IoT Now: ISSN 2397-2793
Q3 2019 • VOLUME 9 • ISSUE 3

IoT now

HOW TO RUN AN IoT ENABLED BUSINESS

TALKING HEADS

Everynet's Lawrence Latham explains how interoperable and open networks build the IoT ecosystem at minimal cost

AGRICULTURE
IoT efficiency in the field. See our Analyst Report at **www.iot-now.com**

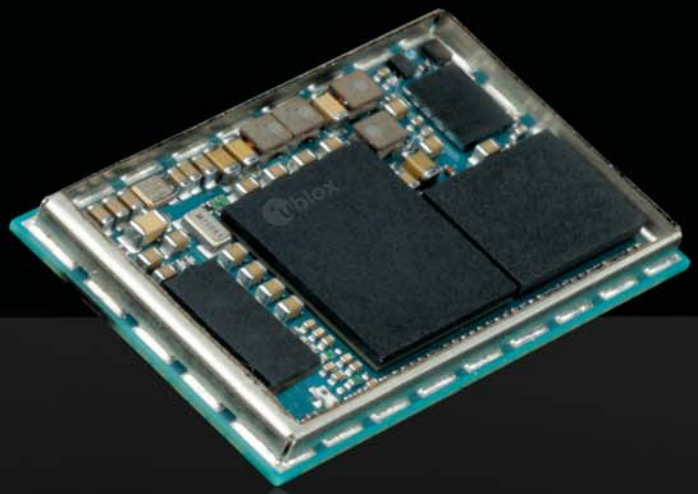
INDUSTRIAL
How IoT is improving operations. See our Analyst Report at **www.iot-now.com**

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

SMART HOMES
New efficiency for living, working and playing. 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: 6-PAGE SMART HOMES REPORT: Will whole-home systems dominate point solutions as the market matures? • How IoT at the edge adds value for enterprise IoT users • Why collaboration can lead to an improved IoT data monetisation model • It's time to stop dirty devices dragging down smart home security • Will IT and OT integration pave the way for artificial intelligence? • Why smart buildings will flourish only when whole life costs are considered • Frameworks for IoT device security reviewed • Inside the high risk world of securing IoT healthcare • Are some IoT devices too smart to be secure? • News online at www.iot-now.com



SARA-R5 LTE-M and NB-IoT module:

IoT security for a better, safer connected world.

www.u-blox.com/sara-r5

CONTENTS

IN THIS ISSUE

This season's latest technology trends have a new catwalk

As you read this issue, as usual, you'll encounter a vast array of different technologies many of which are identified by descriptive words to help us navigate the complex and convoluted maze of technologies upon which the Internet of Things is built. Classic horizontal categories such as information technology (IT), communications technology and operational technology (OT) are being joined by data management technology and edge technologies along with a slew of vertical technologies designed for specific industries or specific technological ecosystems.

Technology, regardless of the word appended in front of it, is what it always has been; a tool or set of tools to enable business cases, processes or functionality. The additional words help to categorise and identify the likely applications and composition of a specific technology and help users short-circuit the need to understand everything. They enable specialism and for expertise to be developed in clearly demarcated functional areas.

However, they also enable a hypecycle to be created which can be as damaging to clarity as it is helpful to understanding. Digital transformation technology, for example, has become almost meaningless as the transformation tag is added to almost anything from air conditioning to zookeeping. Sometimes these tags create a form of industry shorthand to describe the latest technology trends and this is valid, useful and helpful as complicated new concepts are explained and the value of specific functionality is outlined. People know that if a term such as digital transformation or edge intelligence is used, the conversation is about the introduction of internet-enabled business models or the idea of having more powerful devices at the edge to enable distributed decision-making.

These tech trends form the basis of a new form of communication that is needed to clarify, segment and explain innovation and how it will benefit users, enterprises and those who supply it. IoT is so large and so multi-dimensional that this segmentation is vital to enable insightful explanation and clear demarcation between various technologies and disciplines. This issue of **IoT Now** certainly contains numerous technologically distinct topics and these range from LoRaWAN to edge computing, to digital business, to smart buildings and encompass security and smart home automation.

For this reason, our sister publication **IoT Global Network** has launched a new series of technology-specific publications, called **IoT Global Network Tech Trends**, which focus in-depth on a distinct technology area. The first Tech Trends publication, titled 'IoT at the edge opens up a whole new world' is out now at **www.iotglobalnetwork.com** and is free to IoT Global Network members. It contains specially-commissioned features, interviews and use case examples in addition to an analyst report that details how the edge has developed and where innovation is likely to take it next.

We hope our readers will find that the technology-specific, in-depth Tech Trends publications augment the content of IoT Now and provide them with detailed insights into the latest technical innovations.

Enjoy the magazine and our latest Tech Trends!

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:

Robin Duke-Woolley, chief executive, Beecham Research

Saverio Romano, strategic advisor, IoT Analytics

Martin Bäckman, IoT analyst, Berg Insight

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 807411

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

Hoopo raises US$3.5m in seed funding from GiTV, Chartered Group and TAU Ventures

Hiro Mori, Toshiba of Europe

hoopo, a geolocation specialist that claims high-accuracy low-power capabilities via the Internet of Things (IoT), has secured a US$3.5 million (€3.1million) funding round from **Chartered HighTech** JIHTV1 fund, **TAU Ventures**, and **Global IoT Technology Ventures** (GiTV).

hoopo has now raised a total of US$5 million, including previous rounds from the initial investors in **Mobileye**; Israeli investor, Zohar Gilon; and Ben Marcus, co-founder and chairman of **AirMap**.

The company was founded in Israel by a team of experts with more than 120 years of combined experience in RF communications and tracking systems. Its unique technology enables GPS-less geolocation by providing accurate positioning for low-power devices. With this latest round, hoopo will scale up the business operations on a national and international basis.

hoopo's geolocation solution enables companies to locate their valuable assets utilising low-power wide area (LPWA) networks, without the significant cost or battery consumption that can be associated with GPS.

"hoopo's innovative solutions are transforming the possibilities of asset tracking," said Mr. Hiro Mori, general manager of Israel Development Office at **Toshiba of Europe**. "For a while now, we have been searching for an ultra-low-power tracking solution that is capable of providing high accuracy for our various use-cases and we are happy to have identified hoopo as an ideal solution for our clients."

Antonio Pietri, Aspen Technology

Aspen Technology acquires Mnubo and Sabisu for IoT tech

Aspen Technology, a global provider of asset optimisation software, has signed an agreement to acquire **Mnubo**, a Montreal, Canada-based provider of purpose-built artificial intelligence (AI) and analytics infrastructure for the Internet of Things (IoT). Mnubo enables industrial companies to assemble and deploy AI-driven IoT applications quickly, at enterprise scale. The Mnubo technology will accelerate the realisation of AspenTech's vision for the next generation of asset optimisation solutions that combine deep process expertise with AI and machine learning.

In addition to deploying AI-powered applications, the ability to visualise vast quantities of information and analysed data is critical to the evolution of the smart enterprise. To further enhance these capabilities AspenTech has acquired **Sabisu**, a UK-based company that provides a flexible enterprise visualisation and workflow solution to deliver real-time decision support.

"The actionable insights from AI powered applications will help AspenTech customers to achieve a truly smart enterprise. I am delighted to welcome the highly talented teams from both Mnubo and Sabisu to AspenTech," commented Antonio Pietri, the president and chief executive of Aspen Technology.

Frédéric Bastien, the co-founder and CEO of Mnubo, added: "The global adoption of AI and IoT technologies is powering the next wave of industrial-digital enterprises. Our location in Montreal's world-class AI ecosystem enables AspenTech to establish a Centre of Excellence for these cutting-edge technologies, and to attract some of the best talent in this space. We are very excited to continue to develop innovative AI solutions that target IIoT at enterprise scale, under the AspenTech umbrella."

NEWS IN BRIEF

Wireless Logic Group buys Matooma for European growth

Wireless Logic Group, a European IoT connectivity platform provider, has acquired **Matooma**, a Montpellier, France-based IoT connectivity specialist established in 2012. Today, Matooma claims a broad base of customers using its secure network solutions across multiple applications.

The Matooma acquisition, for an undisclosed sum, is Wireless Logic's third purchase in 2019 following deals to acquire Dutch-based **M2MBlue** and **SIMPoint** in February and June respectively. The three new organisations join the UK-headquartered IoT connectivity platform provider as it continues expansion throughout its European network.

Commenting on the most recent acquisition, Oliver Tucker, group CEO of Wireless Logic Group, said, "We are delighted to be welcoming the Matooma team into the group. In just seven years, they have built an enviable reputation in France by delivering highly responsive and tailored IoT connectivity services, supported by exceptionally strong leadership."

IMS Evolve and Current partner to deliver IoT-enabled savings

Industrial Internet of Things (IIoT) company, **IMS Evolve**, has announced a strategic partnership with **Current**, powered by **GE**, to deliver IoT solutions to the food retail sector.

The partnership uses IMS Evolve's integration and automation capabilities and Current's Daintree wireless controls infrastructure to offer a solution that is helping food retailers reduce operational costs and improve the customer experience.

The new partnership aims to achieve significant savings across energy, waste and maintenance by exploiting real-time data from assets across the enterprise. A popular US regional grocer recently installed the new unified IMS/Current solution across nearly 200 stores and is on a path towards saving hundreds of thousands of dollars in the coming months simply by identifying and removing excess defrost cycles in refrigeration cases, the companies say.

NEWS IN BRIEF

Berg Insight reports 18m North Americans used connected care solutions in 2018

A new report from analyst firm **Berg Insight** has found that around 18 million people in North America were using connected care solutions at the end of 2018. The figure encompasses users of medical alert systems, connected medication management solutions and remote patient monitoring (RPM) solutions in Canada and the US. RPM is the largest and most mature connected care segment having a total of 16.1 million users at the end of 2018.

The market for medical alert systems is considerably smaller with an estimated total of 3.1 million users, whereas the number of connected medication management users reached 900,000 at the end of 2018. There is an overlap between the market segments as medical alert users can also be equipped with a medication management solution or an RPM solution, and vice versa hence the estimate of 18 million total connected customers. The market is forecast to grow at a compound annual growth rate (CAGR) of 18.3% during the next six years to reach 49.4 million connected care users by 2024.

Consumer robotics shipments to reach 74mn by 2024 as coding tools become ubiquitous

A new study from **Juniper Research** predicts that more than 74 million consumer robots will be shipped in 2024, up from an estimated 28 million in 2019. It also forecasts that vendors' focus on educational features in consumer robots, such as coding tools, and adding features to established device ranges will increase the consumer value proposition; driving the growth of consumer robotics adoption over the next five years.

The new research, *Consumer Robotics: Sector Analysis, Leading Innovators & Market Forecasts 2019-2024*, found that shipments of domestic aide robotics, including robot vacuums, mops and lawnmowers, are forecast to reach 47 million in 2024 from only 19 million in 2019. It also forecasts that the domestic aid segment will account for nearly two thirds of global consumer robotics shipments by 2024.

M2M connections to exceed 1.6bn by 2024 driven by eSIM adoption, says Juniper Research

Elson Sutanto, Juniper Research

A new study from **Juniper Research** has found that the global number of cellular M2M connections will reach 1.6 billion by 2024; rising from 596 million in 2019. This represents growth of 165% over the next five years. The firm forecasts that remote provisioning and innovative anti-fraud measures enabled by embedded SIM (eSIM) technologies will drive adoption of cellular M2M services in key sectors including automotive, smart cities and connected agriculture.

The new research, *M2M: Key Verticals, Technology Analysis & Forecasts 2019-2024*, found that adoption of eSIMs will grow 350% over the next five years to exceed one billion eSIMs globally by 2024. It urged eSIM vendors to add modules that support emerging technologies, including 5G and low power M2M networks, as soon as possible to increase adoption.

Research author Elson Sutanto said, "eSIMs will continue to be essential in accelerating the adoption of M2M services. Offering the eSIM standard across all cellular technologies will maximise the technology's value across all M2M sectors."

The research also found that 5G's impact on the M2M market will be limited in the periods. It forecast that only 15 million 5G connections will be in use by 2024, after initial commercial network launches this year. The research anticipated that the automotive sector would be the primary industry adopter over the next five years; accounting for 70% of 5G M2M connections by 2024.

Deutsche Telekom and Software AG partner to create global Cloud of Things platform

Deutsche Telekom and **Software AG** have announced a strategic partnership to deliver IoT services on a global scale. Deutsche Telekom and its enterprise customer unit **T-Systems** will expand their Cloud of Things offering, using Software AG's Cumulocity IoT platform.

Adel Al-Saleh, the chief executive of T-Systems and board member of Deutsche Telekom, said: "We're delighted to be extending the reach and capabilities of our Cloud of Things IoT platform alongside our partner. Software AG's technology is critical in enabling us to scale an already successful service and introduce new functionality, giving us the confidence to move into new sectors. Our strategic partnership will help us continue to drive innovation and provide the best possible platform and services for clients, both from the enterprise sector and Germany's world-leading Mittelstand."

Adel Al-Saleh, T-Systems

Sanjay Brahmawar, the chief executive of Software AG, added: "This is a new way of partnering and co-operating to offer complete IoT solutions for the real-time economy. Customers can simplify their IoT and integration needs with self-service analytics and gain insights to accelerate their businesses for the fully connected future. We look forward to scaling this partnership and making it a global success."

Former Tata Communications' director joins SIMO Corporation as CEO of IoT and B2B business unit

Ludovic Lassauce, SIMO Corporation

SIMO Corporation, the parent company behind Skyroam, a portable Wi-Fi device, has announced the establishment of a new IoT and B2B business unit, with **Ludovic Lassauce**, former head of mobile and Internet of Things in the Asia-Pacific region for **Tata Communications**, appointed as chief executive. The new business unit will enable any third party devices with its virtual embedded SIM (eSIM) technology that the company claims is already serving more than ten million Skyroam Wi-Fi users globally.

SIMO Corporation's virtual eSIM technology has been developed and used for over ten years and has many worldwide patent, with a total of more than 100 million users relying on its global connectivity service platform. The virtual eSIM service eliminates the barrier for OEMs to integrate connectivity into their devices by removing any physical SIM card.

Ludovic Lassauce, CEO of SIMO Corporation's IoT & B2B division, said: "I am glad to join SIMO Corporation to offer the best services to these OEMs and create an ultra-connected society in which billions of intelligent Internet of Things devices can be always connected to improve our daily life thanks to our powerful virtual eSIM service."

