means the MNOs in Europe need to partner with a Brazilian MNO for connectivity in Brazil. Even if they use an eSIM, they can change the profile from Europe to Brazil but then cannot manage the SIM from the same platform used in Europe. If the profile has been changed, then you need to use another CMP from the Brazilian service provider. That will involve different application programme interfaces (APIs), different language and different currencies for tariffs.

We offer an alternative – a single pane of glass as an overlay. Our platform can connect directly into the core network of an MNO and can also be integrated on top of other CMPs. It means that for an industrial company with several million SIM cards, they could use our platform to manage their SIM cards in a consolidated way. This is our overlay capability.

This is also interesting for MNOs because they had either multiple CMPs in place – many have bought multiple CMPs over the years – and many have found themselves with several CMPs and then not able to offer consistent services to all their customers. They are looking at our platform to provide an overlay on top.

RD-W: How many MNOs are you currently working with?

AC: At present, we have implemented in 11 networks and are planning to double that in the coming months. We have several in Asia, several in North and South America and also in Europe. ■

www.mavoco.com

The growing trend is that industrial companies are now using IoT to monitor, support and improve how their products are being used beyond those that need IoT for the product to exist

IoT connectivity and subscriptions platforms evolve and will fragment throughout industries and use cases

IoT markets are and will become more and more segmented over the next few years. As every industry develops, the Internet of Things (IoT) won't simply remain the same as it is today. The entire IoT industry will develop into many subsegments, each with different requirements to cover specific needs

This fragmentation into categories such as: massive IoT, mission critical IoT, telemetry IoT, industrial IoT or many other variations will create enormous challenges for the IoT ecosystem. Therefore, platforms such as **MAVOCO**'s MAVOCloud CMP - connectivity management platform, which helps telecoms providers to manage, bill and analyse connectivity services for IoT devices will step up to fix those challenges. This also applies for subscription management platforms which are the basis for any recurring business model nowadays.

Current connectivity management platforms are already a part of the telecoms industry transformation. Those platforms help providers to evolve their business models from delivering connectivity for human-to-human interaction to connectivity for IoT devices and services. A simple example for this kind of change are SIM cards that deliver connectivity for 50 cents. They can certainly not be compared to SIM cards that cost €1,000 per year. Businesswise, it's not possible to expect and deliver the same services, technology and platform capabilities at these vastly different price points. As more CMPs come to market, there will be a higher mixture of offerings for low, mid and high average revenue per user (ARPU) SIMs. Not every telecoms provider is currently using a CMP and therefore is partially not able to handle all the IoT business case mentioned above with the same technical ability and to do so profitability.

New opportunities for CMPs in different other areas

In 2018, **McKinsey & Company** reported the global IoT market was valued at US$190bn. By 2026, it is forecasted to be worth US$1,1bn. This extraordinary and rapid growth will be evident in 2020 even though the coronavirus crisis will affect the numbers a bit and postpone some growth to the beginning of 2021. Nevertheless, this growth will impact the entire industry and create opportunities for enterprises but also cause massive challenges.

On the one hand there is a significant driver, on the other hand there is a big challenge. To reduce the complexity, globally active companies often want to deal with only one network operator, that offers worldwide connectivity at a consistent quality and price level. Such a comprehensive service is not widely available, therefore the setup of global IoT business solutions is a complex issue for the enterprises as well as for the network providers. It requires a large number of capabilities such as those provided by MAVOCO's MAVOCloud.

Smart cities, utilities and the transition into the subscription economy

Grand View Research has reported that current urban population of 55% is expected to increase to 68% by 2050, so cities and providers within those ecosystems will face massive challenges. Therefore, the demand for sustainable infrastructure owing to increasing population and urbanisation has become a key driver for the growth of the market. The smart city market was valued at US$624.81bn in 2019 and is expected to reach a value of US$1.7 billion by 2025. Areas like smart surveillance, e-mobility, smart lightning and smart infrastructure will be some key areas within this growth. ▶

Let's look at some sectors such as energy, water, waste collection and break down the challenges, opportunities and the use of CMP software, which, for example, enables the transition to the subscription economy and creates new business models and opportunities in these areas.

Big energy data and information collection

Demand response information is one area for utilities, which might be impacted because of the growing amount of real-time energy consumption data. To understand the energy demand of, for example, a building or a city and to create automated reports, real-time billing, as well as analytics that make the data available to other parties or systems are required. This massive challenge can be solved by using IoT tools such as subscription management platforms which can provide all those important capabilities mentioned above.

Predictive energy supply and energy community billing

Local energy suppliers need to collect real-time energy consumption data through various meters within a community. Those can be so-called prosumers producing their own energy by using photovoltaic panels and selling the energy back to the utilities, for example, or even sharing it with their neighbors or other stakeholders. The major complexity is to set up automated billing processes, to notify customers when a predefined level of power consumption has been reached as well as to alert them in the case of abnormal patterns deviating from their historical consumption.

E-charging Infrastructure for urban E-Mobility

The growing number of electric vehicles (EVs) especially in urban areas requires a rethink regarding the management and billing of those solutions and the integration and merge of multiple systems. There will be a necessity for single platforms to monitor consumption, manage subscriptions, create various pricing models, track charged energy and execute billing duties. This will make life for municipalities as well as the customers and users way easier.

Current IoT and CMP platforms need to deliver technical as well as commercial capabilities to the entire IoT value chain and enable the so called B2B2X approach. This includes the management of subscriptions, the subscribed products and the usage. When it comes to subscriptions – for telecoms or non-telecoms purposes - the MAVOCO MAVOCloud SaaS Subscription and Billing platform delivers those important features to cover all the required functions such as:

Subscription management

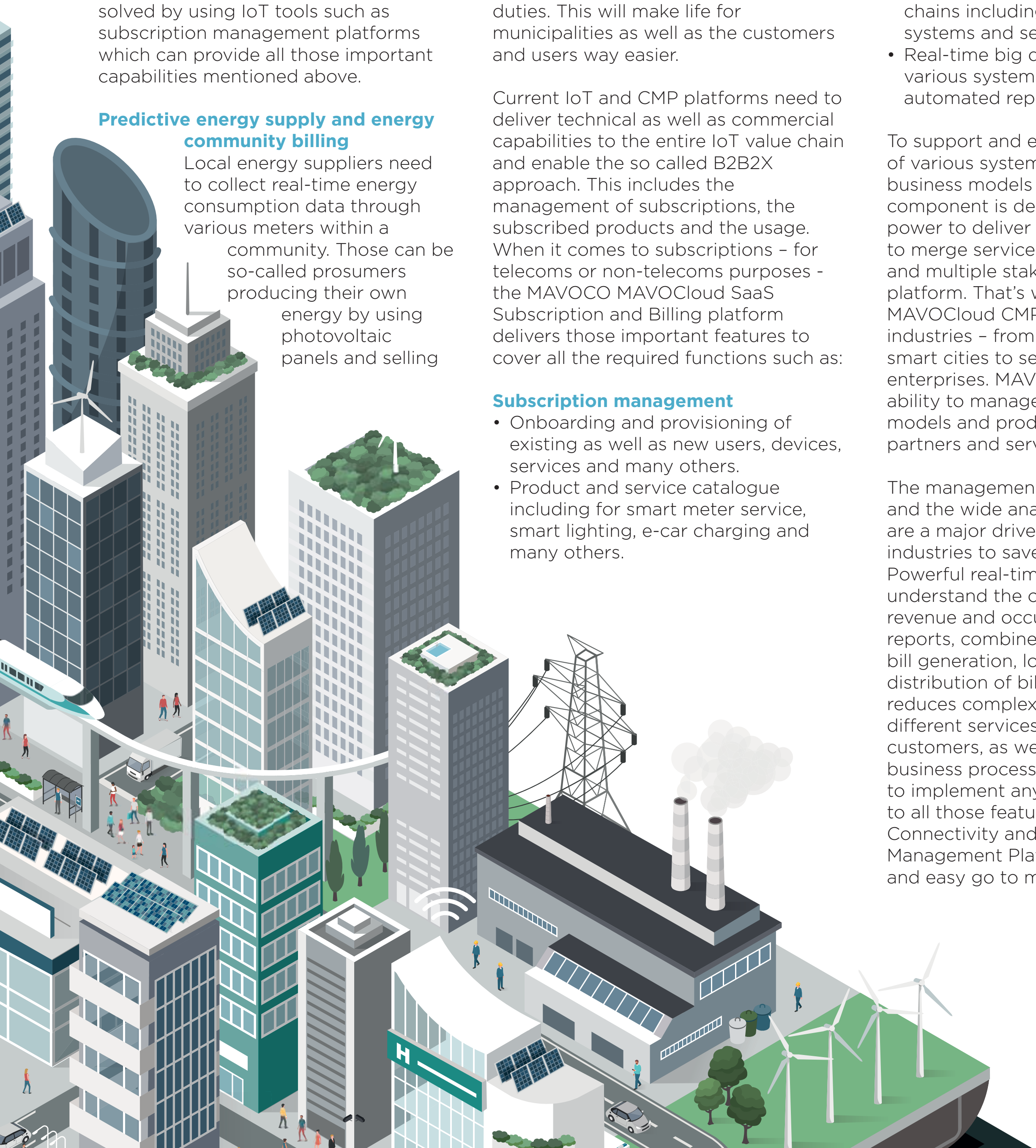
- Onboarding and provisioning of existing as well as new users, devices, services and many others.
- Product and service catalogue including for smart meter service, smart lighting, e-car charging and many others.
- Setup specific price plans based on events, time, volume and charge per kW/h, meters, minutes, kilobytes or any other relevant unit.
- Generation of automated and consolidated bills of all subscribed services.

Billing, reporting and integration

- Overview of available data, tariffs and subscriptions.
- Real-time data of consumption and the resulting cost at pre commission, end customer price and other stages.
- Customer self-service including start, cancel, change or renew subscription – simply manageable throughout one platform.
- Facilitating of multiple billing and payment models such as pre-paid or post-paid, monthly fees, recurring payments and many more.
- Implementation of complex value chains including various stakeholders, systems and setups.
- Real-time big data collection from various systems, data analytics and automated report generation.

To support and enhance the integration of various systems and new disruptive business models an additional core component is desperately needed: The power to deliver functionality in order to merge services and manage partners and multiple stakeholders from a single platform. That's what MAVOCOs MAVOCloud CMP provides for multiple industries – from telecoms, utilities, smart cities to service providers and enterprises. MAVOCO provides the ability to manage multiple business models and products from various partners and service providers.

The management of price plans, tariffs and the wide analytics functionalities are a major driver that helps multiple industries to save costs and time. Powerful real-time analytics help to understand the consumption, expected revenue and occurring cost. Multiple reports, combined with an automated bill generation, local taxation and the distribution of bills saves time and reduces complexity. The integration of different services, organisations and customers, as well as the necessary business processes offer the capabilities to implement any business model. Due to all those features MAVOCO's Connectivity and Subscription Management Platform enables a quick and easy go to market strategy. ■



Welcome to the era of software-defined IoT connectivity

IoT organisations need to access seamless, cloud-based network solutions for IoT connectivity on a global scale in order to reach their targets of hyperscale device deployments. Nir Shalom, the chief executive of floLIVE, tells Robin Duke-Woolley, the chief executive of Beecham Research, that control of the technology stack, the connectivity and the data from end-to-end is vital to provide the connections customers with simplicity of management, a ubiquitous global footprint and access to the network technology of their choice

Nir Shalom, floLIVE

Robin Duke-Woolley: You were previously in a senior position at AT&T, why did you leave there to join floLIVE?

Nir Shalom: I saw three things coming together with floLIVE. Firstly, a product market fit that made a lot of sense to me with an immediate understanding of the problem that the company was trying to solve and how the solution met that need. I have seen many start-ups while at AT&T – and with many I could see that they had an interesting idea but it didn't really meet a specific need. With floLIVE I saw a company with an intelligent vision, one that makes sense and solves problems for real customers.

Secondly, I noticed that floLIVE, unlike many of the companies in this specific field of global connectivity and networking solutions for IoT, owns the entire stack of technology that is required to build a solution from A to Z. This is very important. We talk about the market and we talk about technology but to really be able to serve customers in a valuable way you need to control the technology stack. floLIVE has all the pieces in place to do this.

The third thing comes down to the company culture and passion. I came across a set of founders who truly understand the market and have a great vision and are great people to work with.

RD-W: So, what exactly does floLIVE offer?

NS: From a customer perspective, we see a lot of manufacturers that would like to move up the value chain and keep in touch with their devices throughout the product lifecycle. Manufacturers understand that to improve their market position and provide the best customer service, their products need to work properly at all times, and the only way to do that is to control the technology stack, the connectivity and the data. Many customers want this globally and to have it provided in a simple way. At present, global manufacturers have two options. The first option is to go with a global subscriber identification module (SIM) from one operator, which results in vendor-lock in. That operator may have permanent roaming issues, it may not be sufficiently secure in each country when roaming, and you may want to build a relationship with another operator and be unable to explore that.

The second option is to integrate with multiple operators. However, while integrating with one operator is complex enough, integrating with several gets even more complicated and confusing. Each have their own different platforms, support systems and ways of doing things.

What we offer is a global, cloud-based and software driven connectivity and networking solution for IoT that allows such manufacturers to connect their devices anywhere in the world reliably and manage them simply using a set of representational state transfer (REST) application programme interfaces (APIs) or a simple graphical user interface (GUI). Our technology allows us to support any cellular technology from 3G, and LTE, to narrowband IoT (NB-IoT), LTE-M and 5G.

Our unique architecture is achieved by deploying a set of core networks developed from the ground up in various regions worldwide. We then interconnect all of these networks into a global powerful IoT platform. We implement our cloud-based, core mobile network in different regions of the world and we partner with local connectivity providers – local mobile network operators (MNOs). We buy the local connectivity from them and then offer our customers the connectivity with one single API, one single interface, one single bill worldwide plus all the facilities to make that work – provisioning, activation and others. We reduce all that complexity down into real simplicity. ▶

SPONSORED INTERVIEW

RD-W: Do you use eSIM?

NS: Definitely. We encourage the use of embedded SIM (eSIM). We support both the standard as well as our own method that provides more efficiency. Customers can choose either. We also support softSIM initiatives. In fact, we support all new and existing SIM initiatives.

It's really all about what the customer needs. Sometimes the standard method will work best. Other times, the standard method is expensive for certain use cases. In such cases, we can offer a more proprietary solution that is more cost effective.

RD-W: What makes floLIVE different?

NS: Our architectural and technology approach is unique: Firstly, we build our own technology and 4G/5G core mobile network to specifically address the large variety of IoT use-cases, such as NB-IoT/CAT-M on one hand and high throughput use cases on the other. Secondly, we implement it in various locations worldwide to build a unique 4G/5G IoT-dedicated network that takes advantage of a modern cloud-based solution.

This kind of approach is taken to provide an optimised IoT solution for our customers from a performance and security perspective, as well as providing seamless control, compliance and management.

The vast majority of the platforms on the market primarily deal with data management and the ability to build vertical sector applications on top. We are less focused on that. We provide a seamless, cloud-based network solution for IoT connectivity on a global scale, and we provide both networking and device management. We can do this in a really flexible way because we have the whole technology stack in the cloud. A customer may want a dedicated global network for example. Within this, its devices are connected to a private network slice and the slice will be dedicated for this specific customer alone.

RD-W: Is that network slicing specific to 4G and potentially 5G?

NS: Our technology is fully 4G compliant, and soon our global network will be migrated to support 5G, too. This global LTE/5G network provides the slicing capabilities to our customers as mentioned above. We do not deal with network slicing on the radio access network itself. We do network slicing on all of the logical parts of the network – the evolved packet core (EPC) level of the core network itself. We use our own core network, with the radio access networks from the MNOs. Controlling the technology and network topology also allows us to expand our cloud-based network to a customer premises if needed, to provide a unique solution.

RD-W: Are there other unique elements in floLIVE?

NS: Yes, there are several. Let me describe one more in brief. We call this, software-defined connectivity (SDC). IoT solutions are suffering from a lot of friction – lots of things need to come together for a solution to work. SDC provides the ability to consume the services with REST APIs or micro-services. When building a complete IoT solution, connectivity is a big part of that. SDC empowers the customer to use our entire set of capabilities managed via a simple set of APIs or microservices that you can consume and build as part of your broader IoT solution. To do that, you need to abstract all the telco complexities into something that application developers can integrate in an easy way, as simple as building blocks. That is a very powerful offering for application developers. ■

We build our own technology and 4G/5G core mobile network to specifically address the large variety of IoT use-cases, such as NB-IoT/CAT-M on one hand and high throughput use cases on the other

www.flolive.net

flo. LIVE
Connecting Devices
at Cloud-Speed

Eseye utilises floLIVE to expand its global IoT connectivity to cut costs and complexity and achieve new growth and success

Eseye is a leading global provider of IoT connectivity. Since 2007 it has been serving more than 2,000 companies deploying IoT devices across all industry verticals.

floLIVE has recently supplied Eseye with a virtual connectivity infrastructure in new regions, with complementary management and reporting capabilities via its cloud-based platform, utilising floLIVE's rich application programme interface (API) suite.

This provides Eseye with an innovative unified connectivity management solution to manage international mobile subscriber identification (IMSI) numbers from numerous operators, increasing Eseye's global footprint, adhering to privacy regulations and roaming restrictions, improving its troubleshooting capabilities and allowing it to focus on adding value to customers by expanding into customised and personalised service for specific needs

Business impact of floLIVE

- Reduced operational costs
- Eliminated complexity of integrations
- Improved incident resolution time from days to minutes

Eseye needed a solution to accelerate the roll-out of its IMSI localisation offering across multiple territories. The traditional approach was to use multiple mobile network operator (MNO) profiles, each covering a different region. However, this was costly, siloed and time consuming, from onboarding and initial integration, to ongoing support and maintenance. Eseye felt that there must be a better way.

Through its research into potential connectivity partners, Eseye realised that it was looking for a specialist solution that would greatly reduce the number of MNO relations and integrations, and that could be easily customised to support the evolving needs of connected devices. This partnership would free up Eseye to focus on delivering value added services to its global customer base. ▶

Eseye was introduced to floLIVE, and felt an instant connection – not only in terms of a strong organisational and cultural fit, but the company was reassured that the floLIVE team was knowledgeable with many years of experience in the industry.

"We have been particularly impressed with the support provided by the floLIVE team and their responsiveness and personalised service," said Adam Hayes, the chief operating officer of Eseye. "With floLIVE's focus on developing their feature-rich platform and extending partnerships with mobile operators, we can see how much both our own company and our customers in turn are going to continue to glean from this relationship."

www.flolive.net

The results - floLIVE provides all the control and flexibility Eseye needs on a global scale

- **A highly developed market offering:** floLIVE's cloud based platform allows Eseye to focus on developing its own core service with unparalleled time to market. One example would be extending IoT integrations with hyperscale cloud providers, enabling Eseye to increase its global footprint exponentially. It also significantly reduces the time to market to bring new localised IMSIs on-line.
- **Less complexity:** It had previously been a full-time operation just to track and manage the multiple MNOs and their disparate upgrade and service schedules, support variables and varying levels of transparency. With the floLIVE platform in place, Eseye has a unified telecoms solution, reducing the number of multiple integrations required and eliminating the previous complexity.
- **Lower maintenance costs:** With everything easily visible and accessible from a single cloud dashboard, Eseye can maintain an extremely high level of service quality, at a reduced monthly cost.
- **Revolutionised service:** Eseye is now in a stronger position to support its own customers and maintain its devices. Historically, it would have taken a huge amount of resources to track down a problem and then get an answer from a third-party. Now, floLIVE provides one point of contact that enables incident response to be handled in minutes.

About floLIVE

floLIVE provides secure, cloud-native connectivity solutions to service providers, cloud providers and enterprises looking for seamless global coverage. The platform comprises distributed core networks that provide local connectivity while being centrally managed and controlled over the cloud. This unique approach enables manufacturers to benefit from high performance, secure and regulatory-compliant local connectivity with the flexibility and elasticity of a cloud-native platform. floLIVE's solutions are offered as-a-service in a pay-as-you-grow business model.

Get in touch at **www.flolive.net** to discuss your bespoke requirements.

SPONSORED CASE STUDY

MAVOCO

IoT Connectivity and Subscription Management Platform.

For the IoT world and beyond.

www.mavoco.com

Global IoT Insights

Made in Sweden

Contact us for more information about our M2M/IoT market research or to arrange a meeting.

We cover in-depth all the areas illustrated below:

mHealth

Smart Cities

Connected Cars

Retail Applications

Smart Homes

Wearables & Consumer Electronics

Smart Grids

Industrial M2M

Fleet Management

M2M & IoT Strategies

Horizontal M2M & IoT Solutions

M2M Forecast Database

Berg Insight - 15 years of leading M2M/IoT market research

Based in Sweden, we have been specialising in all major M2M/IoT verticals such as fleet management, car telematics, smart metering, smart homes, mHealth and industrial M2M since 2004. Our vision is to be the most valuable source of intelligence for our customers. Berg Insight can offer numerous market reports, detailed market forecast databases and advisory services. We provide custom research tailored to your requirements including focused research papers, business case analysis, go-to-market strategies and bespoke market forecasting.

Our clients include many of the world's largest mobile operators, vehicle OEMs, fleet management solution providers, wireless device vendors, content providers, investment firms and venture capitalists, IT companies, technology start-ups and specialist consultants. To date we have provided analytical services to 1000 clients in 72 countries on six continents.

info@berginsight.com | Phone +46 31 711 30 91 | www.berginsight.com

BERG INSIGHT

SMART ELECTRICITY METERING 2020

THE CURRENT STATE OF PLAY

IoT NOW ANALYST REPORT

SPONSOR

aeris®

Levi Östling,
Berg Insight

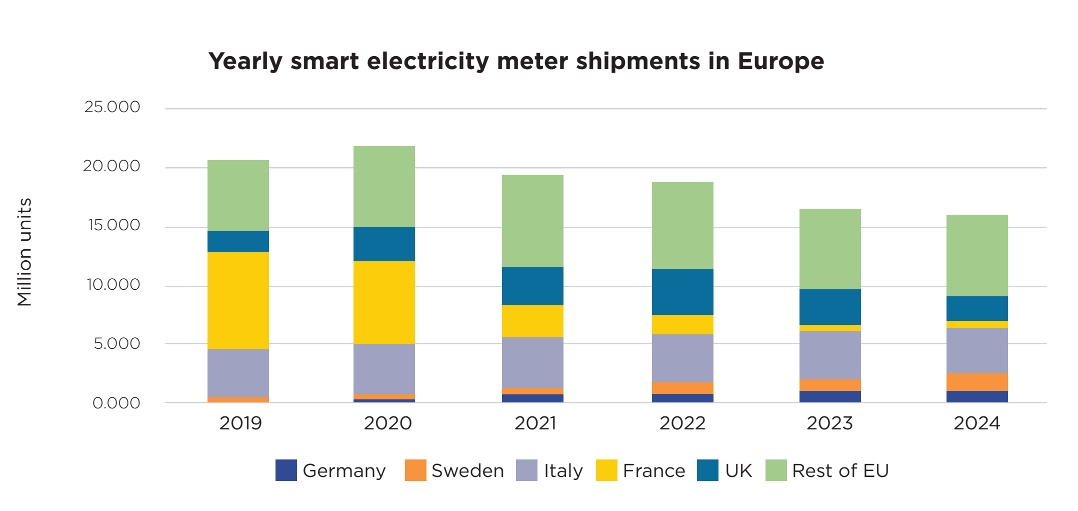
Smart electricity metering – the current state of play

The energy sector is in a stage of slow but gradual transformation. The share of renewable generation is on the rise and energy efficiency programmes are having a tangible effect on power consumption. Micro-generation and electric vehicles are part of a new reality where traditional utilities must reconsider their future strategies. Smart meters have now been around for almost two decades and are widely regarded as a cornerstone for future smart grids, writes Levi Östling, an IoT analyst at Berg Insight

Between 2014 and 2019, the penetration of smart electricity meters in Europe increased from 24% to around 50%. The corresponding growth in North America was from 43% to around 65%. Berg Insight estimates that the penetration will exceed 70% and 80% respectively in the two regions by 2024. Meanwhile, several major markets in East Asia will have reached a penetration of 100%. The large Indian market is now also joining the smart metering race, aiming to roll out a total of 250 million smart meters in the next few years

The EU27+3 region is home to about 290 million metered electricity customers. In terms of market drivers for smart metering adoption, Europe stands out from a global perspective through its history of implementing cross-border smart metering policies. In 2009, the EU's third energy package entered into force and directly influenced the member states to put smart metering on their political agendas. The directive required member states to conduct cost-benefit analyses (CBAs) and given a positive outcome roll out smart electricity meters for at least 80% of the customers by 2020.