Lassauce led Tata Communications' mobile and Internet of Things business in the Asia-Pacific region, making it the fastest growing business for Tata Communications. Prior to joining Tata Communications, he served as the general manager for IoT in Singapore Power, the state grid company from 2015 to 2017, creating various smart building solutions.

Tachyum appoints Kiran Malwankar vie president of system engineering

Tachyum has appointed **Kiran Malwankar** to the position of vice president of System Engineering. Malwankar, a 30-year veteran of both pre-IPO companies and industry leaders, holds 21 US patents in technologies such as I/O virtualisation, PCIe, storage virtualisation and flash/solid-state media.

Malwankar joins the company after founding or joining a series of successful start-ups that delivered innovations in memory, artificial intelligence (AI), IoT, cloud and flash devices; five of these companies were acquired and one went public. In addition, he has held executive and senior-level engineering positions at dominant vendors such as **Cisco**, **Violin Memory**, **Nishan Systems/McDATA**, and **Aprius/FusionIO**. He holds a master's degree in electrical engineering from the Indian Institute of Technology in Mumbai.

"I am honoured to oversee Tachyum's breakthrough processor architecture and bring it to today's most interesting applications and environments – supercomputing, hyperscalers, AI, deep machine learning, edge computing and IoT," said Malwankar.

Interoperable and open networks build the IoT ecosystem at minimal cost

Lawrence Latham is the chief executive of Everynet, the provider of wholesale LoRaWAN networks for IoT. The company is building out national networks across the globe with the aim of providing robust nationwide capacity to wholesale customers at a cost that stimulates trial of new IoT use cases. Here, he tells IoT Now managing editor George Malim, how the company differs from a traditional network provider and what his plans are for developing the business further

George Malim: Why have you decided to build out national wholesale networks?

Lawrence Latham: We realised that what IoT really needs is a means for organisations to have access to network capacity so they can trial new use cases at minimal cost. If you can bring down the cost of a trial to a few dollars per year, suddenly the barrier to trialling is removed and innovators and use case owners are empowered. Some will succeed and some will fail but the cost of failure doesn't have to be prohibitive.

GM: Why have you chosen LoRaWAN for these networks?

LL: If you're an operator today the choice is confusing. If you're looking at LTE-M you need to understand how much it will cost – the upgrade isn't free. You could also consider narrowband IoT (NB-IoT) or unlicensed alternatives but the challenge of understanding the options and making a choice remains. And, you're trying to do this at the same time as your focus in on your 5G consumer business and investing in 5G.

So much of the focus is on what happens in the US or western Europe but these markets are not representative of the other places in the world. To have LTE-M or NB-IoT, which are complementary to LoRaWAN, you have to have 4G networks in place and you need these to have ubiquitous coverage and then you need to pay for the base station upgrade.

Looking at all these different solutions may be a career-defining decision so what's an operator to do? In the past, the operator would have taken the gamble with LoRaWAN and made the capex to build the network and own it 100%. Now though, the capex is a significant burden and owning the network doesn't help create the ecosystem. If you do it all yourself you get all of the risk, all of the opex and all of the capex but you don't bring partners in to share the risk and the reward and these partners, critically, are able to help in building the ecosystem.

I think low power wide area networks (LPWANs) have been mis-named, the most important thing isn't the low power, it's the low cost. Perhaps we should be talking about LCWAN instead because cost to me is just as, if not more, important than power consumption to achieve scale.

People talk about the network technologies without really engaging from a business economics point of view. Price elasticity really does matter and can make or break an IoT use case. Pennies matter. LoRaWAN means we can bring the appropriate amount of capacity to a market at a very low cost and this creates opportunities.

GM: You're adamant that Everynet doesn't want to become an enterprise supplier or sell directly to use case owners. Why have you taken this approach?

LL: We don't sell gear and we don't sell licences to wholesale customers either. All we do is sell them the airtime on a pay-as-you-grow model. We build and manage the coverage and are able to give our wholesale customers their own private secure network server so they control access to the network. This keeps it simple for us – we want to have no more than ten clients in any country.

We think there's an important role for us to play. If one mobile network operator builds this capacity, it's proprietary and enterprises hate being stuck with one operator. By selling capacity to multiple wholesalers we enable enterprises to have a choice of providers while keeping the financial cost of the network low. A country only needs one set of LoRaWAN infrastructure, there is no business rationale for building competing networks because the capacity is sufficient and the cost of replicating the same base infrastructure is prohibitive. Unlicensed spectrum is shared spectrum, so building duplicate networks offers no advantages and only adds costs.

We certainly will only enter markets where there is no LoRaWAN network because there's no logical argument for building two networks, it just adds cost.

GM: How do you select which markets to enter?

LL: The first question is whether there is a public network planned or already in place. If the answer to that is yes, we move on to the next country for the reasons I gave earlier. Next we look at what the payback will be. We typically require a wholesale partner and an anchor use case or two to move things forward. However, a great advantage we have is that we can see what's working in our other countries and we'll share information on what's happening in our ecosystem if you share what's working in yours.

In general, though, we want to go to places where there aren't national networks and low GDP per capita countries are where this type of network can be extremely successful. Even if cellular solutions existed, the market couldn't afford them so, because we've figured out how to cost effectively build and deploy networks, we can really stimulate IoT. Our networks in Latin America, for example, work better than the cellular network in terms of coverage and performance for IoT applications.

Our goal by 2023 is to cover 25 countries.

GM: To what extent does Everynet have a role in terms of stimulating usage of IoT?

LL: A lot of countries have struggled with the costs of IoT networks and they need their own business cases to be built. We have field service engineers and enablement teams that help each of our partners to integrate the solution with customers' own systems as quickly as possible. We have application engineers and hardware people that can help with devices, to get up and running and to ensure connectivity is available.

Our ecosystem means the cross-pollination of ideas from country to country is possible but the most important thing is that we realised early that IoT is not going to be able to scale up radically until connectivity becomes a virtual commodity. Our model of deploying at minimal cost makes this a reality and, while being interoperable and open flies in the face of the traditional proprietary model, I believe it's what IoT needs and as billions of devices connect using LoRaWAN, the low cost IoT market will be the one where most of the action is.

How Everynet goes to market

Selling capacity to a small number of wholesale partners presents a very different business model to a traditional network supply business and Everynet has developed a portfolio of go to market capabilities to support its customers. The company's chief customer officer, Tom Nelson, explains what this involves

GM: How does Everynet go to market?

Tom Nelson: We're doing very innovative work in building out neutral wholesale networks via LoRaWAN. As part of that, we're very involved with our partners and have built a go to market programme for them where we help them on-board to the network, enable best practice and help them quickly monetise and enable scale.

Our visibility into implementations around the world means we can draw on our experience and help them explore go to market projects and drive awareness.

Our technology readiness programme exists to help partners take advantage of LoRaWAN. There's a very robust ecosystem surrounding LoRaWAN and we can help make introductions for the hardware, software, testing and other capabilities partners require. We can package these together to help partners launch quickly.

Our commercial on-boarding track focuses on working with partners, often on-site in workshops, to think through use cases. There are massive opportunities in terms of LoRaWAN use cases from smart cities to green initiative and asset tracking to marine solutions. Our sales enablement tools mean we can also help partners identify use cases that are likely to be successful and then help them launch quickly so they can generate revenues rapidly.

GM: How do you make your knowledge from other markets available to partners?

TN: We are open and interoperable and helping to enable the LoRaWAN ecosystem by placing that on the network with a variety of use cases. This gives us an edge over single country network providers because we have realised that best practices work in a variety of countries so we'll share these across markets. Of course, behaviours might be different from market-to-market so we provide support to get solutions into the market and drive devices so our partners get volumes of connections.

GM: In what ways do you see LoRaWAN developing in the coming years?

TN: This space is really exciting to me. If you take a look at the new use cases and solutions that are being introduced they will ultimately help enterprises reduce cost, increase revenues or achieve both.

What's particularly exciting is that Everynet is not just about one country and LoRaWAN is a common element globally. We are helping in a consultative manner where our customers need it. Now is a really interesting time because we have networks in place and real examples of how we are reducing the cost of IoT and driving new revenue for our partners. ▶

Our visibility into implementations around the world means we can draw on our experience and help them explore go to market projects and drive awareness.

Chris Stone,
Everynet

The chairman's view

Chris Stone became chairman of Everynet in 2017 and has held c-level positions at a range of technology-related businesses. Most recently he served as chairman of CityFibre, a UK-based provider of fibre infrastructure that built out a nationwide network of wholesale capacity before being sold to a Goldman Sachs-backed consortium in 2018. Here he explains the similarities between building a fibre infrastructure business and the goal of rolling out low cost IoT networks at immense scale

George Malim: What attracted to you to become chairman of Everynet?

Chris Stone: I could see the parallels between what we achieved at CityFibre and what Everynet is doing. Building a neutral host network for service providers to monetise is a really attractive model. Fibre has a bandwidth model that is the polar opposite to low cost IoT connectivity yet the same rules apply.

When you deploy fibre, the thing that gets in the way are the permissions you need to put the fibre in. You also have to do it all in one go and once you've built the network the rationale for somebody else to build capacity in the same place is very low. The capacity is extremely large and the cost of the build is great so there's no incentive for competitors.

CityFibre determined that the unit of construction for fibre is a city and targeted cities to gain permissions so, once the capacity was built, wholesale operators and mobile operators all came to us so they could start selling their products and services over the network. You sign up lots of operators very quickly.

The same thing is true with LoRaWAN networks in the world. However this time, the unit of construction in a country rather than a city. If you build at a country level, the capacity of a LoRaWAN network, although individual packet size is small, means you can handle billions of packets. Nationwide LoRaWAN networks will be able to handle billions of connections.

The idea is to build national networks and provide them to wholesale customers. I like this model because once you've built the network the owners and developers of the use cases don't have to think about where or how they'll access connectivity.

GM: Although the service is low cost, building national wireless networks is capital intensive. Isn't it a major challenge to raise the financing?

CS: It's true that this is a business that requires capital upfront to build networks. With CityFibre, we sold the equity for a lot of money to big infrastructure providers once we'd proved the model. We raised £250m by selling equity and took on debt of £250m to get started and, since its sale, the new owners have committed to spending £2bn to continue.

Investors are comfortable with this because customers of networks are very sticky. Once you give a customer a full fibre connection in the UK they're never going back to what they had before. The same is true in IoT. Once you get used to having the information that IoT devices generate, you're never going back to business without it.

GM: How dependent are you on owners of use cases coming to market at great scale?

CS: The great thing about the business model is the volume layers up and up and up. What we've been really focused on is to take away the barriers to trial for whoever it might be so they can take forward a use case. For example, if I was a printer company in Brazil and I wanted to know every time a printer moved location, I could decide to put trackers on 2,000 of my printers and get to an average cost of US$5 per device. The cost of trial needs to be acceptably low to open up new opportunities and encourage people to try. If it works great but if it doesn't the cost hasn't been prohibitive. It's this that will truly drive volumes. ■

www.everynet.com

How IoT at the edge adds value for enterprise IoT users

A few years ago it was fashionable to argue that all Internet of Things (IoT) data must end up in the cloud and that all of the really smart stuff was therefore in the cloud, writes Robin Duke-Woolley, the chief executive of Beecham Research. That was a throwback to the machine-to-machine (M2M) era, in which data from all connected devices was expected to be sent to a central server for processing and subsequent distribution of the information created. That approach was the most cost-effective method given the types of applications being connected at the time. These were essentially not time critical for the operations of the business and typically involved forms of status monitoring of activities that may then require some form of field support such as repair, replenishment or resetting

Since then, the opportunities for connecting assets and devices have evolved considerably. Several billion devices are now connected to the internet using an increasing variety of connectivity technologies – fixed line, Bluetooth, cellular, LoRa, Sigfox, Wi-Fi and satellite to name a few – all of which incur costs in one form or another. Over the next few years, many more billions of devices are expected to be connected. At the same time, the need for near real-time processing of the data generated by many of these is also increasing as IoT becomes more central to business operations. IoT in the enterprise is now rapidly encompassing business critical activities where any interruption of service could be catastrophic.

Why IoT at the edge?

Take as one extreme example the future of connected, autonomous vehicles. If these relied exclusively on a wireless network to operate, as indeed mobile handsets do, what would happen if that network suffered downtime? What would happen if those vehicles needed to operate in areas where there was poor or even non-existent network coverage? Even in good coverage areas, if all the data processing for vehicle operations was conducted in the cloud, that would require time to send the data, have it processed centrally and then returned for action by the vehicle. That delay, or latency, could easily be more than 100ms for each vehicle – an eternity when considering the traffic issues in even a medium-sized city. On top of all this, this method would also require an enormous about of processing in the cloud to cater for all the vehicles that may be connected at any one time. In addition, of course, it would require large amounts of cellular connectivity and the costs associated with that.

As this illustrates, for some connected devices a substantial amount of the data processing needs to be available in near real-time with minimal latency and with no risk of downtime. That means carrying it out at the point where the data is created – at the network edge where the devices are located.

This Analyst Report first appeared in **Tech Trends**, the new publication from IoT Now's sister brand **IoT Global Network**. The first issue, sponsored by MultiTech, is titled 'IoT at the edge opens up a whole new world' and is available at **www.iotglobalnetwork.com**

Robin Duke-Woolley,
Beecham Research

In the case of autonomous vehicles, while processing data at the edge is critical to the operation of the vehicle itself some data, such as warning of incidents ahead, potential traffic delays due to congestion and even booking of service appointments, does still need to be processed centrally.

This means there is a balance to be struck for each type of application – how much processing should be carried out at the edge versus in the cloud? At the same time, connectivity to the cloud comes at a cost – in particular, when cellular or even satellite connectivity is used. Enterprise IoT users must assess all of this when defining their IoT solution requirements.

What is edge processing and what are the key benefits?

Edge processing refers to the execution of data aggregation, manipulation, bandwidth reduction and other logic directly on an IoT sensor or device. In the context of enterprise IoT, which includes Industrial IoT (IIoT), edge refers to the computing resource that exists close to the sources of data, for example industrial machines such as wind turbines, industrial controllers such as supervisory control and data acquisition (SCADA) systems and magnetic resonance (MR) scanners. These edge computing devices typically reside away from the centralised computing available in the cloud.

The aim is to put basic computation as close as possible to the physical system, making the IoT device itself as smart as possible. Only the data that needs to go to the cloud is then sent. For example, this could be to put the individual device data into a wider context such as data analytics related to the performance of a complete solution.