Last year, the EU strengthened its commitment to smart metering technology further by adopting the recast Electricity Directive (EU 2019/944). The new directive among other things addresses the issue of negatively assessed CBAs by requiring revisions of such cases every four years. New deadlines for roll-out completion have also been established – member states now need to reach a penetration rate of 80% within seven years from a positive assessment, or by 2024 for member states that have initiated systematic smart meter roll-outs before 4 July, 2019. Another important element of the new directive is also ▶



Source: Berg Insight

that it strengthens the rights of European electricity consumers in a number of ways – perhaps most remarkably by giving every end-consumer the right to have a smart meter installed upon request.

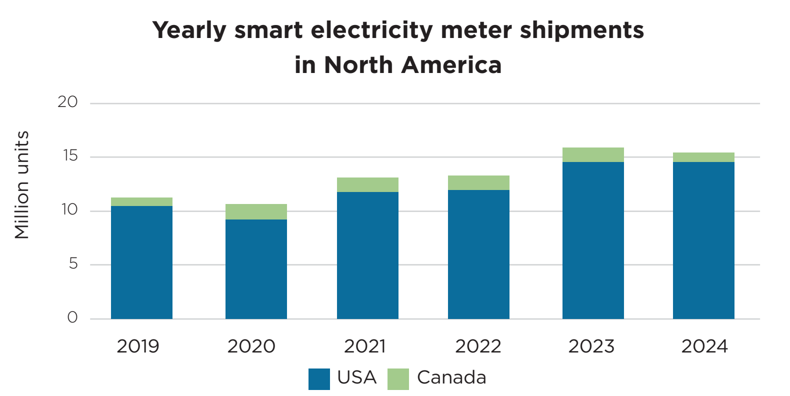
Adoption still varies greatly by country

Although EU regulations are advancing to encourage widespread adoption of smart metering technology, deployment statuses for the European countries vary greatly as national governments ultimately play the key role in adoption. Countries such as Sweden and Italy had for example completed smart meter roll-outs before the concept of CBAs was even adopted. By the end of the last decade, countries such as Finland, Estonia, Malta, Luxembourg, Norway and Spain had also completed nationwide roll-outs. Second-wave installations are now emerging in the first-mover markets as the deployed systems have reached their end-of-life. In Italy, **Enel**'s distribution arm e-distribuzione is leading the way with plans to install more than 40 million second-generation meters by the end of the 2020s, while the Nordic countries Sweden and Finland are about to follow suit in the next few years.

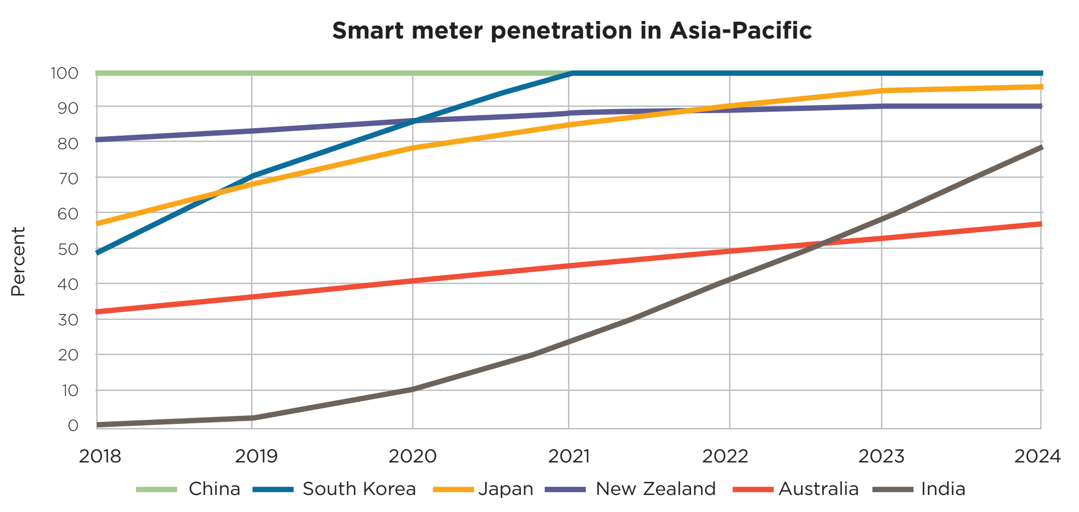
Large-scale first-wave roll-outs are furthermore currently in full swing in several other major European countries, including France, the UK and the Netherlands, while countries such Ireland, Belgium and Lithuania are just now beginning such roll-outs. In some European countries, a major take-off in smart metering deployments is not likely anytime soon. One of these countries is Germany, Europe's largest market in terms of electricity customers. The country has long been held back by protracted standardisation efforts and modest deployment targets set by the regulator. While mandatory roll-outs for customers using more than 6,000 kWh per year commenced this year, the implementation for the vast majority of residential customers is still optional and a drastic change in the level of smart metering adoption is thus not likely to occur in the market in the near future.

Moderate growth in the post-boom North American market

The North American market comprises a total of around 170 million electricity customers. The region has been at the forefront of smart grid technology adoption and now has more than 100 million smart electricity meters installed. While large-scale roll-outs had already started to emerge across North America in the mid-2000s, the market experienced a major boost during 2009–2013 through the American Recovery and Reinvestment Act, resulting in the completion of a large number of projects in the early 2010s. Adoption has since then progressed at a slow but steady pace and is today mainly driven by legislation at the state or province-level, largely unaffected by competitive market forces. The investor-owned utilities (IOUs) that dominate the electricity sector are subordinate to state regulatory commissions authorised to veto any investment deemed too costly for end-customers. While some states or provinces have consistently criticised the benefits of large-scale smart meter roll-outs in proportion to the implementation cost, others have actively promoted smart meter deployments and adopted progressive policies for a green technology transition. As a result, some regions have completed their smart metering roll-outs while others are less than 10% deployed. ▶



Source: Berg Insight



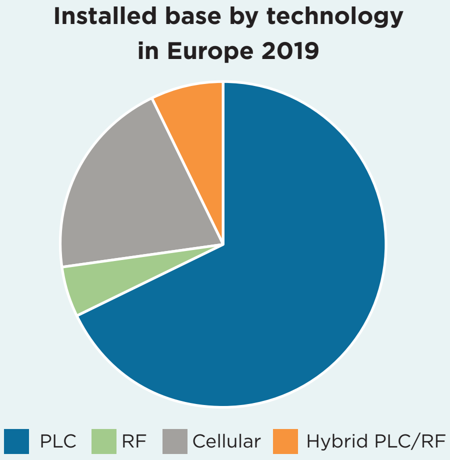
Source: Berg Insight

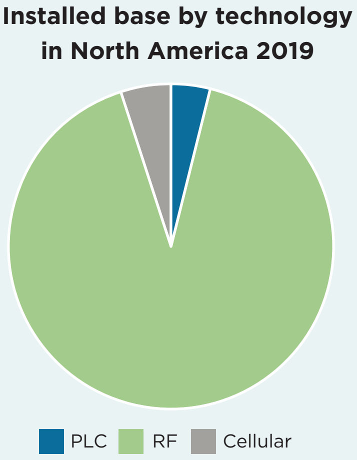
Focus shifts to smaller utilities in the build-up to second-wave roll-outs

There are around 3,200 utilities operating distribution networks in the North American electricity market. Approximately 35 of these have one million customers or more, while over one hundred have more than 100,000 customers. A majority of the large players are IOUs, which together serve more than two thirds of all electricity customers in North America. Most of these are now either fully deployed or in the process of rolling out smart electricity meters, while a few still lack approval from state authorities to launch large-scale roll-outs. As a result, the small number of major tender announcements in the last few years has led many vendors to increasingly focus on the thousands of smaller municipal and cooperative utilities operating in the region – at least until the second wave of large-scale roll-outs for the first-moving IOUs take off in the next few years. In the next couple of years, major ongoing deployments by IOUs such as **Con Edison**, **Duke Energy**, **Ameren**, **Entergy**, **PSEG**, **National Grid** and **Xcel Energy** will nevertheless account for the majority of meter installations. Although some utilities have already started replacing first-generation smart meters, Berg Insight expects that second-wave roll-outs will really take off around 2023. A characterising theme of these deployments will likely be the utilisation of meters with greater computing power and edge intelligence capabilities which can support distribution automation operations – a highly sought-after and fast-growing application area in North America as improvements in grid resilience and reliability are highly needed to counteract the vulnerability of the region's antiquated grid infrastructure.

East Asia's ambitious national roll-out strategies lead the way in Asia-Pacific

Asia-Pacific constitutes the world's largest and fastest growing meter market and today has an estimated installed base of more than one billion electricity metering devices. In terms of smart metering adoption, East Asia constitutes the clear leader in the region. More than a decade ago, South Korea and China launched national policies for their government-owned national utilities to complete the construction of nationwide smart grids by the year 2020. The latter completed its unprecedented roll-out in 2018 after having installed a total of more than 550 million smart meters. In addition, second wave roll-outs have already been initiated due to the relatively short life span of Chinese standard metering equipment. South Korea's deployment for its 23 million electricity customers has on the other hand been subject to a series of delays caused by technical concerns and tendering process issues, making it increasingly likely that project completion will be postponed by one to two years. Meanwhile, Japan has set a target to reach full deployment of smart meters for its 86 million electricity customers by 2025. All the electricity distributors in the country have accordingly launched territory-wide smart meter deployments and are now well on their way to complete roll-outs according to schedule by the end of 2024. ▶





Source: Berg Insight

The awakening of the Indian market

As the smart metering markets in East Asia are maturing, attention is now shifting to another part of Asia – India. The national government has identified smart grid technology to be a potential solution to fight operational losses which have plagued the country's utilities in the past two decades. In 2018, the Ministry of Power stated the extraordinary target of reaching nation-wide coverage of smart prepayment meters for all 250 million electricity customers by 2022. Large-scale deployments of smart meters have now started in the country, following a lengthy period of pilot projects. The poor financial shape of the state-owned utilities which dominate the market has moreover led the government to go for a business model where a separate government-owned entity aggregates demand from a number of utilities and subsequently procures meters in bulk, thus lowering the cost of equipment for the individual utilities as compared to stand-alone procurements. With more than ten million units contracted to date, the government-owned organisation EESL is so far unmatched by stand-alone smart meter procurements on the Indian market. After the recent establishment of a national smart meter standard, equipment tendering has started to pick up pace and the market is now expected to see massive growth of smart meter shipments in the next few years. The aim of 250 million installed meters by 2022 might however not be very realistic.

Connecting the smart energy eco-system

Today, three broad technology groups dominate the smart metering communications market – power-line communications (PLC), radio frequency (RF) and cellular technology. The technology choice varies broadly by region and country. In Europe, PLC technologies such as G3-PLC and PRIME today account for approximately two thirds of all smart metering installations while domestic PLC standards developed by the national utilities dominate the smart meter communications space in China and South Korea. The vast majority of meters installed in North America are in contrast using proprietary sub-GHz mesh or point-to-point RF networking platforms, while 920 MHz RF mesh networks constitute the primary connectivity option for smart meters in Japan. In countries such as Australia and New Zealand, cellular communications is instead favoured – largely due to the market-driven roll-out model characterising these two countries. In India, the smart meter communications space is so far two-fold – isolated procurements of smart meters from single utilities have favoured RF mesh networks while EESL has chosen GPRS connectivity.

Smart meter communications in 2020 and beyond – what's next?

The rapid development of new technologies for the Internet of Things has a major impact on the smart metering market. Utilities planning for new smart grid projects and roll-outs in the 2020s ▶

have a wide range of increasingly sophisticated wireless technologies to choose from as networking platforms. Hybrid PLC/RF solutions are rapidly gaining adoption in regions such as Europe and China and are likely to continue to grow at the expense of stand-alone PLC solutions over the coming years. The adoption of 3GPP-based LPWA technologies such as narrowband IoT (NB-IoT) and LTE-M will likely result in an even more far-reaching technological transformation. Optimised for cost-sensitive and mission-critical IoT applications, these technologies eliminate some of the main drawbacks which have held back wider adoption of cellular communications in the smart metering space and are now quickly becoming popular for smart metering applications. In Europe, the major Dutch utility **Enexis** has already started to deploy meters using KPN's LTE-M network while **Trustpower** in New Zealand has been using **Spark**'s LTE-M network for smart meter connectivity since last year. In Sweden, **Telia** is set to connect some 2 million meters using a mix of NB-IoT and LTE-M in the upcoming second-wave roll-outs by **Ellevio**, **E.ON** and **Kraftringen**. **Fluvius** in Belgium is now entering the full-scale roll-out of 1.3 million NB-IoT-connected meters in partnership with Proximus. ESO in Lithuania has furthermore chosen NB-IoT as the networking platform for its upcoming nationwide roll-out of 1.9 million meters, scheduled to begin later this year.

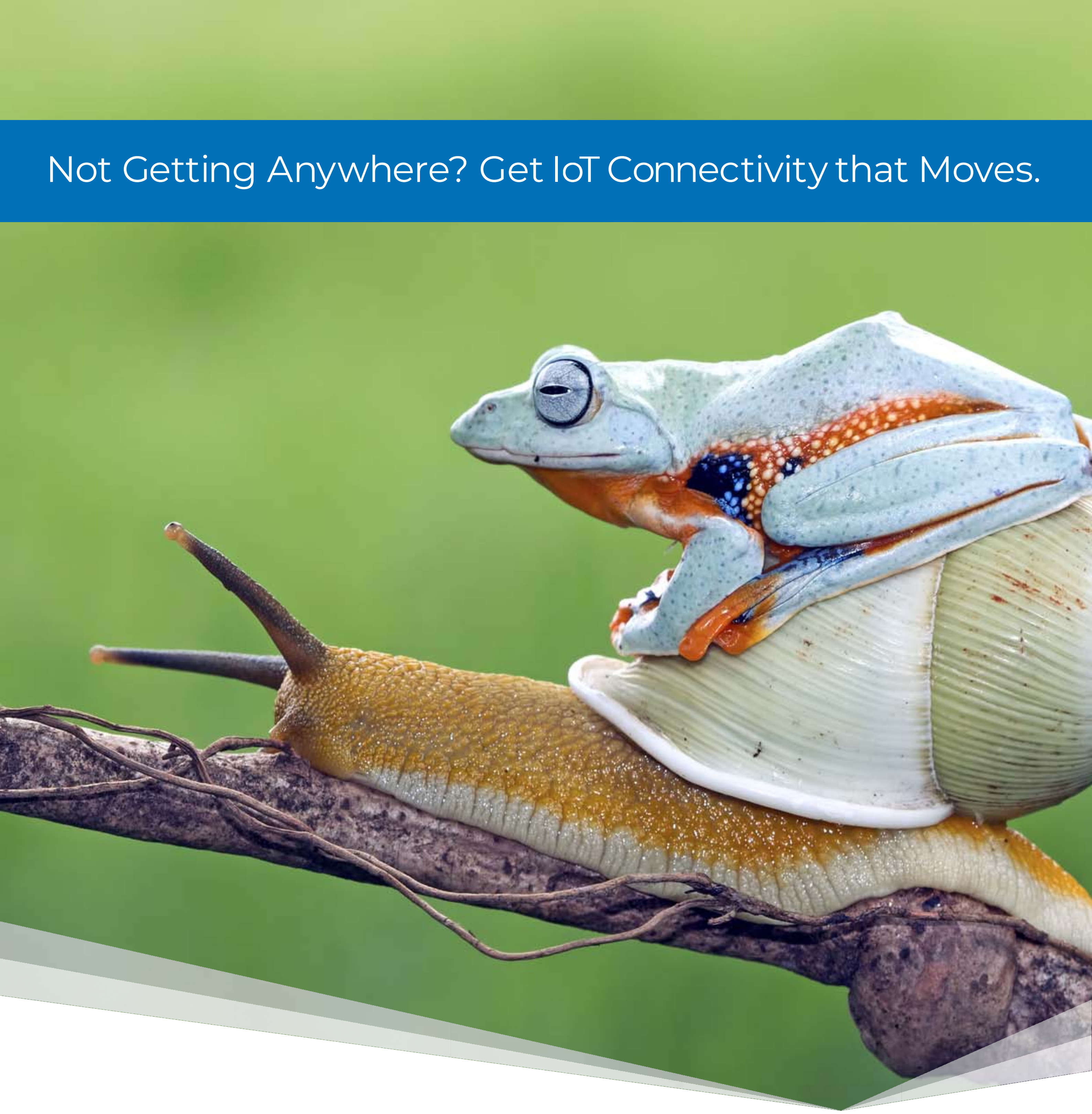
A major interest in 3GPP-based low power wide area (LPWA) technologies is also expected in Asia. The adoption of NB-IoT across multiple verticals in China is now starting to spread into the country's smart metering segment. A preference for NB-IoT communications has also started to appear in the tenders issued by **EESL** in India and Berg Insight expects that the government-led deployments in the country will favour the technology once the relevant network infrastructure is in place. In the next few years, adoption of 3GPP-based LPWA is nevertheless most likely in the mid- and small-size utility segment, which to a greater extent can benefit from the increased deployment flexibility that point-to-point communications enables. ■

About Berg Insight

Berg Insight is an IoT analyst house based in Sweden. We have been specialising in all major M2M/IoT verticals such as fleet management, car telematics, smart metering, smart homes, smart cities, mHealth and industrial M2M since 2004. Our vision is to be the most valuable source of intelligence for our customers. Berg Insight can offer numerous market reports, detailed market forecast databases and advisory services. We provide custom research tailored to your requirements including focused research papers, business case analysis, go-to-market strategies and bespoke market forecasting.

Our clients include many of the world's largest mobile operators, vehicle OEMs, fleet management solution providers, wireless device vendors, content providers, investment firms and venture capitalists, IT companies, technology start-ups and specialist consultants. We have provided analytical services to 1,000 clients in 72 countries to date.

If you have any questions about our market report subscriptions and advisory services or simply want to understand how Berg Insight can help you, don't hesitate to contact us at: **info@berginsight.com**


Not Getting Anywhere? Get IoT Connectivity that Moves.

Aeris powers IoT applications in the utilities sector

Around the world, utilities are often under heavy public scrutiny as the services they provide often constitute integral parts of the infrastructure we all need and, therefore, also the basis for a well-functioning society. Utilities have faced increasing pressure to adjust their operations to account for the growing public concerns of environmental and economical sustainability. The term 'smart utilities' now has been around as a catch-phrase for more than a decade, referring to the potential of leveraging technology and, in particular, the Internet of Things (IoT), to transform utilities into efficient and future-ready enterprises.

By connecting the multitude of assets in electricity, gas, water and waste networks, entirely new ways of undertaking traditional utility services are emerging. Mohsen Mohseninia, the vice president of International Market Development for Europe at Aeris Communications, spoke with Johan Fagerberg, the chief executive at Berg Insight, about Aeris' activities to help make utilities smart

Aeris serves a broad range of utility applications, such as smart metering and management of renewable energy sources, water and wastewater, electricity and gas. Examples of clients include **Detetronic, BBOXX, Paygo Energy**, **Badger Meter** and **Lorentz.** Detetronic creates and delivers intelligent network monitoring for the European water industry to help maintain a clean, pollution-free and flood-free environment. BBOXX provides clean energy solutions to off-grid communities, including innovative plug-and-play solar powered systems to improve access to energy across Africa and the developing world. Paygo Energy sells gas a service using an innovative pay-as-you-go scheme. Badger Meter is a manufacturer of flow measurement and control solutions. And Aeris also supports Lorentz' roll-out of solar powered water pumping solutions worldwide.

IoT connectivity technology choices

The rapid development of new technologies for industrial Internet of Things (IIoT) has a major impact on the smart utilities market. Utilities planning for new smart grid projects and rollouts in the 2020s have a wide range of increasingly sophisticated wireless technologies to choose from as networking platforms. Supported by massive R&D investments in the mobile communications industry, the latest cellular technologies are optimised for cost-sensitive and mission-critical IoT applications and are gaining traction in the utilities space.

Today, Aeris manages close to 15 million cellular IoT connections for 300-500 clients. About 20-25% of the connections are for clients in the utilities sector. The current deployed units primarily can be found in the US (60%) but also scattered across Europe, Africa and Asia.

"The most suitable technology to use all depends on the type of application, as well as where the client is deploying and for how long the devices need to be in the field. You also need to consider whether they are battery powered or have a ▶

SPONSORED INTERVIEW

Mohsen Mohseninia
Aeris

power source," says Mohseninia, pointing out that Aeris focuses on the delivery of cellular 2G, 3G, 4G, LTE-M and soon also narrowband IoT (NB-IoT) when available.

"We are seeing that for off-grid energy customers in rural Africa and Asia-Pacific, the technology of choice still is 2G and moving forward LTE-M," he adds. "When we look at on-grid solar deployments, LTE CAT 1-4 is a common choice in developed countries. 5G could be relevant to wind farms and remote management and virtualization where speed is important."

Aeris can help manage connectivity costs

Aeris' business model is to enable the customers' business model and make its clients successful. Aeris can do this because the company has spent more than ten years working with IoT customers, understanding their needs and building billing and business support systems to cater for those needs. A significant flexibility has been built into the system to be able to support customer needs from pre-paid to post-paid, from bundled to pay-as-you-go and from monthly rolling contracts to fixed-term contracts.

Aeris has a proven track record in bringing the total cost of ownership down whilst significantly improving the quality of service. For example, a customer in solar off-grid used to have a monthly cost of US$0.4 per device to support its service which was reduced to US$0.2 per device and month after switching to Aeris. The client has 100,000 devices so this equates to a US$0.72 million reduction in cost over a three-year period.

The Aeris Fusion IoT Network

"Our core role is to take our clients on a journey from unconnected products to connected services. Put simply, we help companies, large and small, to win with IoT. We provide highly reliable and scalable connectivity for IoT devices through our Aeris Fusion IoT Network", says Mohseninia.

Fusion is about building intelligent applications that help Aeris customers aggregate and enhance the data that they get at the edge, together with additional sources of data that Aeris can provide that can then go to the cloud for further processing. For example, Aeris is focusing on machine learning and artificial intelligence (AI). A further microservice is about location-aware over-the-air (OTA) upgrades. In the future, Aeris believes that OTA will become ever more critical to operations so they have developed a service specifically to manage that. Aeris has built a microservice that allows its customers to sequence their OTAs rather than broadcast them. This significantly improves the success rate of OTAs and, as a result, decreases the cost of the overall OTA activity.

Another example is ConnectionLock that prevents access to unauthorised endpoints or IP addresses, creating an additional layer of security for IoT devices. If the SIM card gets stolen from a device, Aeris ConnectionLock ensures that the SIM card can connect to no other IP address or URL. The Aeris Fusion IoT Network adds intelligence - a set of microservices to help customers reduce their costs, improve their service quality and take advantage of the new technologies. It brings intelligence to the application layer.

The impact of COVID-19 on the utilities sector

With the current COVID-19 pandemic, now more than ever, it is important to use IoT solutions. Aeris has identified changes to IoT connectivity activity since the onset of COVID-19. There has been no change in the traffic from solar and other utilities applications. As a comparison, Aeris has seen a decline in network activity among customers involved in logistics and passenger cars at the same time as remote health applications have experienced an increase in traffic. "The COVID-19 pandemic also is a time when IoT can demonstrate extra value for connected devices in avoiding unnecessary human contact. Smart meter infrastructure, for example, means that you don't have to send someone to collect data," concludes Mohseninia.

Nothing is certain about this current health crisis, we don't know when it will be over or what the fallout will look like. But we do know that we have the tools available to reduce the risk as much as possible and help to alleviate healthcare services when they need it the most.

Simply by maximising the number of patients that can be attended to by doctors in the hospitals, and reducing the number of people that need to come into the hospital for regular appointments, IoT could take a huge weight off the shoulders of medical staff.

As events unfold, IoT could well play a big part in alleviating the strain on our healthcare systems, only time will tell if remote care is ready for such a task. IoT is also proving its value in other industries during the pandemic. It is rising to the challenge of handling the huge logistics burden being placed on retailers to ensure food supply, for example. Others such as utility providers are utilising IoT to minimise risk to their employees by eliminating non-essential activities. IoT, for example, can be used to prioritise maintenance for machines that are close to failure while postponing routine work that can be delayed.