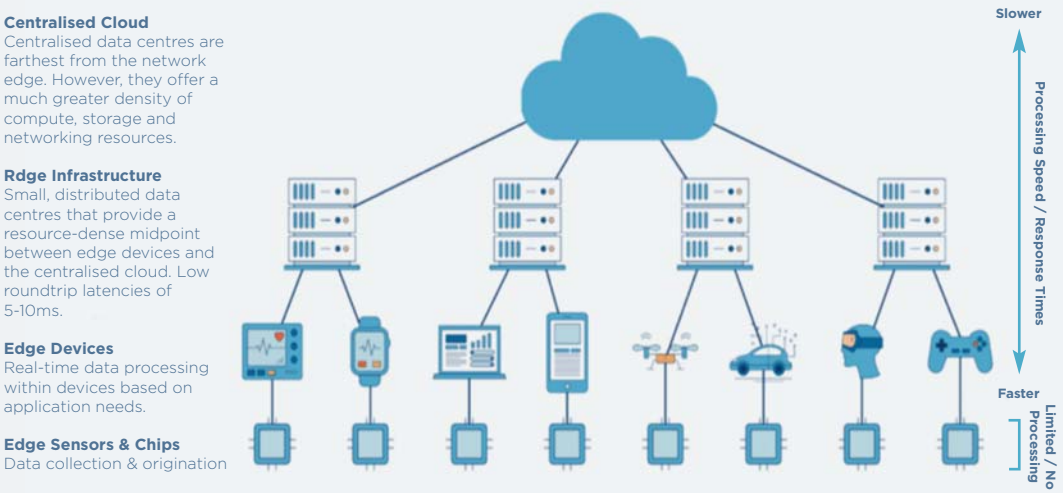
Processing data at the edge has several key benefits, in particular:

- **Bandwidth/storage cost** As the amount of data required for smart operations increases, and the number of internet-connected devices continues to grow, the cost of sending that data to the cloud and storing it centrally also grows. This bandwidth cost can be significantly reduced by only sending data to the cloud that is required for operations at that level and also sending this in summarised form. This requires local processing at or near the edge for bandwidth reduction.

- **Reliability** A primary motivator driving edge adoption is the need for robust and reliable support in hard to reach environments. Many industrial and maintenance businesses simply cannot rely on internet connectivity for mission-critical applications. As noted in the example above, connected cars could not meet their potential without local processing. Even wearables must be resilient enough to work effectively without connectivity always being available. For these use cases and many more, offline reliability makes all the difference.

- **Latency** Latency refers to the time difference between an action and a response. As also noted above, the latency introduced by sending data to the cloud, processing it centrally and then sending it back to the edge for subsequent action introduces delays that may be critical when near real-time actions are required. The connected car is one such example. For manufacturing companies as well, ▶

The edge computing ecosystem is comprised of four primary areas



From edge sensors to the centralised cloud (Source: WinSystem)

mission-critical systems cannot afford the delay of sending data to the cloud. Cutting power to a machine just too late is the difference between avoiding and incurring physical damage.

- **Privacy and security** A system that relies on connectivity to the cloud inherently presents more security risks. Related to this is privacy of the data. Protecting privacy is both a potential asset and a risk for businesses in a world where data breaches occur regularly. Companies largely reliant on cloud technology have been scrutinised for what they know about users and what they do with that information. In the healthcare market, for instance, privacy is a requirement in the US under the Health Insurance Portability and Accountability Act (HIPAA). Each hospital bed currently has about 20 sensors and it is estimated - by IBM - that data breaches cost the healthcare industry three times more than any other sector. As the number of sensors collecting and processing data continues to grow, privacy represents real value for healthcare companies looking to balance innovation with protection of patient data. Edge processing helps to alleviate some of these concerns by bringing processing and collection into the environment where the data is produced. If necessary, it can then be encrypted.

How should edge processing be organised?

With the proliferation of internet-connected devices, efficiency in data transmission and processing is becoming increasingly important. While cloud computing has traditionally provided a reliable and cost-effective method for handling this data, the continuing rapid growth in IoT has created the need for lower network latency and more reliability. Edge processing is now emerging to meet these demands. It involves placing computing resources closer to where the data originates – such as motors, pumps and generators – or at the edge where there are sensors. These processing resources may be located in the devices themselves or in edge infrastructure at a slightly higher level that can act as small, local data centres.

For example, **Tesla** cars have powerful onboard computers which allow for low latency data processing in near real-time collected by the vehicle's many peripheral sensors. This provides the vehicle with the ability to make timely, autonomous driving decisions.

On the other hand, in the healthcare sector, most wireless medical devices do not have the resources to process and store large streams of complex data. As a result, smaller, modular data centres are being deployed to provide storage and processing capacity at the edge.

The chart illustrates four layers for the evolving edge processing ecosystem:

- **Edge sensors and chips** This is where data is initially collected. These technologies include sensors and chips manufactured for a wide range of use cases in addition to the standard application-specific integrated circuits (ASICs) and application-specific standard products (ASSPs), which are optimised for specific use cases.

- **Edge devices** These devices provide the first line of processing and storing of sensor information. They include the edge sensors and ▶

chips, which collect the data, as well as the computational resources to process and analyse it to an extent. These edge devices range from smart watches to autonomous vehicles.

- **Edge infrastructure** Data centres come in all shapes and sizes. More recently, microdata centres are being deployed to offer a very local, resource-intensive midpoint between the edge devices and the centralised cloud. They offer far more data processing and storage capacity than the edge devices themselves. They also offer extremely low latency compared with the centralised cloud, which could be located a long way away.

- **Centralised cloud** Cloud computing has become a a primary location for storing, analysing and processing large-scale data sets. On the other hand, the cloud is not the place for analysing data and delivering insights in real-time. Instead, this is where edge data from many different sources is aggregated to provide an overall system perspective or other historic data. It is also where most of the integration between operational technology (OT) data and IT data tends to happen, for ongoing distribution within the wider enterprise.

The edge infrastructure level can aggregate data from edge devices or edge sensors, or both. One example of this is the recently-launched mPower Edge Intelligence offered by **MultiTech**, which extends the functionality of MultiTech router and gateway products. mPower Edge Intelligence simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud and management and analytics, while also providing the programmability and processing capability to execute critical tasks at the edge of the network. This reduces latency, controls network and cloud service costs, and ensures core functionality – even in instances when network connectivity may not be available. It also provides strong security features.

Integrating OT and IT

The OT domain involves operational processes such as industrial and factory automation, supply chain management and asset monitoring, whereas the IT domain involves business process and office automation, enterprise web and mobile applications where data is consumed. Integration of OT and IT therefore brings together the whole enterprise into one system sharing the same data.

The OT can benefit from this integration with a more efficient, scalable, managed and secure infrastructure into which numerous applications are layered. These include predictive maintenance and remote asset monitoring and management. Benefits on the IT side include secure real-time communication with the enterprise's assets while retaining the requisite efficiency for creating, scaling, maintaining and securing the infrastructure. The result is an opportunity for increased operational performance, protection of profit margins, customer retention and the creation of new business models.

In this way, edge processing for IoT is not just an opportunity to improve operational performance, it has implications throughout the enterprise that ultimately impact on both its efficient use of resource and potential for cost reduction and its ability to compete in its own market with superior customer support.

How to catch water leakage before it catches you

Few of us think about the impact of water damage to our properties until it's too late and the damage is done. According to a report from ConsumerView, titled 'Quantitative Assessment in Europe', 50% of households in Europe have experienced water damage. Similarly, the Insurance Industry Research organisation estimates that 14,000 people in the US experience a water damage emergency at home or work every day and the annual cost to insurance companies is approximately US$2.5 billion. When it comes to water damage, there is no doubt that the cost to owners and insurers can be crippling for citizens throughout the world

Doing nothing and assuming that it can't happen to you is the worst course of action. Fortunately, proactive, preventive measures that utilise leading IoT technologies are now available and more and more households and businesses are adopting them to set up warning systems to prevent impending disasters.

Based in Sweden, IoT solution provider, **iioote**, which is a LoRa Alliance member, has developed a preventative solution that uses **Semtech**'s LoRa devices and wireless radio frequency technology. Semtech's solution is composed of a widely adopted long-range, low-power solution for IoT that gives telecoms companies, IoT application makers and systems integrators the feature set necessary to deploy low-cost, interoperable IoT networks, gateways, sensors, module products and IoT services worldwide. IoT networks based on the LoRaWAN specification have been deployed in 100 countries and Semtech is a founding member of the LoRa Alliance, an open, non-profit organisation dedicated to promoting the interoperability and standardisation of low-power wide area network (LPWAN) technologies to drive implementation of the Internet of Things.

Based in Sweden, IoT solution provider, iioote, which is a LoRa Alliance member, has developed a preventative solution that uses Semtech's LoRa devices and wireless radio frequency technology

iioote's newest preventative solution, SenseIoT, utilises LoRaWAN-enabled temperature and humidity sensors, LoRaWAN gateways and the SenseIoT sensor-to-platform system, which detects and addresses water leaks in private buildings before damage can occur. Sensors are installed in risk areas in the vicinity of water and sewage pipes, such as in kitchens, bathrooms and basements. A LoRaWAN network connects sensors to the backend where data is analysed, visualised and acted upon.

iioote's LoRaWAN gateway of choice is **Multi-Tech Systems**' MultiConnect Conduit an award-winning, programmable gateway for the Internet of Things. The Conduit is a configurable, manageable and scalable LoRa gateway for industrial IoT applications.

iioote's SenseIoT is a system that monitors moisture and mould in properties with wireless sensors using the LoRaWAN standard. The solution has been tested by the **Research Institute of Sweden** (RISE) in a four-month test of a warning system for moisture and water damage. The conclusion of the measurements found that, when appropriate and correctly placed sensors are used, a water leak can be detected at an early stage thereby avoiding consequential damages. Minimisation of the expansion of a water leak can also be enabled.

How iioote works

Humidity and temperature sensors are installed in places where there is a high risk of water leakage, for example in bathrooms, kitchens, attics and building basements. The sensors report their measured values on a regular basis and in the case of excessive values, based on monitoring values set in the device, will send immediate alerts. By monitoring the trends of humidity and receiving leakage alerts property owners and landlords can avoid serious damage or respond ultra-quickly in case of an incident. In this way, expensive moisture and mould damage can be avoided or minimised.

The sensors are wireless and battery powered with a lifespan of up to ten years depending on configuration. Moreover, installation is straightforward and does not require a plumbing technician or electrician.

The sensors are connected to a public LoRaWAN radio network built for IoT, or can use a residential or private LoRaWAN network. The humidity and temperature information are transmitted wirelessly to the cloud-based SenseIoT monitoring and alarm solution in which thresholds can also be set to match the local monitoring conditions, as we can expect bathrooms to be more humid than an attic or basement. ▶

The sensors' data values and trends are made available in easy to understand reports and alarms or notifications can be configured for different threshold values. The system is easily accessible via web readers and mobile devices. Depending on where one sits in the value chain, the return on investment (ROI) for a full solution is measured in months rather than years due to the cost effective LoRaWAN sensors, gateways and software solutions. For insurance companies the number of claims would come down substantially and in case of an emergency leak the damages will be much lower given the immediate response. For building owners and landlords, the trend analysis will make sure buildings remain in good shape and do not need major repairs after many years of exposure to out of band humidity and fast responses to leakages will limit the resulting damages and create better customer satisfaction. Humidity is often also related to health risks and loss of irreplaceable materials which is not reflected in amounts.

SenseIoT in action

Recently the SenseIoT solution was installed in the renovation project of a 1938 tenant-owned apartment building situated in the suburb of Kålltorp in Gothenburg, Sweden. The project included updating of all drainage pipes and the electrical system as well as building refurbishment. A water leak in such a house, which in some cases could take three to five years to detect, would be extremely expensive and would make it very difficult to dry and rebuild. With this in mind, the installation of the new SenseIoT system was a very good solution for detection of water leaks and prevention of prolonged damages.

In the bathroom, the sensors were placed in the wall near the bathtub tap and in the floor construction near the floor drain. There is also a reference sensor placed in the same floor construction section where the floor drain was placed eight feet away. The reference sensor is used to monitor the development of humidity spread in the construction during leakage. In the kitchen, the sensor was placed in the space under the sink cupboard and floor. The sensor is used for detection of both dishwasher leaks as well as leakages from the sink for pressurised and passive water intrusion.

"The SenseIoT solution gives us security against unpredictable costs for the estate when it comes to water leaks and it is also a quality label for each tenant-owned apartment. We get constant information about humidity, temperature levels and more, enabling us to know the status in the building at all times. As an extra bonus, we will receive a discount on the insurance," says Henrik Berntsson, the chairman of the board of the tenant association within the building.

Discounts from insurance providers are significant, as the solution provides a metric to ensure the cause of damage is accurately determined. "The saving can be huge and should be de-facto for all real estate owners, insurance companies and others," adds Berntsson. The charge for a system varies with volume. The average size of a building is 20 apartments for tenant-owned apartments in Sweden. Such a system would cost around a US$1,500 one-time fee and around US$1,000 yearly for the SenseIoT subscription. An option is offered for monitoring of data and site visits when a leakage is assumed. ■

The SenseIoT deployment

About iioote AB
iioote works with companies, organisations and municipalities in implementing IoT in their businesses, from analysis of needs and strategy to planning, implementation and system integration. iioote has expertise in IoT, IT and telecoms, combined with industry-specific skills from the construction, machinery and automotive industries. iioote integrates solutions that drive the development of simple and innovative IoT in the community. This is enabled by radio systems that use low-energy technology, low power wide area networks (LPWAN).
More information about iioote can be found at: **www.iioote.com/en**

About MultiTech
MultiTech designs, develops and manufactures communications solutions for the industrial internet of things (IIoT) – connecting physical assets to business processes to deliver enhanced value. The commitment to quality and service excellence means you can count on MultiTech products and people to address your needs, while its history of innovation ensures you can stay ahead of the latest technology with a partner who will be there for the life of your solution. Visit **www.multitech.com** for more information.

MULTITECH

Why IT and OT integration and IoT edge processing are paving the way for AI

Information technology (IT) and operational technology (OT) have been coming together in IoT for several years now. Robin Duke-Woolley, the chief executive of Beecham Research interviewed Roberto Siagri, the chief executive of Eurotech, to explore the advantages of this and assess what progress has been made in integrating the two technologies

Robin Duke-Woolley: What is the main concept behind IT/OT integration, as you see it?