The immediate need is to reduce workforce – and customer – exposure to the virus and by collecting data and analysing it to gain insights, organisations can do more remotely, automate more effectively and optimise their organisations so time spent at risk is minimised. The pandemic provides an opportunity for IoT to demonstrate the multiple layers of value it can add and to increase trust in and familiarity with IoT capabilities for the changed world that follows COVID-19. ■

www.aeris.com

With Aeris, BBOXX provides clean energy solutions to off-grid communities

Companies operating in the most remote locations, with products purpose-built for off-grid, rural, and often hostile environments, require a reliable global mobile network that provides consistent connectivity worldwide to enable effortless remote monitoring of energy systems. To overcome these many life-critical, energy-delivery issues, there is significant need for reliable GSM and CDMA connectivity to deliver functional, energy saving solutions

The World Energy Outlook estimated that 1.2 billion people, equivalent to 16% of the global population, did not have access to electricity in 2016, with many more people living with an electricity supply described as poor quality or unreliable. More than 95% of those living without electricity are in sub-Saharan Africa and developing Asia, 80% of which live in rural areas. The United Nations Foundation has stated that "energy powers the world's economic engine," adding that, "from the perspective of jobs, security, climate change, food production, or increasing incomes, access to sustainable energy for all is essential for strengthening economies, protecting ecosystems, and achieving equity."

BBOXX—Energising the world

BBOXX designs, manufactures, distributes and finances innovative plug-and-play solar powered systems to improve access to energy across Africa and the developing world. The company recognises the importance of sustainable energy and, as such, aims to provide 20 million people with electricity by 2020.

Through a vast network of shops and outlets, BBOXX focuses on giving people, many in off-grid communities, access to electricity, while offering superior customer service. Its core products are a range of solar powered battery boxes that sit in a home and allow users to power small appliances, such as lights, mobile phones, refrigerators or computers.

BBOXX needed to use real-time data to identify device issues early — with pro-active alerts sent to customer service agents to ensure that system problems could be fixed before they evolved. Because of this, the company required a reliable cellular network that enabled effortless remote monitoring and access to real-time data, as well as the ability to configure and adapt each system so as to maximise battery life and provide cost-effective solutions for both itself and its customers.

In addition, BBOXX products are manufactured without a known destination and, as such, with certain mobile network providers, a local SIM card would have to be inserted into the device following sale and then would require local configuration. This process required additional time, cost more, and hindered operational effectiveness. Therefore, mass global deployment of solutions only was possible by working with a reliable cellular network partner that provided end-to-end monitoring, no matter where in the world systems are deployed. And a partner that could connect to multiple carriers, regardless of location. ▶

SPONSORED CASE STUDY

Customer Benefits

- ANALYZE AND MONITOR SYSTEMS TO EXTEND BATTERY LIFE
- REAL-TIME ACCESS TO DATA USAGE, ALERT MANAGEMENT, AND DEVICE CONNECTIVITY MANAGEMENT OVER THE SIM LIFE CYCLE
- SIMPLE PLUG-AND-PLAY, WITHOUT THE NEED TO CONFIGURE LOCAL NETWORK SETTINGS
- REAL-TIME DATA PROVIDE INSIGHTS
- INSIGHTS TO TROUBLESHOOT ISSUES
- SINGLE GLOBAL ACCESS POINT
- PREDICTIVE AND PROACTIVE MAINTENANCE

Aeris IoT Solution: Reliable network connectivity enables global deployment

Aeris offers multiple, non-steered network connectivity in East and Central Africa, the principle areas where BBOXX deploys, thereby enabling real-time gathering of actionable data. Aeris' global support of major cellular technology standards, such as GSM, CDMA, and LTE, also ensured that BBOXX could deploy its devices in any location during global expansion.

With the Aeris IoT Services platform, BBOXX can install the Aeris global subscriber identity module (SIM) at the point of manufacture, reducing both supply chain costs and deployment time. Also, by utilising Aeris' single global access point name (APN), the solar-powered BBOXX system could be deployed on a simple plug-and-play basis, without the need to reconfigure to local network settings.

By utilising the Aeris connectivity management platform, AerPort, for IoT devices, BBOXX was able to have real-time access to data usage, alert management, and device connectivity management over the SIM life cycle.

An easily deployed and remotely monitored global clean energy solution

Aeris IoT Services' network connectivity enables BBOXX to remotely monitor its devices. Configuration and deployment times have been reduced significantly. Predictive and proactive maintenance help lower ownership and maintenance costs. And, these plug-and-play devices can be switched off from a central location if troubleshooting issues arise or if payments are not met. All this adds up to the lowest possible TCO for an IoT solution.

> ***"By working with Aeris, we can ensure that our solutions have optimum reliability and our customers can be sure their devices possess a reliable connection, at all times, no matter the location. Aeris' high-quality service and IoT expertise ensure that we can offer the best clean energy solutions to off-grid communities worldwide,"***
> *Christopher Baker-Brian, co-founder and chief technology officer, BBOXX*

ABOUT BBOXX:

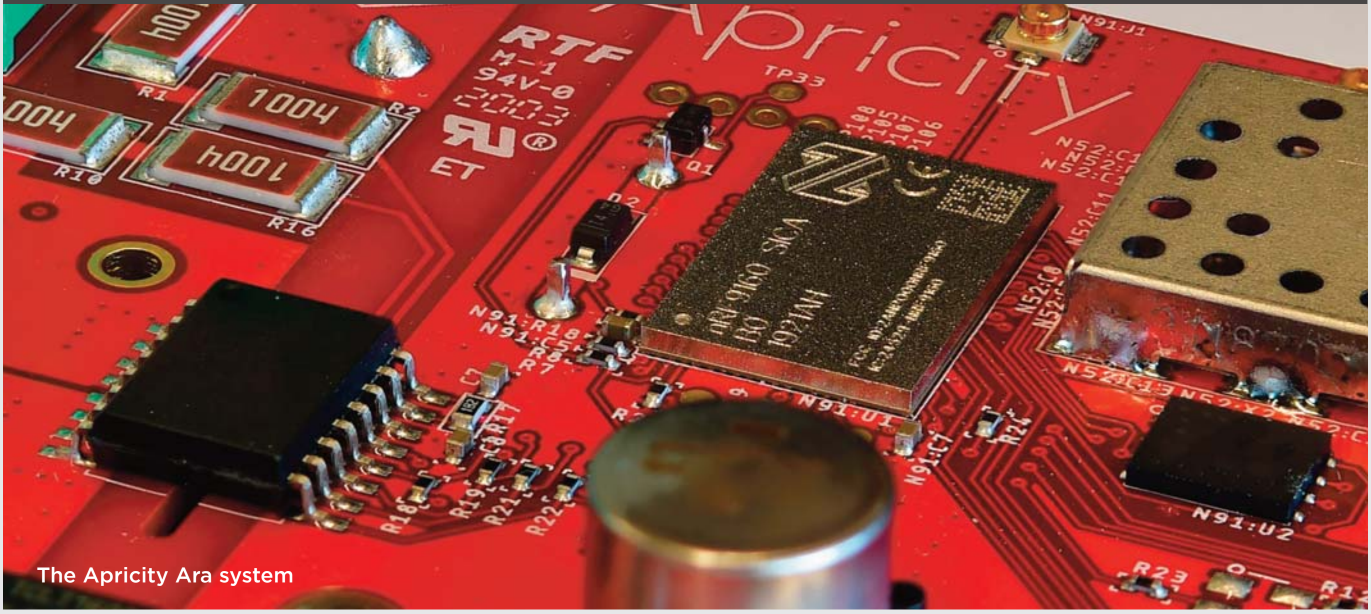
BBOXX is a venture backed company developing solutions to provide affordable, clean energy to off-grid communities in the developing world. We are fully vertically integrated, controlling every part of our customer experience. Our market leading products and appliances, coupled with our SMART Solar platform, bring machine-learning and customer experience optimisation to rural Africa. Our ground-breaking financing structure has brought off-grid solar into the world's financial markets. With more than 80,000 systems deployed so far, 300 staff across five offices in China, U.K., and East Africa are waking up every morning to work with BBOXX to electrify 20 million people by 2020.

ABOUT AERIS:

Aeris is a technology partner with a proven history of helping companies unlock value through IoT. For more than a decade, we've powered critical projects for some of the most demanding customers of IoT services today. We strive to fundamentally improve their businesses by dramatically reducing costs, accelerating time-to-market, and enabling new revenue streams. Built from the ground up for IoT and road tested at scale, Aeris IoT Services are based on the broadest technology stack in the industry, spanning connectivity up to vertical solutions. As veterans of the industry, we know that implementing an IoT solution can be complex, and we pride ourselves on making it simpler.

Cellular IoT helps to avoid US auxiliary power stations being fired up

Domestic water heaters are estimated to be responsible for up to 20% of power usage per house in the US. Now, by using a cellular IoT LTE-M wireless water heater controller, they can be selectively switched on and off during the day, so water is still near optimal temperature but unnecessary electricity consumption during peak periods can be cut



The Apricity Ara system

This avoids spikes in demand that can greatly increase the cost and inefficiency of running local power grids and can avoid extra power plants being brought online to meet demand during peak periods.

Oslo, Norway-based **Nordic Semiconductor** reports that US engineering and product design agency, **Apricity**, is helping multiple power utilities in pilot field studies throughout the States to avoid having to rely on firing up environmentally-polluting auxiliary power stations to meet prime-time demand.

This is done using the Apricity Ara cellular IoT and proprietary wireless mesh domestic water heater controller. The Apricity Ara employs both a Nordic nRF9160 multi-mode LTE-M / NB-IoT System-in-Package (SiP) and Nordic nRF52840 System-on-Chip (SoC). The entire application runs on the nRF9160's64 MHz Arm Cortex-M33 application processor with 1MB of Flash and 256KB of RAM memory.

In operation, an Apricity Ara is attached in-line with the power supply of each water heater. This allows the heater to be controlled remotely by the local power utility using the LTE-M version of cellular IoT wireless technology. However, as some water heaters were located in environments with poor LTE-M coverage such as basements, Apricity found it also had to support the cellular communications with a proprietary wireless mesh. This enabled any Ara unit with no cellular service to communicate with any other Ara that had good cellular reception and continue to be controlled by the utility.

"In the U.S, tanked water heaters are often installed as always-on devices with no user- or demand-based control and so they continually consume energy reheating the water," explains Apricity chief operating officer, Jacob Betcher. "During times of peak electricity demand, asking dormant hot water heaters to temporarily reduce their energy consumption is a very effective power load reducing method. With some simple local monitoring, it is possible to allow water heaters in-use to continue heating, while reducing standby heating of water heaters not in use."

Betcher continues: "Hot water tanks are in effect an energy storage medium and by making a large number smart you are effectively creating a huge energy storage tank. You can charge this in a much more optimal way if allowed to have some control over which times of day the tank is actively heating stored water."

"It's also important to note the reliability of our solution," adds Apricity engineer, Evan Biskey. "While non-cellular wireless water heater controllers do exist, they are an order of magnitude less reliable. And why they haven't been popular before now with utilities is that the utilities found themselves having to not only set-up and install, but also maintain the wireless connection on an on-going basis because there would always be some kind of gateway that could periodically go down. Part of the reliability of cellular comes from the fact it requires no gateway to connect and uses the strong existing commercial cellular networks."

"This enabled us to make our solution fit and forget and is why we included a proprietary mesh capability to supplement the cellular connectivity and push the reliability uptime figure as high as possible," says Biskey.

"Local power grids can't store excess energy and have to buy-in expensive power from other grids to meet peak demand to avoid brownouts and blackouts," comments Geir Langeland, Nordic Semiconductor's director of sales and marketing. "This application demonstrates how cellular IoT can be used to spread demand out and reduce energy consumption and costs for consumers and utilities." ■

Connected street lights to reach 15.2% global penetration of smart city platforms by 2025

Research by Bristol, UK-based Rethink Technology says that the US$5.2bn annual market for connected street lighting (CSL) still has massive potential. The CSL market has been driven largely by the introduction of LED lighting, which gave adopters huge savings on their energy bills. However, now that the low-hanging fruit is dwindling, as old analogue lights die off, the CSL market needs to embrace the smart city opportunity, providing both a standalone application as well as the networking infrastructure on which to build additional functions

Rethink Technology says there will be some 62.9 million connected street lights worldwide in 2025. However, based on its research, the number of these lights that will be directly integrated into a Smart City Platform (SCP) and used in collaboration with other smart city applications will only reach 9.6 million, or 15.23% of all CSL units deployed – despite nearly a full decade of the majority of CSL tenders including some element of SCP functionality.

While this sounds discouraging, says, Rethink Technology, the street lighting market is slow moving, as are the cities. Contracts typically span 20 years, a lengthy window in which to migrate these lights to an SCP. So the smart city market does seem to be gradual, but it has unmatched global scale.

Globally, the number of pole-based lights is estimated at 350 million, with up to 150 million more lights on buildings, street furniture, and some scene lighting. For cities, lighting has almost always been the largest ticket on the energy bill, and the sales pitch for the LED vendors was that simply swapping from old analogue luminaires to new digital LEDs would save around half of the old energy bill. This freed up cash could then be spent elsewhere in the city. Around 20% of the lighting stock has been converted to LED to date, so there is room for growth in LED, as well as in the supporting CSL offering.

CSL deployments let cities schedule and coordinate lighting levels to match the local conditions, to ensure that the city is always appropriately lit and not wasting power. The dimming capabilities of LEDs also allow for dynamic lighting choices. LED units also last much longer than older analogue ones, with less truck-roll expenditure.

CSL can slash this cost even further. Connectivity lets the network identify luminaires that have failed. Anomalies in luminaires can be reported back to the Central Management System (CMS), which could indicate a looming failure that can be fixed pre-emptively.

The CSL fleets also enable other smart city applications to be built on. The CSL's networking capabilities can be used by other smart city applications that might not justify such a network deployment in isolation, but which could piggyback on the connections between these lights and the SCP.

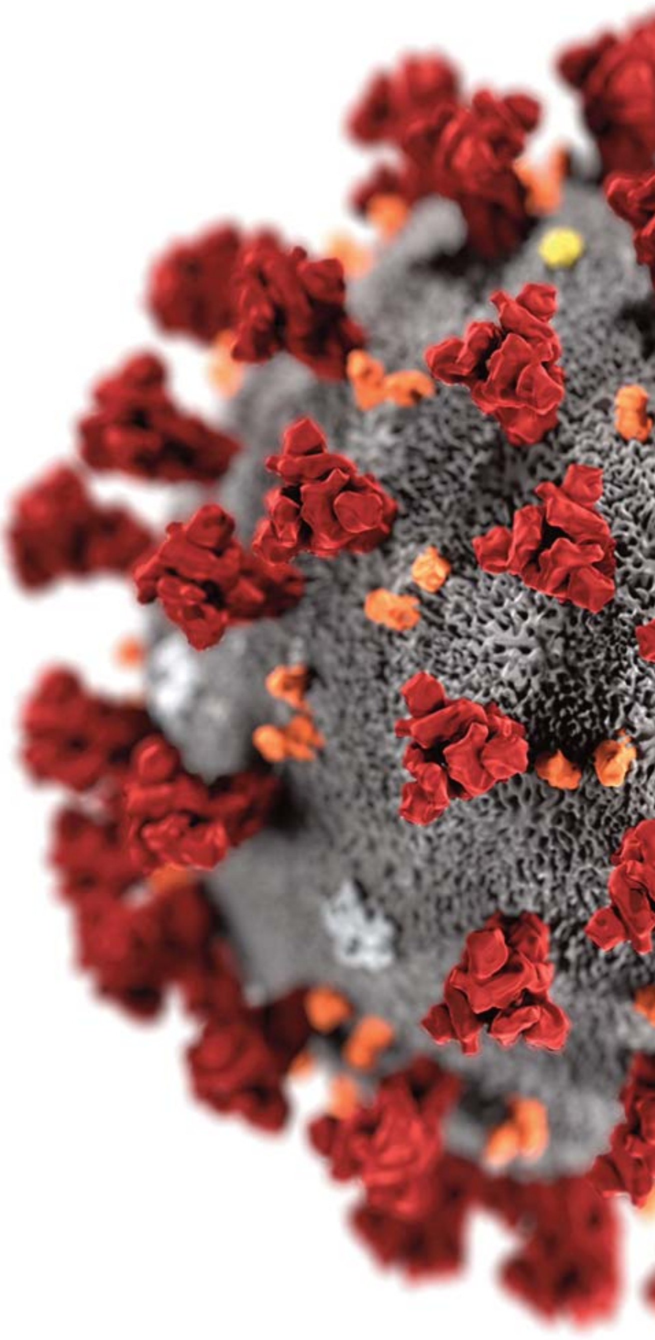
These include environmental sensing for air quality and noise pollution, presence detection and footfall analysis to guide dimming schedules, data-heavy tasks like video analytics for traffic and pedestrian routing, and public safety – including flood and weather warnings. ■

COVID-19 is writing a new world order

Amidst the socio-economic disruptions caused by COVID-19, the common cause of finding a solution to the pandemic has brought together individuals, institutions, communities, governments and society at large, writes CP Gurnani, the managing director and chief executive of Tech Mahindra

Looking at such collaborative initiatives, I get a sense of optimism, since my conviction is that the advanced knowledge of technology and ingenuity will help the global population to fight and defeat this viral attack.

One may argue that it may take some time before an antidote is found. Meanwhile, alternative systems and approaches can be developed that will not only help manage the current crisis but also create new ways of doing business in future.



The global impact

Measures taken by various countries to counter COVID-19 have set a few benchmarks. They provide options for agriculture, manufacturing and other industries to conduct their operations in the face of such a crisis.

Singapore, for instance, has an aggressive contact tracing effort and legal authority to order people into quarantine. In Italy, the country's whole population of 60 million has been restricted from travelling out of their homes, except for urgent healthcare or work reasons. Schools and universities, as well as public gatherings, have been banned until further orders. Similarly, India, the United States, China, the United Kingdom and African countries have shown solidarity in this time of global crisis. All of them are exploring alternative methods, systems and processes to ensure that there is business continuity.

Healthcare

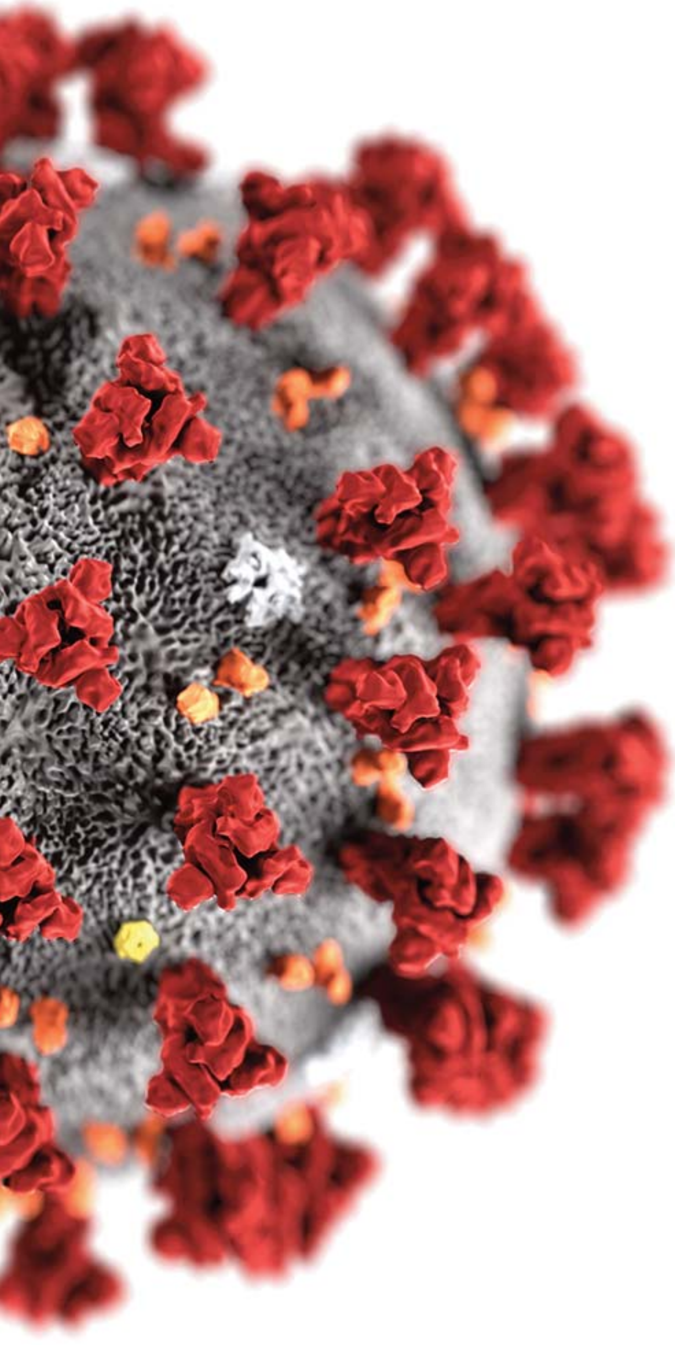
US agencies are encouraging people who feel unwell to first talk to doctors remotely, by video or phone, to avoid filling waiting rooms. Imagine the comfort with such a permanent healthcare system for patients in a country like India, travelling from distant places for specialised health services.

Telemedicine in India is currently at a nascent stage. Systems like those adopted by the US administration to counter COVID-19, when powered with the network of the future - 5G - will give a tremendous boost to telemedicine in India. It will also open up opportunities for entrepreneurs to set up back-end operations in remote, inaccessible and remote parts of India, which in turn would also create job opportunities.

Education

The Kerala government in India has announced that it will provide extra 5G bandwidth across the state, as it expects more people to work and learn online amid the virus outbreak. All school districts in New Jersey have prepared for remote classes, in case schools needs to be closed. A colleague spent all of last week testing systems with students at homes for online learning. E-learning, without any doubt, is in the limelight. Could this be the new future of school education? I am sure it would be the new normal, even after the world has mitigated the effects of COVID-19. ▶

The Kerala government in India has announced that it will provide extra 5G bandwidth across the state, as it expects more people to work and learn online amid the virus outbreak



CP Gurnani,
Tech Mahindra

Agriculture

In few other parts of the world, robots are already doing farm work. With the breakout of COVID-19, this has gained more traction and robots have replaced a slew of farming activities. In agriculture, 5G can further enable improvement in the entire value-chain, from precision farming, smart irrigation, improved soil and crop monitoring, to livestock management. 5G technologies' promise of expanding and accelerating connectivity without sacrificing battery life will be particularly beneficial to farmers, and is already improving veterinary diagnostics, crop protection, reduction of fertiliser use and smart irrigation systems that conserve water.

Remote working

During my last visit to the US, many of the conversations I had were centred around COVID-19. I must admit that there is a perceptible change in the way we socialise, work and commute. But the significant changes are already visible. The 'workplace of the future' is ever-evolving and gradually shifting to accommodate new ideas, technology and working arrangements.

In addition to encouraging our employees to work from home, we have also deferred all our internal events, which required large gatherings and encouraged everyone to leverage technologies like telepresence and videoconferencing adequately. Industry reports before the COVID-19 outbreak estimated the value of enterprise video conferencing at US$4.48bn by 2023, but now it could touch that figure in 2020. This is a clear indicator of a new trend that will enable and support work from remote locations.

We are currently in an existential crisis where the focus is on issues that relate to personal safety, emerging practices required for handling the pandemic, managing concerns about employees and customers.

However, this will ultimately enable us to re-structure our priorities, and ways of living and working to define a new normal. It will help us reimagine the future, ensuring we remember – the importance of building a sustainable world, focusing on healthcare and general hygiene, using technology to enable new ways of working and living. ■

You don't have to outrun the lion, simply stay ahead of the herd

Everyone knows weak security poses a threat to their business, and the connected devices of IoT present a substantial attack surface for hackers. However, there appears to be a general attitude among organisations of hoping a breach won't happen to them, and this attitude can see inadequate device-level security incorporated from the solution concept onwards. Although security technology is mature, it can be complicated and costly to design and manage. Organisations have to balance this expense and complexity against the competitive landscape and the ultimate return on investment of their IoT solution.

Typically, it takes a breach or introduction of new regulation for security to become a priority, but it doesn't have to be like this. By adopting a clear security architecture, organisations can address many of the security basics. They can also outsource many of the management burdens to specialist providers, enabling them to focus on the core business. For many, the goal only needs to be to have better security than other organisations that then present softer, more attractive targets for hackers.

Alon Shamir, the senior director of product management for Pelion Device Management at Arm, and Duncan Jones, a senior product manager with responsibility for chip-to-cloud security at Arm, discuss security with George Malim. In essence, even though security is a never-ending quest, organisations should not lose heart and instead focus on getting a fit-for-purpose security architecture in place, enabling them to layer additional security on to that as the landscape evolves ▶

SPONSORED INTERVIEW

George Malim: What does Arm see as the key threats that affect device-level security?