Roberto Siagri: The point of this integration is that before this new software paradigm, factories and products were not connected with the IT side of the organisation. IT was mainly related to the administration and commercial activities, whereas data from factories and products were isolated from IT and not available in real-time. By the way, factory and product data were collected by people, not by machines. Nowadays, with this new methodology we call the Internet of Things, we can digitally connect IT and OT. This is the result of the evolution from embedded computers to edge computers. Embedded computers were not necessarily connected to other computers. They were doing a job in isolation and this job was the automation. Machine automation was mainly related to taking care of the real-time needs of the machine and not related to integration with the IT infrastructure.

Now, if you think about it, before we had smartphones, phones were not data processing machines, just a voice processing machine. With the smartphone, people have figured out how to transfer applications and how to make use of a wide range of data. So why not do the same with machines? If you do this, you are doing IoT, a new paradigm that emerges as an evolution of embedded computers and machine-to-machine (M2M) communication. M2M was the start of it – connecting machines to servers not necessarily through the internet. This was very specific – certain data collected for a dedicated application. With this new IT/OT integration, data become the minimum common denominator of all the devices,

including machines, products, assets and others, that you have in your organisation. It means that, in the end, the main purpose is to create a common data lake that contains all the digital twins of your organisation.

RD-W: What do you then do with that data lake?

RS: First you have to create a data lake without any real final purpose, just to collect the data coming from the different parts / devices of the organisation, then you can create a federation of loosely coupled apps around the data lake and these apps are no more hierarchically interconnected than they were in the past. Now that we have entered into the app economy, you can start thinking with agile methodologies. You design just what you need, when you need it. Following this approach, data producers are decoupled from data consumers. This means that what produces data does not have to know what or who will be using them and how they will be used: you just need collect as much data as you can.

RD-W: Does that not mean you end up with collecting a lot more information than you're ever going to use?

RS: In the beginning you don't need to know. That's the beauty of the thing. In the past, you just collected the data that you needed, thus limiting your future capabilities, as what you know now is not what you will know in the future. The idea here is that because you have the things that are producing data, and because the cost of collecting and storing data is so low, why not store everything? The reality is that the more data you collect, the more value you will have in the future. How can you think about artificial intelligence (AI) if you don't have a large amount of data – especially historical data? If you don't have the examples, you can't train your AI software.

RD-W: Do you think organisations accept that argument, that they should collect more data than they really need because in the future they'll need it? Often, some sort of return on investment (ROI) analysis is needed before they do anything.

RS: You must enter this new digital production mindset. If you don't switch from industrial production to digital production, you will never find how valuable your data are. Sometimes when you do innovation or research, you don't know if you are going to have an outcome. But you start anyway. So, if you insist on the old model of ROI, then you will just look at the short-term improvements and, in this case, you just need a few data. If you have a long-term strategic view, then data – all data – become very valuable. For example, if you think that your product could become a service, or more connected with services, then without data you cannot work that out.

RD-W: Looking now at edge versus cloud, cloud has been at the centre of IoT, but now we have much more focus on the edge. What do you see as the right balance between processing at the edge versus the cloud?

RS: If it is real-time, such as in a factory, there is no option but to process data at the edge. If you have a very high throughput of data and you don't want to transfer all that to the cloud, you need to pre-process it at the edge first. Also, there are now increasing security concerns. Security needs more processing power at the edge. In addition, in a factory environment there is often a need to keep the data in the factory, without moving all the data to the cloud. So, some stay local, some go to the cloud. Finally, you must to be resilient against wide area network (WAN) connectivity or data-centre failures: you need more edge computing. What that split should be depends on the needs of the individual company. In the end, these are the reasons to design a distributed data centre with gateways increasingly forming the local infrastructure.

Roberto Siagri, Eurotech

RD-W: Would you say the intelligent gateway at the edge is becoming more important as the edge computer?

RS: Yes, more and more edge computers are taking on all the functions and this will increasingly be the gateway. To me, the difference between edge computers and embedded computers is that the latter do not need to be involved with connectivity and cybersecurity. They are mainly used in isolation, with no connection. On the other hand, edge computers must have all the features of cybersecurity already built in, because they are always connected and must have the capability to manage connectivity. This is the main difference between the two.

www.eurotech.com

IoT data must be monetised effectively for potential to become reality

Revenue generation and management have always been important objectives for the telecommunications industry. With the advent of IoT, these objectives have become even more relevant, considering that the large amount of data produced by IoT deployments is a strong source of new revenue opportunities. Saverio Romeo, a strategic advisor at IoT Analytics, spoke to Akil Chomoko, the product marketing director at MDS Global, to explore further the issues facing IoT monetisation

Saverio Romeo (SR): MDS Global can be defined as an agile IoT monetisation vendor. Can you explain to our readers what that consists of?

Akil Chomoko (AC): MDS Global offers a fully managed, cloud-based solution called IoTMonetised. It is a solution that can rate IoT application services for the purpose of charging end customers and settling with partners in the service chain. The challenge for many IoT enablers and communications service providers (CSPs) is that the IoT monetisation model changes significantly from one IoT project to another. For example, one may be based on price per mile, while the next may be based on savings made, with many variations in between such as for peak and off-peak rates or other variables.

The MDS Global IoTMonetised solution has specific service features that enable agile adaptation to these business models and integration with IoT applications to accelerate their time to market.

Equally important, most IoT enterprises do not have the expertise and skills to manage event-based charging, billing and payment collections. We run all this real-time, with full transparency and with full assurance, which covers accuracy to fraud management and ultimately, we become their monetisation practice.

SR: What types of customers do you serve with your services and platform solutions?

AC: We've profiled our customers into five categories. The first one consists of CSPs that are looking to move beyond selling connectivity to deliver full IoT solutions and services to IoT-based enterprises. The second one consists of systems integrators who are looking to support IoT enterprises with agile, low-cost monetisation solutions as opposed to traditional complex and costly projects.

The third group are IoT platform vendors that require revenue management features to help their customers monetise the IoT applications they build on their platforms. The fourth category are end IoT enterprises that need direct support to monetise their IoT innovations.

And finally, there is a growing market of virtual IoT operators and MVNOs, who are looking to offer a more complete bespoke IoT service enablement solution to customers.

SR: What benefits have your customers experienced after adopting MDS Global IoT monetisation services?

AC: Our solution is ready to deploy, opex effective and strongly revenue generating in comparison to bespoke developments and traditional billing solutions.

Many IoT ventures have limited initial capital for the development and deployment of their IoT application. Usually, they have not considered the cost of billing management services. Our solution makes monetisation more accessible. There is no need to hire a billing and settlements team. The MDS Global team is ready to go.

We offer the ability to swiftly evolve and change a service level agreement (SLA) as required. As a company's pricing model becomes more sophisticated, MDS Global's agile platform and intellectual property can adapt as fast as they do, enabling them to compete.

Finally, we have a team which offers thought leadership and experience with B2B and B2B2X charging models. We have strong experience and credibility, having had projects with some of the largest enterprise operations for nearly 20 years.

SR: Can you briefly discuss some real examples?

AC: We recently started working with **Veriown**, a Chicago-based IoT company, which is combining solar power with internet connectivity. Veriown has partnered with specific third party suppliers, including MDS Global and one of the UK's largest mobile providers, to deliver services that have a monumental impact on the quality of life experienced by end-consumers who are typically based in environmentally or economically challenged countries.

Veriown provides a single device known as the CONNECT that acts as a clean energy, internet, media, education and commerce hub. There is an integrated SIM and tablet within the device that provides access to online education, entertainment and commerce to Veriown customers in remote end-user locations.

The mobile operator provides the connectivity for CONNECT. Veriown then determines which components customers can access based on the proposition they sign up to. It operates a revenue sharing model between the CSP, the local deployment partners and the local content partners. MDS Global's IoTMonetised solution is used to calculate the revenue share for each partner, which incorporates reconciliation of data from the suppliers. Veriown will also use IoTMonetised to view customer transactions, and manage their balance, propositions and payments, enabling greater business visibility and tailoring packages to suit customer demand.

Using this infrastructure, Veriown is launching several free and add-on services that will provide consumers with solar energy for charging and lighting capabilities, access to news, weather and educational content, and access to an online catalogue of steaming radio and video content.

SR: What challenges have you experienced in proposing your approach to customers?

AC: Many IoT enterprises think of cost-plus or competitive pricing models as the only way of launching their business. Often these approaches make IoT business plans high-risk and unfeasible.

Many have not really worked backwards from a truly value-based pricing offer and thought about how to incorporate their partners and suppliers into a revenue or benefit sharing chain. When you distribute revenues this way you link together risk, reward and quality, which is more sustainable for some businesses, their customers and often many partners.

We often encounter far more complex and too ambitious monetisation models. Instead, they should start simple and build in complexity as their service and ecosystem evolves.

SR: Which emerging technologies do you see affecting IoT monetisation models?

AC: There are several emerging technologies that will impact our solution features. This includes the likes of blockchain, cryptocurrencies, eSIM, 5G, network slicing via software defined networks and network functions virtualisation (SDN/NFV) models, IoT data lakes and edge computing technologies. As a specialist monetisation vendor, it is our role to exploit these technologies to enable new benefits for end customers.

SR: How do you see the next year for MDS Global? What is your short-term strategic focus?

AC: Although there is a lot of industry debate and investment in IoT, it is still in its infancy. Our focus in the short-term is to build awareness of the opportunity to monetise IoT projects better so that they become sustainable in the middle and long-term. This includes supporting many existing B2B and enterprise services so that our customers can exploit these emerging technologies. They too should be able to offer more personalised services that deliver higher premiums. It is becoming a very exciting market for us.

Akil Chomoko, MDS Global

Veriown provides a single device known as the CONNECT that acts as a clean energy, internet, media, education and commerce hub

www.mdsglobal.com

Global companies work in collaboration to improve lives and IoT's commercial model

Technology has the capability to transform lives. Over the past few years, companies, cities and countries have moved to digitise all that they do, driving positive results in numerous ways. Yet across the world, many people still face a number of difficulties from climate change and endemic poverty, to health and nutritional care. While these big issues might seem insurmountable, technology can play a critical role in addressing many of these challenges, while creating a host of opportunities

Figure 1: IoT revenue share (monetisation) model

One important catalyst for change is IoT which, although in its early stages of adoption, is already having a huge impact on people around the world. Network deployment, power requirements, reliability and durability are base level infrastructure requirements that can change lives and it is here that three companies, located across continents have teamed up to solve a simple but essential problem.

Sunshine for change

Globally there are more than one billion people without access to electricity, over two billion without access to formal banking and in excess of three billion without access to the internet. **Veriown Global** is a start-up business with the mission of creating innovative and disruptive solutions that have a life-changing impact to those across the globe with limited or no access to electricity, connectivity, quality healthcare or education. Using the innovation of IoT, Chicago-based Veriown has partnered with one of the UK's largest mobile providers and UK-based BSS-as-a-Service provider **MDS Global**. By combining solar power with internet connectivity, Veriown is able to deliver services that provide a monumental impact to the quality of life experienced by last-mile rural consumers.

By creating alliances with companies that lead in their respective fields, including the multinational tier one mobile operator for internet access, Veriown will operate a revenue sharing model with deployment partners and local content partners. The MDS Global IoTMonetised solution will be utilised to calculate the revenue share to each partner, which will incorporate the reconciliation of data from the suppliers. Veriown will also utilise IoTMonetised to view a customer's transactions,

managing the customer's balance, propositions and payments, enabling greater business visibility and offering the ability to tailor packages to suit customer demand.

David Shoup, the chief technology officer of Veriown, said: "Collaborating with network infrastructure operators and best of breed software providers enables us to provide life-changing solutions to communities that are sustainable for our business. We can now connect off-grid rural consumers anywhere in the world using locally-relevant tariffs and distribution partners, whilst accurately calculating important revenue share."

Veriown provides a single device known as the CONNECT that acts as a clean energy, internet, media, education and commerce hub. There is an integrated SIM and touch screen within the CONNECT device that provides access to online education, entertainment and commerce to Veriown customers in remote end-user locations.

Using this infrastructure, Veriown is launching a number of free and add-on services that will provide consumers with:

- Solar energy for charging and lighting capabilities
- Access to news, weather and educational content
- Access to an online catalogue of streaming radio and video content

Customers will be able to purchase these additional service propositions as a one-off or, if they have sufficient balance, they can have the proposition automatically renew at the end of each period – for example every seven or 30 days. This will be determined by the customer's proposition type.

Gary Bunney, the chief executive of MDS Global, added: "For an IoT model to be both feasible and sustainable, IoT businesses are demanding new approaches to monetisation. The project with Veriown demonstrates the major benefit of enabling a wide ecosystem of services enablers, component manufacturers, system integrators and operational partners to come together and share value from a wide range of business models that tap into the worldwide phenomena that is IoT."

"It is with great pleasure that we are not only facilitating multi-company IoT collaborations, but are also contributing to a project that has major benefits for the underprivileged in our worldwide society," he added. "I hope it will be the start of many projects which empower people around the globe."

Why do we need IoT monetisation?

Consumers and businesses from across all sectors and industries are choosing to pay for IoT applications based on the value they deliver. This value is measured via defined outcomes, usage and/or subscriptions. Examples include pay-per-mile insurance, pay-per-event healthcare and in this case, pay-per-week smart-lighting or streaming content.

Commercial influences such as usage terms, commitment contracts and bundles for discounting drive further sophistication in these business models.

In addition, many IoT applications are delivered using an ecosystem of partner applications, services, devices and connectivity, which require partner management and settlement - continuous money in, continuous settlement out.

To ensure operations are accurate and profitable, IoT businesses need a solid IoT monetisation practice and an agile platform.

MDS GLOBAL

www.mdsglobal.com

About IoTMonetised

IoTMonetised is an agile IoT monetisation solution that is delivered as-a-service via a cloud platform. It is ideally suited to IoT enterprises, like Veriown, that are looking for a solution to manage the monetisation, settlement and assurance of service revenues as they adopt IoT technologies and practices. Complex IoT billing and settlement over customer and partner lifetimes is a new and challenging discipline, but the cloud-based platform and service is available on demand to manage this critical element of business. For further information: **www.mdsglobal.com/iot-application-providers/**

Whole life costs should be assessed when making smart building decisions

Large facilities such as retail sites, office blocks, factories and residential apartments now bring together an increasingly complex network of sensors, machines, devices and apps. Many have been deployed in a fragmented fashion and bringing all of these together across different technologies is a growing headache for building and facilities managers. George Malim examines how IoT platforms are being deployed to simplify and unite management of disparate IoT-enabled functions

At the heart of the challenge is the nature of a large building. Almost by default, buildings are designed to outlast technology cycles and much of the infrastructure, plant, equipment and technology they contain. Inevitably this means technologies are upgraded at different stages and a blend of systems therefore arise – with all of the integration burden that entails.