Alon Shamir: Any conversation about IoT and security starts with the fact that we are seeing more incidents that drive more businesses to be mindful of cybersecurity and invest more in this area. Cybersecurity is complicated, and while it might be heaven for security geeks, for other people, it's hell. There's no silver bullet that can solve security, once-and-for-all, and in every situation. What's needed is a considered, logical evaluation of threats, matched to a plan that mitigates them.

Attacks come from physical and cyber points of origin, and both come with challenges. One comprises the threats you know about and can, therefore, do preventative work to stop. The other involves the threats you don't yet know about, and this is where your weak spot lies. These threats need to be detected so that a mitigation strategy can be developed and implemented. A comprehensive approach necessitates both detection and prevention.

An attack from an unknown or untrusted source on your network means the prevention aspect was ineffective, and you then have to rely on detection to stop an attack. There are two methods of detection to rely on. There is the management data from the device, which can reveal the connections you have open, and this presents a straightforward way to know which device has been breached. The second method is to perform network-level prevention, requiring probes to be deployed all across your networks to detect and identify anomalies.

A famous example of where this would have helped is the Las Vegas casino that was hacked from an aquarium fish tank device that was part of the casino's general network. Proper detection would have identified that the device, which should only communicate with the aquarium service provider, was talking to other casino systems, and this should have triggered an alert, thereby preventing the attack from doing real damage.

Both detection and prevention are essential, but life is not ideal at all times, and you have to adjust to achieve the best security for each use-case, device lifecycle and budget. We do a lot of work on prevention. We have a complete security device lifecycle management strategy, which starts with embedding capabilities into devices at the point of provisioning and continues throughout the entire end-to-end lifecycle.

This in-built prevention capability is so important because, although your devices won't be 100% safe, attackers tend to find and exploit the most easily accessible vulnerabilities. It's like the story of two people running away from a lion; one asks the other: "Do you think you can outrun the lion?"

"I don't have to outrun the lion, I only have to outrun you," is the reply.

The same is - mostly - true in device security. If you make it difficult for attackers, they tend to move on and find an easier target to attack. For this reason, a priority for us is to deliver a strong foundation of security to our customers, even if they're not security experts themselves.

GM: How can IoT organisations and their partners ensure device-level security is optimised? ▶

> ***An attack from an unknown or untrusted source on your network means the prevention aspect was ineffective, and you then have to rely on detection to stop an attack***

Alon Shamir
Arm

Duncan Jones
Arm

[1] https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Often, we think of IoT as a market, but actually, it's a collection of markets

AS: Attackers tend to gravitate to the weakest link, as we saw with the casino aquarium example[1], and get in through that. Therefore, you need to be extremely careful about how you onboard devices and manage them remotely. You can have very good cybersecurity, but once a technician needs to access a device, such as an elevator, they typically have full access. In the case of IoT, the device itself isn't necessarily the target, but the enterprise is. The IoT device is simply how access is gained.

If you can get access through one physical device that is part of the network, the whole network can be exposed. It doesn't matter if you get in through one device or a thousand different devices.

Duncan Jones: When you hear the news that breaches are still happening, that's an indication that some people still see security as something that can be omitted or sprinkled on at the last minute. As tedious as some of these processes are, they are necessary. People are still trying to skip too many steps.

I understand this is because organisations are focused on keeping a low bill of materials (BOM) cost for the IoT device and on getting to market quickly. Still, they need to consider the cost of even one breach.

Some people are doing it right. We're working with customers who choose us because they care about strong security. In addition, there is a difference between devices companies develop themselves – with the necessary security framework – and devices that they may adopt from other sources. We focus on developing devices that are secure in their own right.

This doesn't necessarily mean you need extra components on the device. Still, a fraction more spend can allow you to strengthen the root-of-trust and, for many use-cases, represents only an incremental additional investment in hardware.

Of course, it's not just about what components you put in the device. The structural approach that organisations take to establishing and maintaining their device security architecture is essential. We have a security framework – the Platform Security Architecture – something we make freely available to help organisations with this aspect. Even the cheapest chip can take you a long way in security, just so long as the correct logical structure has been applied.

GM: It's not a one-size-fits-all landscape but what solutions are being brought to market to address device-level security?

AS: I think it's worth pointing out that there is a disparity between different sectors. The Economist Intelligence Unit, for example, has reported that consumer and retail businesses have suffered the highest-profile breaches but are the least concerned about whether these have diminished interest in IoT. In contrast, energy and natural resources companies are the most interested in security.

DJ: Ultimately, it depends on the quality of the job you want to do. In a perfect world, you would do things rigorously and have a threat model developed that exactly matched your IoT application. Arm's Platform Security Architecture identifies various examples of threat models and the processes, elements, and techniques recommended to deliver an appropriate level of protection. Our most security-conscious customers take this approach.

Organisations may want to take on the task of developing their defence against the threats that could affect their use-case. However, not everyone wants to do this, and this is where Pelion comes in. People can get many advantages out of just addressing the basics, but if they are in a high-risk industry or face brand damage, they may wish to go further.

GM: Why are we still having the same conversations about security weaknesses at enterprises despite of all the high-profile breaches and brand damage that's been reported?

DJ: Most of my career has been in security, and you'd imagine that things would gradually get better. But, ultimately, it's only regulation that causes change. We've had cryptography and all the elements in place for years – after all, it's only maths – yet we still find ourselves with breaches in the news. Often these aren't caused by malicious actors doing anything especially clever; it's usually caused because something has been left unencrypted, or a well-known vulnerability left unpatched.

Arm is trying to do as much as we can to support the industry to move in the right direction, but, ▶

[1] https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

unfortunately, my money is on the situation remaining more-or-less the same for many years to come.

AS: Often, we think of IoT as a market, but actually, it's a collection of markets. A cheaply manufactured consumer device has cost as the most important consideration, whereas other use-cases and verticals do genuinely prioritise security.

Five years ago, for example, carmakers wouldn't bother with a secure system-on-a-chip (SoC) design, but now they won't even talk at all without a secure SoC being available. For the utility, automotive, and other industries, the bar is rising and the conversation about security is being held relatively early. I've worked with some of the biggest names in the auto industry, and security was once just an afterthought. Now, that's not the case, it's front and centre.

Sometimes it's regulation that causes this change, but sometimes it's just a case of an attack or an incident going viral that casts a spotlight on security and results in the market reacting. In automotive, the trigger was the Jeep Cherokee hack that saw hackers take control of the systems of a vehicle driven by a Wired magazine journalist. Things like this mean the conversation evolves.

GM: What are the realities of device-level security? There's no such thing as complete security, but what comfort level needs to be achieved?

AS: You're right, and this is where threat modelling helps by juggling the anticipated threats, the required usability, and the desired cost to mitigate. Customers may start by aiming for full security, but when they understand the implications on cost, they may be willing to compromise here and there. Alternatively, there may be implications on the production line with embedding greater security. Also, if your actual production line isn't secure, you have a black hole, and it can be complicated and costly to address. Some trade-offs are possible and a good security model can balance the three issues.

GM: How can Arm help?

DJ: I think the Arm difference is measured by the value that we add throughout the various stages of the IoT device life cycle. For example, we take care of 70-80% of the fundamental, but mundane, security coding required during the application software development phase; this can have a dramatic impact on your time-to-market. Another example involves ensuring that the chain-of-trust has its foundation in secure, trusted identity, and Pelion establishes this at the very earliest opportunity: in device production. We inject the device with a cryptographic key and a certificate. During activation and on-boarding, we use this embedded identity to secure and authenticate communications with both the device management service and the data management platform.

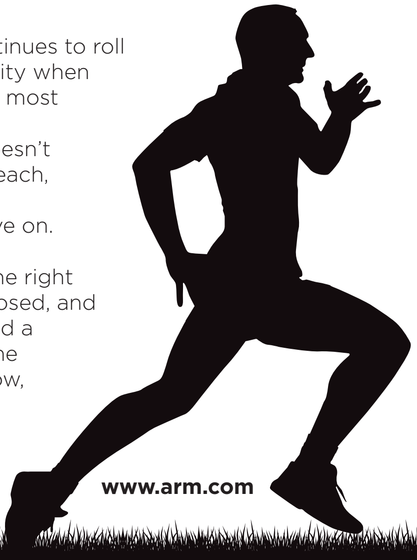
Additionally, the techniques for securely storing and applying over-the-air updates are all managed by the Pelion service; it's essential to ensure that everything that runs on the device is valid. Typically, when the device's firmware or the IoT application software are improved, or a patch is needed to fix a bug or a security vulnerability, you need to apply an update. We ensure this process is securely executed, with signed updates, and an anti-rollback control. There's a surprising amount of device functionality needed to ensure the integrity of the process, and that device availability isn't compromised due to an update being incorrectly applied.

And finally, something that is overlooked, or at least minimised, is the life-long need to monitor device health. We've pioneered a capability to detect and report on anomalies. Collecting specific device operational metrics - for example, CPU and memory utilization - provides insight into how the device is performing relative to accepted baselines. Proactively checking for deviations could be indicative of a software bug that will accelerate battery drain or a cyberattack that's attempting to establish unauthorised connections.

AS: Pelion provides a security framework that extends across the device's end-to-end life cycle. Many times, security rules are broken when companies attempt to stitch things together from multiple sources and do that in a way that isn't secure. We don't sell the chipsets or the devices; we provide the building blocks to run everything and ensure the secure interoperation of systems and devices.

Security is a topic that continues to roll on. We'll see spikes of activity when exciting things happen, but most security breaches still go unnoticed. If a carmaker doesn't need to run and tell of a breach, it won't. They just quietly address the threat and move on.

Astute organisations find the right balance, so they're not exposed, and hackers go elsewhere to find a softer target. That's been the story of security up until now, and it will probably continue that way. ■



www.arm.com

IoT devices at the centre of a storm of cybersecurity badness

The need to secure IoT devices is nothing new but organisations are still forgetting to address the basics – even in the face of a radically enlarged threat surface, George Malim

Too often, poorly secured IoT devices are still providing a backdoor into enterprise systems, allowing malicious actors to cause huge financial and reputational damage to businesses. Organisations, in the rush to compete and win in IoT, have neglected security and there will be a price to pay for that.

"In the race to market IoT devices, security is all too often an afterthought," confirms Max Heinemeyer, the director of Threat Hunting at **Darktrace**. "Smart manufacturers need to think about security earlier in the development process and make it a priority – and allow for easier integrations into a company's existing security infrastructure."

For Nigel Stanley, the chief technology officer at **TUV Rheinland**, device-makers must also shoulder their share of the blame. "The biggest threat is the lack of motivation for manufacturers to ensure they have thought about security issues," he says. "Device design and procurement are driven by cost, and price seems to trump everything. Manufacturers need to think about the impact on their reputation if they are seen to be shipping dodgy, insecure products."

Part of the problem is securing devices isn't simple. "Embedded systems in IoT devices typically have a small footprint, and so too much security functionality can hinder the performance of a device or system, plus it's likely to increase the overall cost of development," says Arlen Baker, the chief security architect at **Wind River**. "The trick lies in building just enough security to mitigate a breach."

So, what is just enough? "This can be worked out using three key criteria," says Baker. "First, the environment - where will the device be deployed; will it be used or accessed by a few people, or several hundreds? Second, access points - how will the device connect and communicate; is it behind a firewall; how much encryption does it need? Third, storage - what kind of data is the device storing and is the data highly sensitive?" ▶

Anna Stergioula, the head of security at **Pod Group**, acknowledges the processing power challenge but also has concerns about the sheer number of IoT devices in deployment. "IoT devices simply don't have enough processing power to host traditional IT security solutions such as firewalls or antivirus," she says. "This makes on-device security tricky to achieve for connected devices, and companies might find themselves compromising on IoT security while beefing up IT security to compensate.

"Due to their limited protection and wide proliferation, IoT devices are far more of a target than typical IT endpoints," she adds. "It also makes no difference where a hacker gains access, so it makes sense to target IoT devices as the weakest link in a network of devices."

Kevin Curran, a senior member of the IEEE and professor of cybersecurity at **Ulster University**, points out that IoT is never at rest so the security requirement is always changing. "IoT ecosystems are dynamic and in constant evolution," he says. "As a result, IoT threats are dynamic and consistently move across the stack, from the firmware and hardware level to the application plane. One key threat is to compromise the human element of the IoT value chain: impersonating a user, stealing their credentials, and circumventing weak biometric authentication deployed in silo modes, is often the easiest way to compromise IoT solutions."