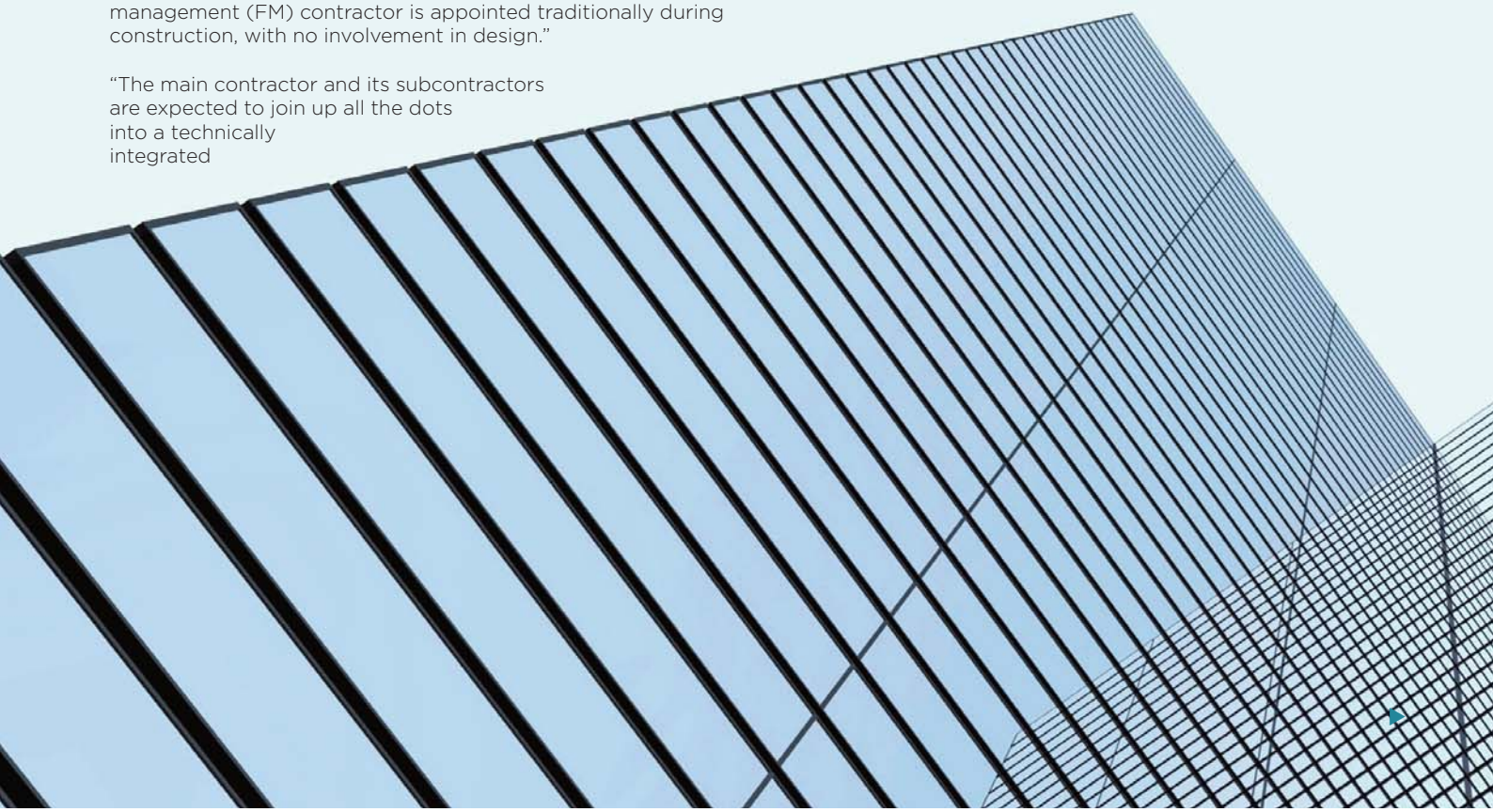
"The current design and build model is not helpful at all," confirms Niko Kavakiotis, the head of building performance and sustainability at **Siemens**. "Any technology solutions that can promote the right integration and IoT setup are diluted throughout the process, ending up in most cases with buildings having various different systems that meet the procurement specs, that are cheap in isolation but do not provide the value of integration; in most cases they fight each other. To make it more graphic, What's the point of putting a Lada engine in an Aston Martin car frame?"

Others see it as a case of too many cooks spoiling the broth. "The procurement process regularly engages different designers at different stages on different terms, and then expects a main contractor to bid for the project having had no involvement in design or systems selections," says George Adams, the engineering and energy director at **SPIE UK**. "Then the main contractor splits the project into packages for further competitive bidding from firms who've had no engagement in the design stages. Equally, the facilities management (FM) contractor is appointed traditionally during construction, with no involvement in design."

"The main contractor and its subcontractors are expected to join up all the dots into a technically integrated entity including the intelligent control systems and mass of sensors and controllers," he adds. "The avoidance of fragmentation is a procurement process that enables continuous responsibility and integrated working to achieve a holistic and joined-up solution from a common data management platform. If the delivery process isn't joined-up then the technical and data integration will suffer, be diminished and operationally not achieve optimum performance. The technology exists, it's the process, procurement and responsibilities that need sorting out."

For Mike Hook, an executive director at building intelligence firm **LMG**, fragmentation can best be avoided by creating a robust, secure, open and integrated platform based upon the **IoT World Forum** Architecture Committee's Reference Model.

"This integrated approach creates a common platform, the Building Services Network, that can be used to provide secure connectivity to any smart device, either operations technology (OT) or IT facilities related, that is located within the building," he explains. "A single physical layer of IP connectivity to support the things underpinned by common policies and management tools and responsibility, creates huge opportunities for efficiency and productivity improvements. These incentives should mitigate the traditional approach to delivering building services which results in unwanted and unnecessary fragmentation."



The real rewards come not only in greater efficiency through simplified management but in the creation of new user experiences that are enabled by better integration of disparate systems.

"Simplifying facilities management systems undoubtedly enables building managers to improve the user experience too," says Dan Bladen, the chief executive and co-founder of **Chargifi**. "With a holistic and integrated technology stack, managers can gain a 360-degree view of how buildings are being used and how they can be improved. This is vital to enhancing user experience. Take a smart office, for example: facilities managers can provide employers with vital insights on the workforce, enabling them to make changes to the workplace experience and ultimately boost employee productivity, efficiency and engagement."

Pioneering organisations are already trying to harness new capabilities, says Hook. "New user experiences are increasingly being offered by innovative organisations such as **Schroders** and **Societe Generale** to their staff via mobile apps that focus on improving the users experience of the building by providing a range of services such as: way-finding, meeting room and/or desk booking, find my closest… and other location based services," he says.

"In addition to the hard or tangible benefits provided by improved energy and space utilisation, truly smart buildings also provide hard savings derived from taking an integrated approach to operational maintenance," Hook adds. "Integrating the IT and OT maintenance functions, supported by remote diagnostics and self-healing capabilities, greatly improves mean time to fault resolution and enables the adoption of usage-based – as opposed to time-based – maintenance policies."

Kavakiotis at Siemens thinks simplification and new opportunities often go hand-in-hand. "It is definitely about simplifying management and tasks, such as booking rooms, fault reporting and others, but there are a whole array of user experiences that can be integrated as to make users more empowered," he explains. "We are talking about location based services, services such as **Comfy** for controlling the direct conditions, personalisation of user conditions, tracking high value assets and many more. These user experiences relate to saving time, resources, using the space more efficiently, as well as feeling more empowered to adjust the space and create your perfect place."

"These go above and beyond simplifying management," he adds. "We are talking about the territory of creating conditions where human beings can unleash their potential. We are talking about connecting people in the building with the building through an IoT network of smart sensors to create a flexible, people-centric building environment. This third component delivers both operational efficiency and an enhanced occupant experience. It's important to note that this is not a good to have. It is happening, and companies who do not realise this potential risk being left behind."

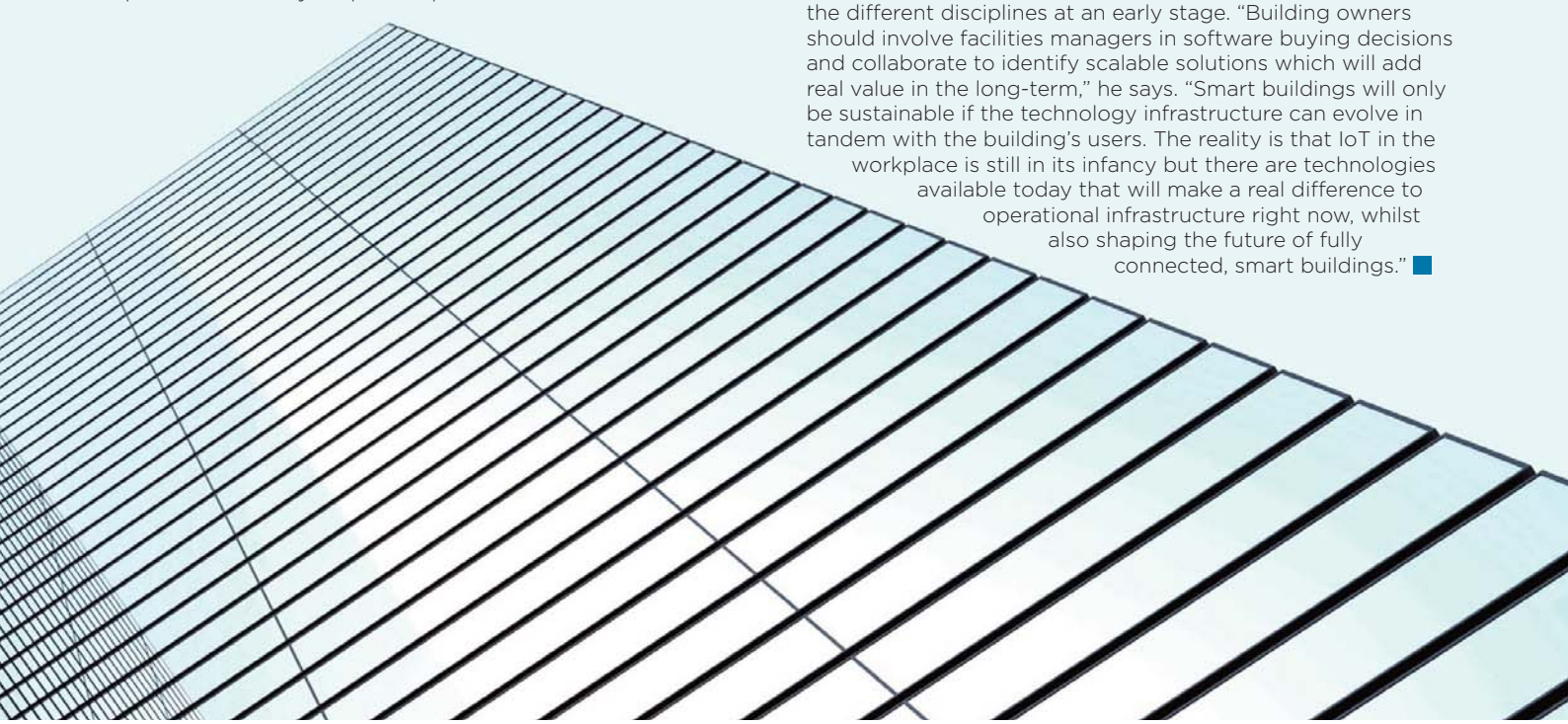
So what can building owners do to open up these opportunities, serve tenants better and potentially generate additional revenue?

"Building owners have the means of establishing a performance-based approach to using analysed data to continuously improve the operations of the building and productivity of the occupants," says Adams. "For example, using IoT technology to monitor and study the occupancy patterns and densities of the space can establish how the operational aspects or factors can be managed more efficiently. This can result in an increase in energy savings and even lead to better space utilisation. It can also identify opportunities for subletting of space to reduce costs or business partnering to improve collaboration and ultimately business results and outcomes."

"Investors and operators need to look at the lifecycle of their building from a business investment point of view rather than a capital cost perspective in relation to sustainability, productivity, efficiency and occupant wellbeing," he adds. "To support this, the integration of facility management skills from the outset of the design would enable better economic decisions for the whole life of the building. Whole life economics of all present and future costs of a building requires a methodology for the systematic economic evaluation used to establish the ownership, including all aspects of the project in order to achieve the best results for the owners and users."

Kavakiotis agrees and urges organisations to start with a wider view of what they are trying to achieve. "Think of how buildings can enable their goals," he says. "Have buildings as part of the strategy rather than bricks and mortar only. If they do not feel they have the time or expertise to do it, partner with a technology consultant to do it properly, or else you run the risk of going down a rabbit hole."

Bladen at Chargifi also advocates greater integration between the different disciplines at an early stage. "Building owners should involve facilities managers in software buying decisions and collaborate to identify scalable solutions which will add real value in the long-term," he says. "Smart buildings will only be sustainable if the technology infrastructure can evolve in tandem with the building's users. The reality is that IoT in the workplace is still in its infancy but there are technologies available today that will make a real difference to operational infrastructure right now, whilst also shaping the future of fully connected, smart buildings." ■




MDS
GLOBAL
IoT enablement
generates 8x more
revenue than
IoT connectivity
Ready to get your share?
www.mdsglobal.com/iot-application-providers/
@MDSglobal
MDS Global

IoT NOW ANALYST REPORT

SMART HOMES

Will whole-home systems dominate point solutions as the market matures?

BERG INSIGHT

SPONSOR

MDS GLOBAL

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

From smart lights and home security systems to connected toasters

Martin Bäckman,
Berg Insight

Smart homes and home automation are ambiguous terms used in reference to a wide range of solutions for controlling, monitoring and automating functions in the home, writes Martin Bäckman, an IoT analyst at Berg Insight. Smart home systems can be divided into point solutions and whole-home systems. Smart home point solutions are designed for a specific functionality such as climate control, video monitoring or access control. Examples of this type of product include smart thermostats, smart door locks and smart lighting systems

Whole-home solutions consist of two or more point solutions that can be controlled from a unified user interface. In its simplest form, a whole-home system can, for instance, consist of a smart thermostat and a smart plug that can be controlled from the same smartphone app. However, in its more advanced forms whole-home systems can be comprehensive solutions that are used to control and automate everything in the home from access control and entertainment systems to window blinds.