Boris Balacheff, an HP fellow and chief technologist for Security Research and Innovation at **HP**, also emphasises the sheer scale of the IoT device security challenge. "Every connected device out there is a potential target for bad actors," he explains. "This means we must consider IoT devices, in the home, the office or public spaces as threats that will be targeted. This is an issue because many IoT manufacturers only offer very basic, if any, device security, and very little manageability support. Devices that are insecure by design, or poorly managed, will create opportunities for attackers, and can lead to breaches of individuals' privacy, to compromise of business or home networks, or even to attackers mounting larger-scale cyber-attacks."

Heinemeyer warns that IoT is often seen as a soft target. "The lack of visibility into the Internet of Things has enabled cyber-attackers to manipulate and exploit it as low-hanging fruit," he says. "IoT devices now far outnumber human beings, and the challenge of identifying all such devices on an organisation's network, from corporate CCTV cameras to parking payment kiosks and smart lockers, has become a task too great for human security teams."

That widely spread of threats adds to the complexity. "Securing assets connected to the Internet of Things is a multi-layered issue," says Tara MacLachlan, the vice president of Industrial IoT Strategy at **Inmarsat**. "Whether it's the physical security of endpoints, the authentication of connected devices, the security of application software, or the connections between IoT devices and the central network, any given IoT system requires attention to the physical devices, as well as a device's operating firmware and software."

"Adding complexity to this landscape has been the emergence of edge computing for the IoT," she adds. "For all the benefits that edge computing brings, from a security standpoint collecting data at the edge can add further security problems. This is because a network's potential attack surface increases with each new device added to the network and these devices may not be as secure as a centralised or cloud-based system. In addition, the small physical size of many edge devices makes them vulnerable to theft or physical attack."

For Simon Wilson, the chief technology officer for the UK and Ireland at **HPE Aruba**, the nature of IoT itself is a security threat. "A key threat is the IoT market itself," he says. "Small IoT devices are relatively cheap to develop, which has created a burgeoning ecosystem of start-ups developing things on a daily basis. Many of the manufacturers we see in the market today will either have moved on to newer things or disappeared from the market entirely. The real risk is that these devices will remain in use, sometimes because we've forgotten that they were there, vulnerable to exploits and un-patchable because there is nobody developing the patches."

Security can always be achieved if you take away the constraints of time, cost and processing power and efforts are being made to balance all these to achieve the 'just enough' device security described by Baker earlier. In the meantime, the Internet of Things is left with the need to be pragmatic.

"Things won't change overnight," confirms Balacheff. "And, while many IoT devices are not designed with security in mind, businesses must carefully manage what is out there already, consider network isolation and network monitoring solutions, or where relevant, not allow certain devices in the environment."

For Curran, uncertainty creates anger. "The IoT market, like cybersecurity, is doomed by vendors' statements that often are more aspirational than real: all this creates confusion and exposes the end-user to the risks of a false sense of security," he says.

Further gaps that need to be closed lead Stanley to take a bleak view of the future. "Cost and price are a big issue, as is the lack of operational technology (OT) cybersecurity expertise," he says. "Finding someone that understands cybersecurity and process, IoT and OT engineering is a challenge. Against this, we have ever-increasing threats from hacktivists through to nation-state actors providing a perfect storm of cybersecurity badness in the world of IoT and OT."

Kevin Curran, Ulster University

Max Heinemeyer, Darktrace

Nigel Stanley, TUV Rheinland

Anna Stergioula, Pod Group

EVENT DIARY

While we have made every effort to ensure the accuracy of this listing, the current COVID-19 pandemic means that many events are changing timing, dates and locations. Therefore please check at the events' websites to ensure details are up-to-date before travelling.

Smart City Expo Atlanta
Atlanta, USA
10-11 June, 2020
smartcityexpoatlanta.com

4th Internet of Manufacturing MW
Chicago, USA
15-17 June, 2020
iom-mw.internetofbusiness.com

Internet of Supply Chain
Chicago, USA
16-17 June, 2020
iosc-mw.internetofbusiness.com

MWC Shanghai 2020
Shanghai, China
30 June - 2 July, 2020
www.mwcshanghai.com

Internet of Things World
San Jose, USA
10-13 August, 2020
tmt.knect365.com/iot-world

TU-Automotive Detroit 2020
Detroit, USA
18-20 August, 2020
automotive.knect365.com/tu-auto-detroit

5G World
London, UK
1-3 September, 2020
tmt.knect365.com/5gworldevent

MVNOs World Congress
Berlin, Germany
1-4 September, 2020
tmt.knect365.com/mvnos-world-congress

IoT World Europ Summit
London, UK
2-3 September, 2020
tmt.knect365.com/iot-world-europe

AR&VR World
London, UK
2-3 September, 2020
https://tmt.knect365.com/ar-vr-world

Blockchain for Business
London, UK
2-3 September, 2020
tmt.knect365.com/blockchain-business-summit

Cloud and Devops World
London, UK
2-3 September, 2020
tmt.knect365.com/cloud-devops-world

AI & ML for the Smart Grid 2020
Brussels, Belgium
8-10 September, 2020
www.smartgrid-forums.com/forums/aiml-for-the-smart-grid

Utility Cloud 2020
Amsterdam, The Netherlands
15-17 September, 2020
www.smartgrid-forums.com/forums/utility-cloud

Digital Transformation North America
Dallas, USA
21-25 September, 2020
dtaw.tmforum.org

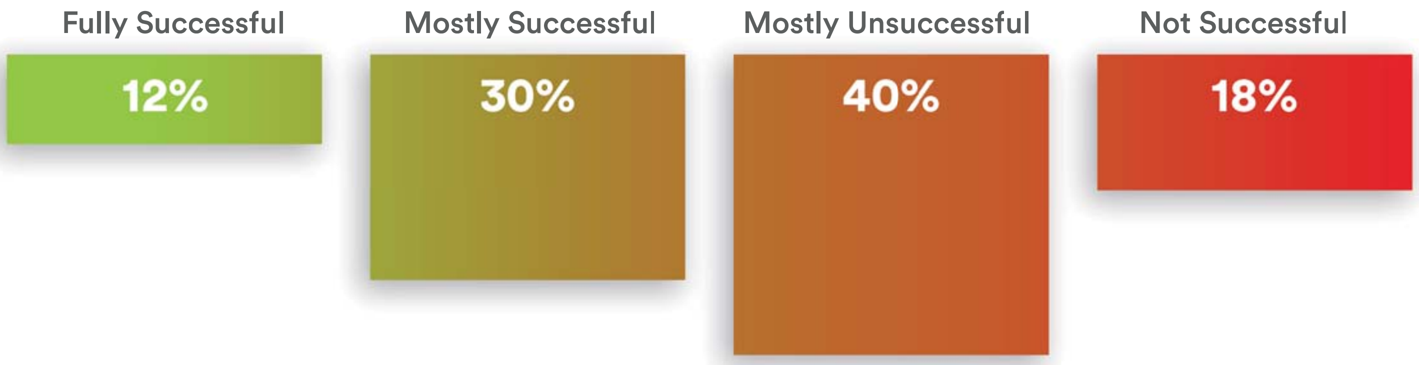
Big 5G Event
Austin, USA
22-24 September, 2020
tmt.knect365.com/big-5g-event

MVNOs Asia
Hanoi, Vietnam
28-30 September, 2020
tmt.knect365.com/mvnos-asia

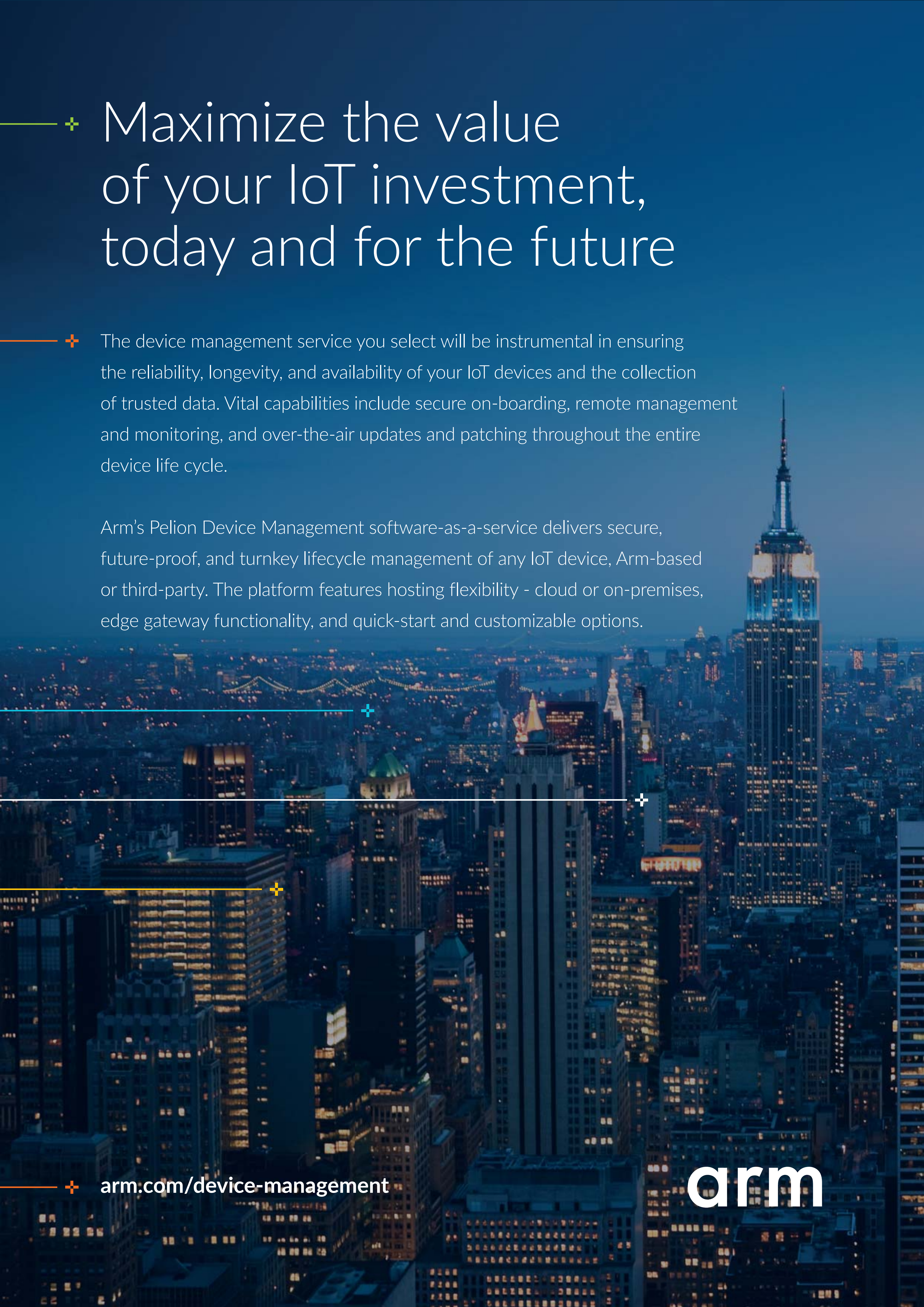
IoT World Asia
Singapore
29 September - 1 October, 2020
tmt.knect365.com/iot-world-asia

5G Asia
Singapore
29 September - 1 October, 2020
tmt.knect365.com/5g-asia

Grid Asset Management 2020
Brussels, Belgium
29 September – 1 October, 2020
www.smartgrid-forums.com/forums/grid-asset-management


Fully Successful
12%
Mostly Successful
30%
Mostly Unsuccessful
40%
Not Successful
18%

Why IoT Projects Fail
br
And What To Do About Them
Why IoT Projects Fail
beecham research
Shaping the IoT future



Maximize the value of your IoT investment, today and for the future

The device management service you select will be instrumental in ensuring the reliability, longevity, and availability of your IoT devices and the collection of trusted data. Vital capabilities include secure on-boarding, remote management and monitoring, and over-the-air updates and patching throughout the entire device life cycle.

Arm's Pelion Device Management software-as-a-service delivers secure, future-proof, and turnkey lifecycle management of any IoT device, Arm-based or third-party. The platform features hosting flexibility - cloud or on-premises, edge gateway functionality, and quick-start and customizable options.

arm.com/device-management