North America is leading the smart home market

North America is the most advanced region in the world for smart home solutions. At the end of 2018, an estimated 28.8 million homes in the region were equipped with at least one smart home device. This represents market penetration of 20.3%. Europe is still behind the North American market, in terms of market penetration. A total of 29.7 million European homes had one or more smart home devices installed at the end of 2018, which gives market penetration of 12.9%. The installed base of smart home solutions are expected to grow substantially in both regions in the coming years. North America will continue to be the most mature market and reach market penetration of close to 44% in 2022. The European market will be larger in terms of number of smart homes but will stay behind in terms of market penetration, at around 36% at the end of 2022.

Connected devices now cover all areas of the home

There are various application areas in the home for smart and connected solutions. Seven primary categories can be found: security and access control systems; energy management and climate control systems; audio-visual and entertainment systems; lighting and window control systems; healthcare and assisted living systems; home appliances; and service robotics. The most ▶

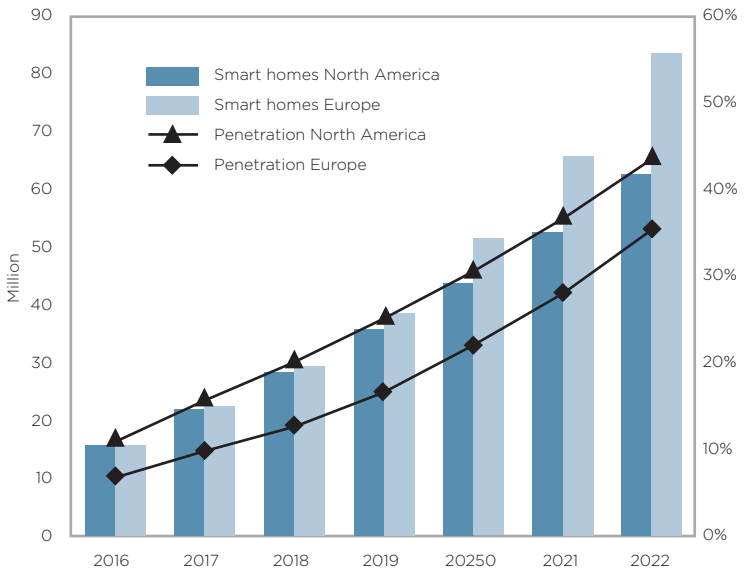


Figure 1: Smart home penetration and installed base (Europe and North America 2016–2022)

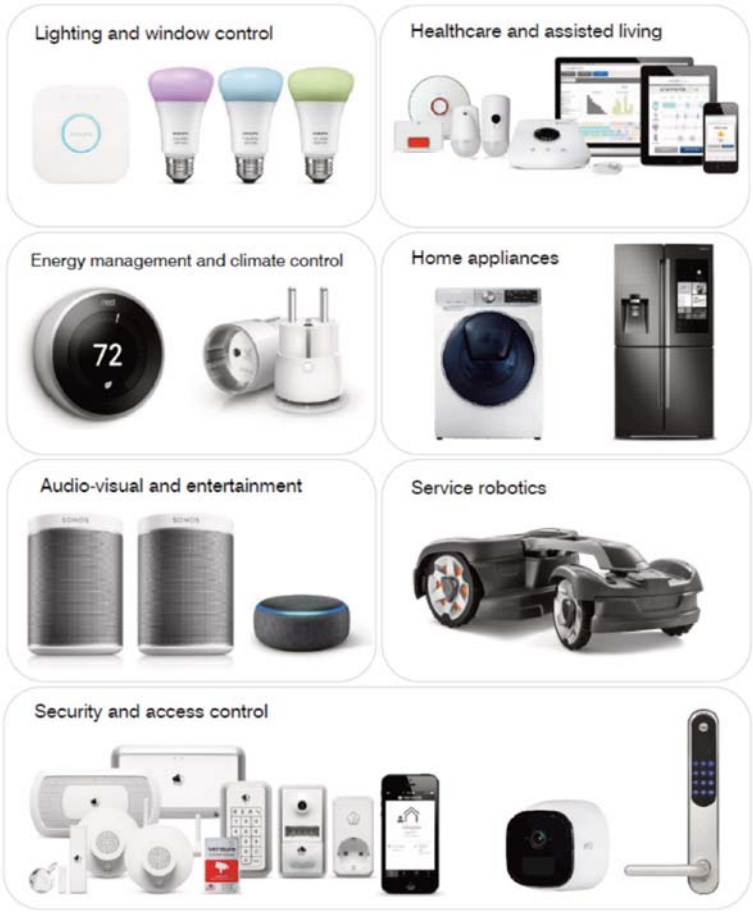


Figure 2: Smart home product categories

Source: Berg Insight

popular smart home product category today is audio-visual and entertainment systems, largely due to the success of voice-controlled smart speakers. These are followed by energy management and climate control systems. The total installed base of smart home products in Europe and North America at the end of 2018 reached an estimated 362 million devices.

Security and access control

The security and access control category comprises smart home devices such as alarm systems, door locks, garage door opening systems and video surveillance cameras. Alarm systems has been one of the first smart home market segments to gain traction. Interactive features such as arming and disarming the alarm systems from a PC over the internet emerged in the early 2000s. However, the popularity of these features really started to take off around 2010 when smartphones and smartphone apps became commonplace. The latest generation of monitored alarm systems often have a range of optional add-on accessories such as video surveillance, smart door locks, smoke alarms and carbon monoxide detectors. Self-monitoring using connected video cameras is also gaining traction as a stand-alone solution for the smart home. Major vendors of interactive home alarm systems include **ADT**, **Verisure** and **Vivint**.

Energy management and climate control

The energy management and climate control category comprises smart home systems that are used to manage energy usage and control temperature, humidity and ventilation in homes. The most popular products in this category today are smart thermostats, smart air conditioners and smart plugs. In addition to this a broad range of new connected devices such as heat pumps and water heaters are emerging on the market. The benefits of connected climate control systems go beyond convenience and the ability to remotely control the home climate. They also help users save energy and in turn reduce their energy bills. For example, smart thermostats can adapt to weather conditions and be programmed to turn off heating during the day when the home is empty and turn it on again in the evening when family members return to their home. The market for smart thermostats is led by **Nest**, **Honeywell** and **Ecobee**.

Audio-visual and entertainment

The audio-visual and entertainment systems category includes control of multi-room audio, TV and video systems. Audio-visual and entertainment systems are popular in mid-range and high-end home automation installations but uncommon in low-end systems. Multi-room audio is a very popular smart home point solution in this category, which was pioneered by **Sonos** but is now also offered by companies such as **Bose**, **Denon** and **Harman Kardon**. In recent years, voice-controlled smart speakers from companies such as **Amazon**, **Google** and **Apple** have been introduced to the market and these have made a significant impact on the smart home market.

Lighting and window control

The lighting and window control category consists of smart home systems that are used to control lights, window blinds, window shades and the opening and closing of windows. Lighting control can be used to adjust the mood in the room and schemes can often be designed for different situations such as morning, movie night and party. Window and shade control has mainly to do with opening windows for ventilation as well as reducing solar glare and heat gain so that the home remains comfortable at all times of the day. There is also an energy management component in both segments. For instance, a smart lighting system can be configured so all lights are automatically turned off when the user leaves the home. Similarly, the operation of window blinds can be automated in an intelligent way so that the use of energy-consuming heating, ventilation and air conditioning (HVAC) equipment can be reduced. Smart light bulbs are one of the most popular smart home device ▶

categories and are often the first smart home product consumers purchase. **Signify** sells smart lighting products under the **Philips HUE** brand and is the market leader. Other major vendors in the category are **IKEA**, **Osram**, **Hive**, **Lutron** and **LIFX**.

Healthcare and assisted living

The healthcare and assisted living category comprises smart home devices that enable continuous monitoring of the user's activities and well-being. The most common devices in this category are sensors in the home, such as motion sensors, front door open/close detectors, fridge open/close detectors, pressure mats and bed and chair occupancy sensors. Smart healthcare and assisted living solutions are evolved versions of traditional assistance systems that usually are called telecare systems or social alarms in Europe and personal emergency response systems (PERS) or medical alert systems in North America. This type of system is offered by telecare market leaders such as **Tunstall** and **Legrand**, as well as by new entrants such as **Doro**, **Greatcall**, **H2AD**, **Essence Group** and **Qorvo.**

Home appliances

The home appliances category comprises a wide range of products such as washing machines, dryers, dishwashers, refrigerators, freezers and ovens. For consumers, the main benefit of appliances being connected to the Internet includes notifications of events such as when the refrigerator door has been left open or when the clothes have been washed. Also, features such as remote start and pause allow users to control their appliances when away from home. Global market leaders in the category such as **Whirlpool**, **Haier**, **Electrolux**, **Bosch** and **LG Electronics** offer a growing product portfolio of connected appliances.

Service robotics

The service robotics market comprises various types of robots which can be used in the home environment. For the average consumer, robots are commonly used for tedious and repetitive tasks such as domestic chores or for leisure and entertainment purposes. The most common service robots developed for the home include robot lawn mowers, floor cleaning robots, assistant robots and telepresence robots. **Husqvarna**, **Robomow** and **Zucchetti Centro Sistemi** offer robot lawn mowers while **iRobot**, **Neato Robotics** and **Dyson** sell robots for floor cleaning. These types of robots have previously functioned as point solutions and been controlled through the companies' own apps, but are now increasingly part of wider smart home systems.

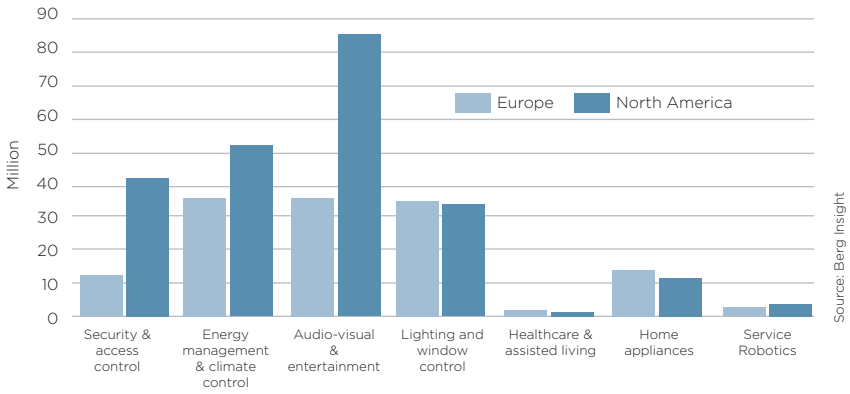


Figure 3: Installed base of various smart home categories (Europe and North America 2018)

Whole-home systems

There are several actors offering complete smart home systems where the user can control everything from window blinds and lights to audio systems and alarm systems, all from a single unified interface. The market is served by a diverse set of vendors with different industry backgrounds. The home automation specialists **eQ-3**, **Control4** and **Crestron Electronics** were some of the first companies offering complete smart home systems. Today, they are seeing increasing competition from ICT industry giants such as **Google**, **Samsung** and **Amazon**, telecoms operators such as **AT&T** and **Deutsche Telekom**, monitored security providers such as ADT and Vivint as well as consumer electronics companies such as **D-Link** and **TP-Link**.

Multiple connectivity standards are used in smart homes

There are many different connectivity standards used in the smart and connected home space. This allows vendors and end-customers to have options for any scenario, but has also caused fragmentation in the industry. Incompatibility among home connectivity technologies increases the level of complexity and uncertainty that consumers and vendors face, which in turn slows down the development of the industry as a whole.

The most common protocols for wireless communications between smart home devices and the hub are Z-Wave, Zigbee, Bluetooth and Wi-Fi. KNX is one of the most common wired ▶

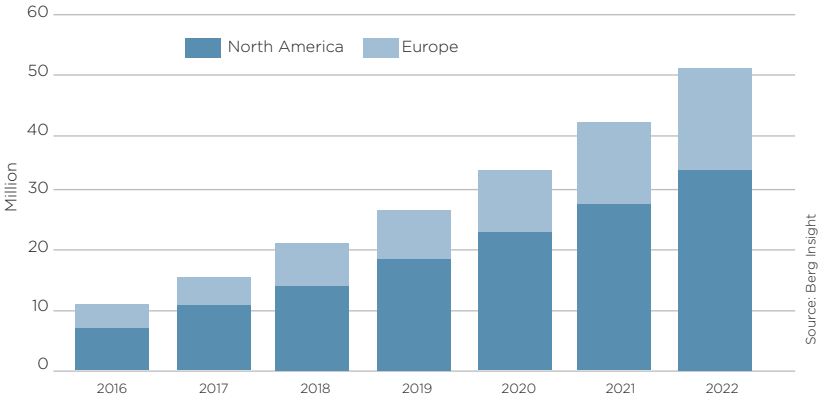
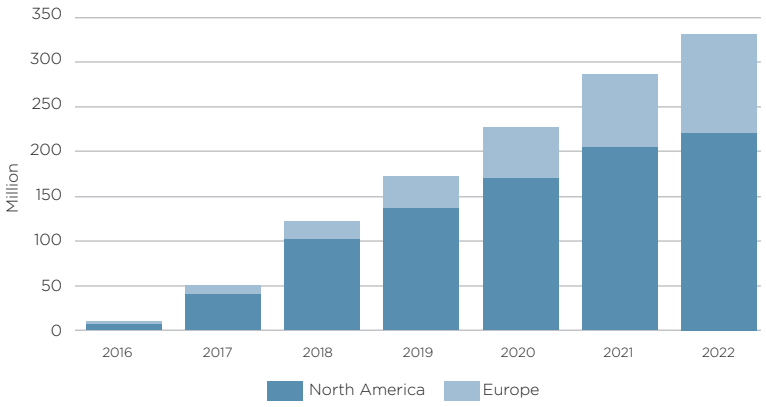


Figure 4: Cellular connections in the smart home market (Europe and North America 2016-2022)

communication protocols. Several company-proprietary communication protocols also exist. Fixed broadband is the primary communication channel between smart home devices and back-end servers. However, cellular technology is used as primary or secondary communication channel to a large extent in the security and access control segment as well as in the healthcare and assisted living segment. Cellular connectivity can also be suitable for smart plugs, thermostats and other HVAC products that can work independently in, for example, vacation house settings that lack fixed broadband connectivity. Furthermore, the mobile operators in North America and Europe are in the midst of rolling out LTE-M and NB-IoT networks which can be a suitable alternative for smart home products such as smoke detectors and door locks.

Home automation offered by leading security system vendors

Many of the leading providers of traditional home security systems including ADT, Verisure, **Prosegur** and **Securitas** have in recent years started to offer smart home products and services in addition to security solutions. These include, for instance, smart plugs, door locks, lights, appliances, climate systems and more that can be controlled from the same app as the home alarm. The rationale behind investing in a home security system is straightforward. Residences are of high value and people are willing to pay to protect their properties. When a home security system is in place, it is easy for users to add various smart home products. Adding smart home products and services to the existing home security offering has been a successful go-to-market strategy for security companies, especially in North America. The region has around 9.5 million interactive security subscribers, meaning they can control the alarm through an app or web interface. An estimated 37% of these, or 3.5 million subscribers, also has one or more smart home products connected to the system.



Source: Berg Insight

Figure 5: Installed base of voice-controlled speakers (Europe and North America 2016-2022)

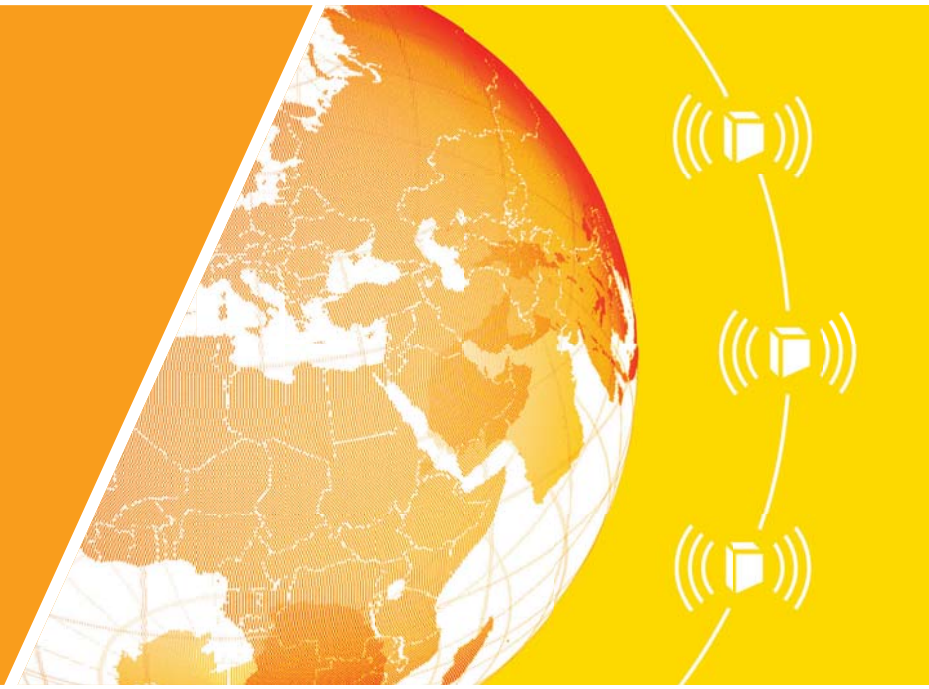
The popularity of smart speakers boosts smart home product sales

In recent years smart speakers with built-in voice assistants from companies such as Amazon, Google, Apple, **Alibaba** and **Microsoft** have become a success. A total of more than 100 million devices have been sold in 2016-2018. North America is by far the largest market globally, but Europe is now catching up. Voice controlled speakers have made consumers aware of the benefits of the smart home and in many ways paved the way for other smart home device vendors. The value of having a smart speaker also increases when more devices such as thermostats, lights and cameras are connected and possible to control using voice commands. Due to this reciprocal relationship between voice-controlled speakers and smart home devices many vendors have made their products and systems compatible with Amazon Alexa, Google Assistant and others. Consumers now also expect smart home devices to be functional with smart speakers from the leading brands.

iBASIS GLOBAL ACCESS FOR THINGS

POWERED BY TOFANE

THE OPTIMAL SOLUTION FOR GLOBAL CONNECTED DEVICES



iBASIS provides cellular data connectivity to IoT devices that enables you to:

- Gain maximum flexibility with the industry's only Open eSIM, for optimal cost versus coverage combination every time.
- Ensure the most cost-effective solution for any requirement leveraging iBASIS' Intelligent Network Selection Logic.
- Benefit from our programmable eSIM that allows for regulatory compliance for permanent roaming and data localization.
- Maximise independence with access to multiple operators and the agility of decision-making in the cloud.
- Rely on the highest global standardisation and security in the industry delivered by GSMA compliance.

YOU MAKE SMART THINGS.
WE CONNECT THEM.

BE THERE FIRST

Looking for a customised solution?
Talk to one of our specialists at
solutions@iBASIS.net

Give us a call at
+1 781 430 7500

Visit us at
www.iBASIS.com

Ajay Joseph, iBASIS

Smart home devices need secure, compliant, easy-to-use cellular connectivity

Ajay Joseph is the chief technology officer of iBASIS, the provider of communications solutions that enable digital players worldwide with global access for their things. The company today serves more than 1,000 customers from 18 global offices. Here, he tells George Malim how the company is supporting organisations with secure, global, cellular connections for Internet of Things (IoT) and smart home deployments

George Malim: What do you see as the greatest issues affecting smart home security?

Ajay Joseph: Customers have come to us asking for connections to smart devices such as white goods going into homes. There are two main options for achieving this. One is via the end user's home Wi-Fi network but this can be limiting because only around 10% connect their devices in this way. This is because doing so is inconvenient and users don't see an upside to configuring the device so it can connect via Wi-Fi.

Manufacturers therefore prefer to have a cellular connection built-in to the device that can immediately connect when it's turned on. They need to track usage and performance and enable preventative maintenance and to ensure that's possible, a cellular network is required.

A further security angle to consider is that many devices go into enterprises as well as the home so this requires a high level of security. It's not just about securing the identity of the device but also about securing the data coming out of the device. In addition, with data regulation such as GDPR in Europe, it's important that the laws of the country or region are followed across the globe.

GM: If you look at the options, from Wi-Fi to low power wide area networks (LPWANs) and cellular technologies such as LTE-M and narrowband IoT (NB-IoT), there seems to be a bewildering choice. Is there a ▶

danger that fragmented connectivity selection increases complexity, creates inefficiencies and, potentially, security weaknesses?

AJ: In terms of what manufacturers are doing, their primary objective is to offer a service that is proactive and enables preventative maintenance. For example, having a fridge that is able to communicate so the maker understands how it is performing means the maker can send an engineer to repair it before an issue occurs. For this to happen reliable, standardised, global connectivity is required.

What we have seen so far is the relationship with the device manufacturer and the device itself. There isn't an intermediate layer that will take advantage of the information. Now though, device makers are moving from selling hardware to entering the services space. This is an angle for them to get revenue.

The way it's structured today is if you're not proactive about how you do the security you could be under threat. This connection extends all the way into the home and back to the manufacturer and, with a cellular subscriber identity module (SIM), there is a trust zone that you can put the security keys inside. By using that you can have end-to-end encryption in terms of the information coming into the device and on to the Amazon Web Services cloud, or wherever.

GM: How does iBASIS help?

AJ: We offer embedded SIMs (eSIMs) in the IoT market. These are a new evolution in the SIM world which enable us to provide global access and deliver an optimal solution for connected devices.

Specifically, what we do in contrast to older global SIMs that provide access via a few operators, is follow GSMA specifications which enable us to connect to multiple operators in a standardised way. This is important for our customers because it gives us the operator credentials or profiles even with Tier 1 operators because they're happy to work with us because we're GSMA certified. The implication being our SIM card works across networks and we're network independent. We typically work with all operators in a country and figure out the best quality or the most competitive price, depending on what the application requires and the appropriate business logic.

GM: Is it just connectivity choice via an eSIM that iBASIS provides?

AJ: No, there's far more to our offering. We distinguish ourselves even further because we are able to comply with data regulations and adhere to data sovereignty rules and protect data with a certain boundary. We're localising the connectivity based on where the device is and then the data that is generated gets encrypted for transmission back to the device maker.

Our customers usually want to focus on their own customers' requirements and acquisition by attracting them to their portals, products and services. The entire network part, which is quite complex in terms of selecting the appropriate operator and keeping data local, is taken care of by us.

GM: How do you see this area developing?

AJ: By installing the eSIM on the production line, knowing that the device will then have secure, high quality, global connectivity, enables a substantial cost saving over retrofitting the connectivity when a device is imported into a market and is also more efficient than producing batches of market-specific devices. All the devices can be the same so this provides a great way to cover as many markets as possible.

This is currently achieved by soldering the eSIM onto the device but soon we will have integrated SIMs (iSIMs). Think of these as part of a semiconductor itself. We'll increasingly work to streamline how SIM capability is embedded into devices.

In fact, we're already working with Nordic Semiconductor, which is best known for its leadership in Bluetooth modems, to make global LTE-M and NB-IoT connectivity easy. These cellular modems are embedded into huge numbers of smart home devices at the point of manufacture and we've partnered with **Nordic Semiconductor** to make cellular IoT connectivity ultra-easy, automatic and instant when using its nRF9160 System-in-Package (SiP) module.

Nordic has achieved this by bundling our globally-usable iBASIS eSIM with 10MB of free initial data into all its nRF9160 Development Kits. All a Nordic nRF9160 cellular IoT customer has to do is register their eSIM on Nordic's nRF Connect for Cloud website to seamlessly connect to the iBASIS network and gain access to an entire range of configurations, monitoring and connectivity services.

We think this is a great example of how iBASIS is simplifying cellular connectivity while bringing customers all the benefits of cellular's security and ease-of-use at the same time as achieving data regulation compliance. ■

Our customers usually want to focus on their own customers' requirements and acquisition by attracting them to their portals, products and services

www.ibasis.com

Dirty devices drag down smart home security

Smart homes are composed of a growing array of devices that connect to home owners and their makers to share data and perform functions from HVAC control and access control to pet monitoring and many more. Different apps have different levels of security sensitivity and also offer different value to users and therefore are sold at different price points. George Malim assesses how this complex and fragmented smart home environment can be best secured while also delivering maximised benefits

Keiron Shepherd, F5 Networks

"Any devices connected to your home network or with internet access can be a stepping stone to more interesting targets, for example banking applications or social media accounts."

The **Avast** 2019 Smart Home Security Report, which used insights from more than 16 million smart home networks across the globe, has found that: 40.8% of digital households worldwide have at least one vulnerable device, putting the whole home network at risk; 59.7% of household routers worldwide are vulnerable; and that, apart from routers and network devices, media boxes, security cameras and printers are the most vulnerable household devices. Smart home security is therefore already a massive issue and one that is only going to exacerbate as greater smart device adoption occurs.

This reality is largely unrecognised by home owners, who have embraced the technologies and glossed over the risks. An online survey of more than 10,000 respondents conducted by **Palo Alto Networks** and YouGov uncovered mixed views on the perceived security of Internet of Things (IoT) technologies, such as smart home devices and wearables: 38% of EMEA respondents believe them to be secure, with a similar number (43%) thinking the opposite.

So, are smart home devices creating security weaknesses for criminals to exploit?

"In short, yes," says Keiron Shepherd, a senior security systems engineer at **F5 Networks**. "Any devices connected to your home network or with internet access can be a stepping stone to more interesting targets, for example banking applications or social media accounts. To illustrate, let's say your smart coffee machine ships with a default admin password and is connected to your Wi-Fi," adds Shepherd. "An attacker could carry out a simple scan using tools such as **Aircrack-ng**. This is a passive scan that can be used without having to be connected to your Wi-Fi network. After that, it is easy to work out what IoT equipment make or model you have on your network."

Jonathan Knudsen, a senior security strategist at **Synopsys**, agrees: "Any device you add to your home network comes with its own security vulnerabilities," he says. "In the best possible scenario, the device vendor has considered security at every stage of their product development, and the result is a product that is reasonably secure."

However, reasonably secure devices won't necessarily be enough as complex interactions between devices of varying security capabilities become more popular. "With this increase in connectivity comes increased risk owing to the complexity and diversity of devices and associated vulnerabilities, which criminals can exploit," says Richard Holmes, the head of cybersecurity services at IT and consulting firm **CGI UK**. "The issue we are faced with in particular is that many of the consumer IoT devices run on old legacy software which, in some cases, has not been developed for many years. The speed with which products are coming to market means that security is still not considered important enough and trying to bolt on authentication such as two factor authentication (2FA) is extremely difficult."

"The very nature of home-based IoT is that it is driven by cost minimisation, rapid time to market, low maintenance and increased integration," he adds. "These are all challenges to good security yet we are bringing these devices into our home – our inner sanctum – with access ▶

Richard Holmes, CGI UK

"In the best possible scenario, the device vendor has considered security at every stage of their product development, and the result is a product that is reasonably secure"

to privileged information about our domestic lives and an increasing ability to control that environment."

Breaches won't just hurt consumers, they could damage the enterprises they connect to and stifle IoT's development in general. "Today's world of connected devices is full of opportunities, but poor security practices risk undermining its success," says Manfred Kube, the head of communications, analytics and IoT solutions at **Gemalto**. "Most recently, researchers from Stanford University found that smart devices sitting in our homes such as smart TVs, printers, game consoles and CCTV, could be a threat to enterprise systems. As more and more smart home devices get connected to the internet, the weak links exposing them to security vulnerabilities are also likely to increase. Consumer habits, particularly around creating weak passwords, need to improve, but manufacturers must also take a security by design approach to their devices from the very outset in order to mitigate those risks."

Timo Laaksonen, the vice president of operator sales for North America, at **F-Secure**, concurs: "New weaknesses introduced by smart home devices range from open communication ports and use of insecure protocols to hardcoded passwords and outdated, insecure software platforms," he says. "Security is often only an afterthought that does not necessarily help sell the product. We need a change in the design process of smart home devices: Security – and privacy, for that matter – has to be considered a crucial design factor and functional requirement from the get go."

It's easy to point the finger at domestic Wi-Fi network security weaknesses but these are far from the only weak point smart home devices encounter. "Wi-Fi based internet connection is the obvious weak spot in many home security products," acknowledges Kube. "Many connected home security cameras offer the chance for the homeowner to watch their house when they are sat on the beach on the other side of the world, using their smartphone, and be alerted for any suspicious activity. However, they can also provide a hacker with a gateway by which they can compromise the entire network. A criminal can also easily disconnect your smart home devices by simply disabling the router cable, which is usually located outside of a house – a pair of snips could be all it takes to perform a very effective denial of service attack."

For Marc Canel, the vice president of strategy for security at **Imagination Technologies**, it's important not to single-out a particular communications technology. "Communications links can become a vector for attacks in the smart consumer marketplace," he says. "However, Wi-Fi and Bluetooth Low Energy (BLE) offer significant advantages for communications in a restricted physical space versus cellular technologies such as 4G."

Cellular IoT connections are certainly not the only way to ensure a secure smart home network. "It is reasonable to assume that not everyone will want to use cellular data to carry out their home automation tasks, though it's a good idea to have an LTE backup in case your main internet connection goes down," says Paul Routledge the UK and Ireland country manager for **D-Link**. "Technology that enables segmentation within a network can help to keep your network safe and secure, for example creating a guest network which doesn't connect to your business laptop, can help protect against viruses and Trojans that may have joined your network. Routers that have built-in home protection can be used to block malicious websites and more importantly, connections, as well as protect your network from becoming an automated botnet should your device become vulnerable."

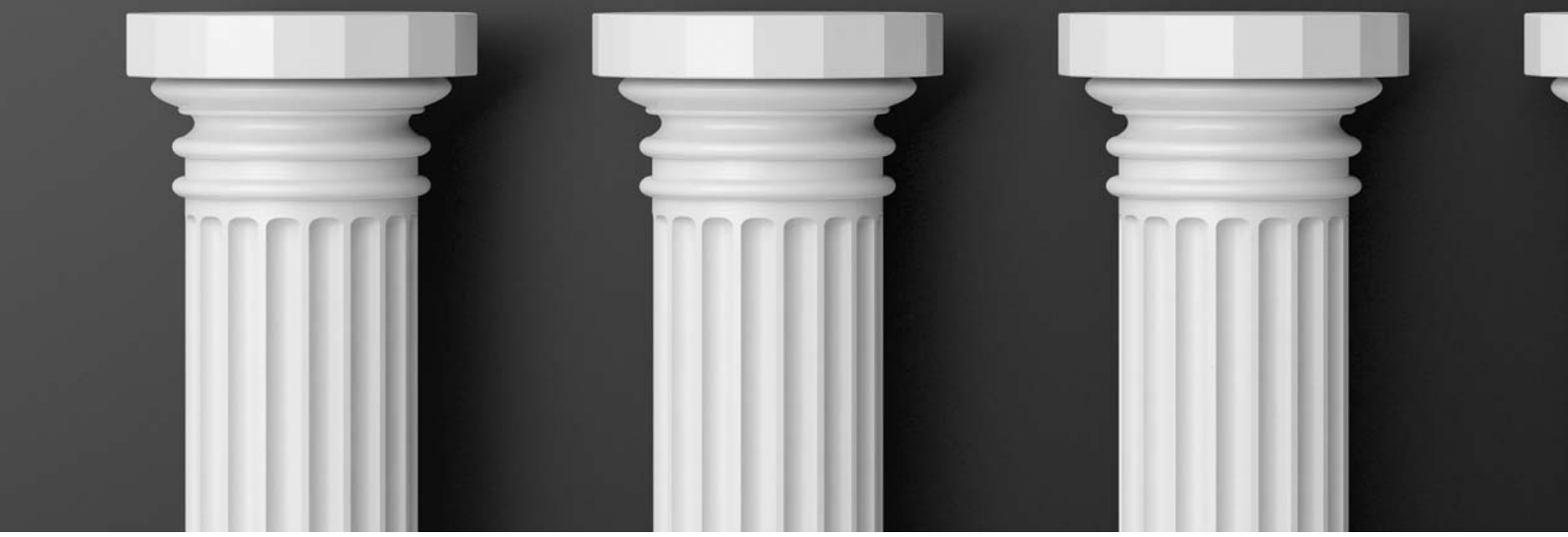
This segmentation provides a likely path to apply different levels of security to different IoT devices and applications. However, users will need to bear an increasing level of responsibility. "Any smart device should be treated as dirty and connected to a separate network - something most security savvy organisations have been doing for years," says Gavin Millard, the vice president of intelligence at **Tenable**. "Take, for example, the convenience of a smart doorbell which can send notifications directly to a phone when someone is near it, even if they don't actually press the doorbell with some models. This is a fantastic security measure, but if an unpatched vulnerability exists within the device it could be compromised by an attacker."

In this way, the physical security benefits enabled by IoT are negated by gaping cybersecurity vulnerability. As the industry matures, it will have to adopt the concept of building-in security to new software and applications if the use cases are to survive the inevitable negative headlines that security breaches will cause. ■

Paul Routledge, D-Link

"It is reasonable to assume that not everyone will want to use cellular data to carry out their home automation tasks"

Five pillars of IoT security start with a root of trust



As the number of connected devices that make up IoT proliferate, Robin Duke-Woolley, the chief executive of Beecham Research, interviews Eric Heiser the head of services and business development, at u-blox to understand the importance of implementing security that addresses five vital pillars

Robin Duke-Woolley: A couple of years ago, u-blox introduced its Five Pillars of Security. How has that developed since then?

Eric Heiser: The five principles are: Secure Boot, Secure firmware over the air (FOTA), Secure Physical Interfaces and application programme interfaces (APIs), Secure Physical Transport Layer and Robustness.

Having introduced those principles, the next step has been to implement them. That takes time and we have now launched these in our new SARA-R5 series which was announced in June. These are multi-band LTE-M/NB-IoT cellular modules, so aimed at the low power wide area network (LPWAN) market which has some particular constraints that have made this an interesting challenge.

RD-W: Is this something you have developed on your own at u-blox or have you worked with partners?

EH: We have worked extensively with world class partners. Firstly, we have a strategic relationship with **Kudelski**, also known as **Nagra**. This company has a security background and it has been doing this for decades. The company provides the security you find in set top boxes, for example, where you download content to your TV. It developed the platform that a lot of the TV content providers use to ensure their content is not hacked or stolen. This means Kudelski protects billions of dollars of content revenue every year, which proves it has a lot of good expertise in security. It also has good experience of doing this at scale, which is very important and very applicable to IoT. Other partners then include **Mocana** helping us secure the communications stack.

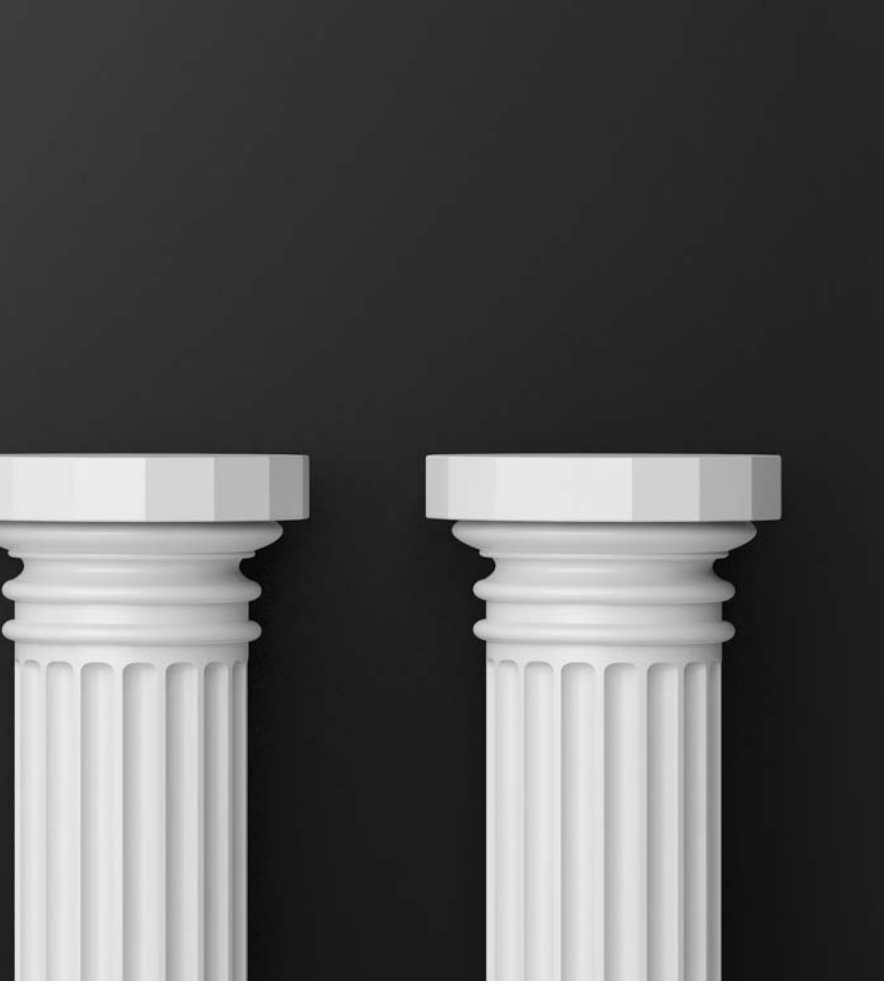
Take the example of the set top box which goes with your TV into your living room and sits there for ten years. You have to keep the security in that up to date for the entire ten years to prevent people from trying to hack into it. That is very similar to the challenge we have with LPWA and the narrowband world in the IoT market.

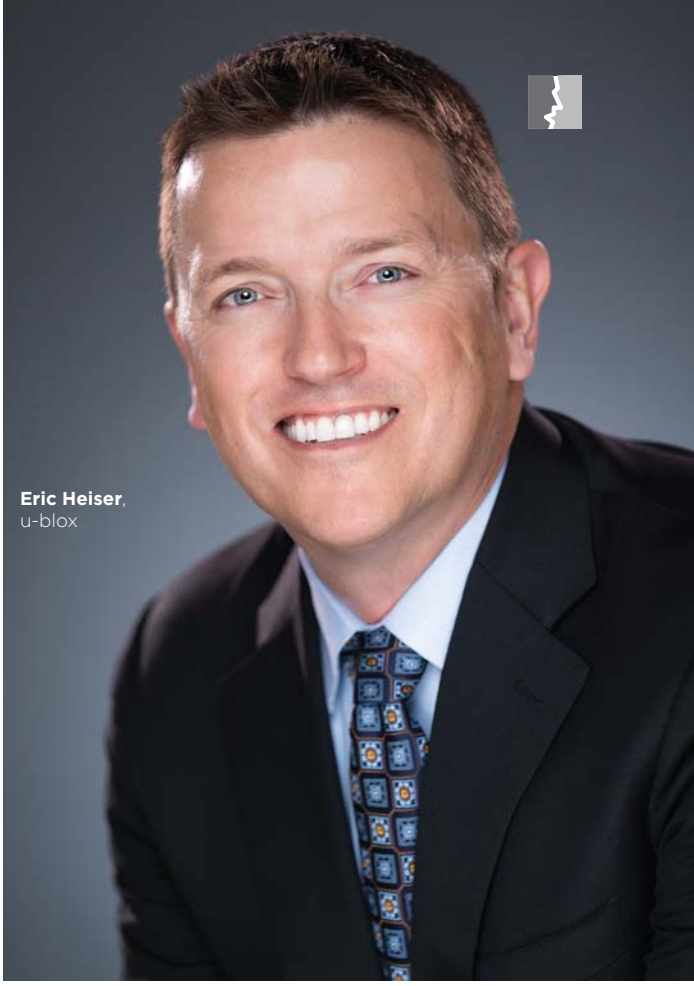
RD-W: Can you describe how that works?

EH: This process was very much focused on cellular to start with. We have a secure production process, where our IT system is hooked together with Kudelski's cloud-based system. Throughout our production process, the secure keys are basically wrapped up inside a layer of encryption, so at no point are the keys ever exposed. They are then inserted into the Root of Trust (RoT) – the secure area of the silicon.

RD-W: How do u-blox's Five Pillars line up with others in the market?

EH: The Five Pillars were our founding principle, which evolved to line up with what others in the industry are saying. **ARM**, for example, talks about ▶





Eric Heiser,
u-blox

it with its PSA (Platform Security Architecture). **Qualcomm** and **Intel** are also similar in their approaches. Secure Boot – that's where you start. You have to have some kind of immutable ID in your chipset, your IoT device, that says this is physically who I am, it can't be spoofed, it can't be changed, this is my identity so it has to be a unique identity in every device. The Secure Boot process has to be wrapped up around that.

RD-W: How important is the Root of Trust?

EH: The RoT is what guarantees all your security functions. Are you doing a secure communication? Are you doing a random number generation? Whatever you are trying to do, you need a RoT, that mix of hardware and software to do a secure function. Can you detect if you have been hacked? If someone can get into your device, you need to be able to detect it and update it. So that's a very important part of the u-blox RoT and our partnership with Kudelski. Our RoT is cryptographically tied from our manufacturing process, then to the cloud with Kudelski's proven architecture. So, we can then say now this device is out there in the world, and it's doing its normal thing, are things OK? If not, can you detect it? Can you update it? Can you do all the things you want?

RD-W: What are the next steps in the secure process?

EH: After Secure Boot you need secure updates. Typically, you hear about FOTA. You have to make sure a secure process can download that code to your device so you know you're only running firmware that you made, then you need secure communications and secure interfaces. These are the first four of the Five Pillars.

RD-W: These are the technical terms. Do you find they resonate well with device designers in the market?

EH: I'm seeing more people talk about the convergence of IT and operations technology (OT), the main point being that IoT is the connection to physical things where cyber is just data. But this is controlling physical things which is why the security is so important. It's a bit different when you start to look at it in terms of what device IoT solution providers are focused on. They look at it from the standpoint of protecting their device security, their data security and then they get into protecting the individual's privacy. So, where I talk about secure boot, secure updates, with those I can provide integrity, confidentiality and availability and then authenticity is part of availability. Those all come from our security stack, our RoT, but from a customer point of view they think of it in terms of device security, data security and protecting the individual's privacy. Those three things actually loop back to the things I was talking about, just expressed differently.

RD-W: The fifth pillar is Robustness. Is that not already an integral part of the first four pillars?

EH: It is certainly included in the first four, but there are parts in robustness that we take in that a security expert might not. For example, making sure that incoming data is valid and should be acted on. This is often outside of a security expert's domain. It may be crucial though, for example in security and safety issues. It has more to do with robustness of the whole solution, the whole design and making sure that data arrives in a manner that says – I can trust this data, I can execute on it, or say: hold on, there's something suspicious here. The robustness goes outside your normal security domain, because you're connected to the physical world. ■

I'm seeing more people talk about the convergence of IT and operations technology (OT), the main point being that IoT is the connection to physical things where cyber is just data

www.u-blox.com

A review of alternative frameworks for securing IoT devices

We are all familiar with forecasts and expectations for growth of the IoT and recognise the enormous opportunities that connected devices represent, together generating huge amounts of data, writes Robin Duke-Woolley, the chief executive of Beecham Research. So long as we can trust it, this data will become increasingly relied on by all of us, driving business insights and transformations everywhere. This trust is all-important. If we are going to depend on this device data, we need to be sure it is genuine

Creating trust means having the right level of security for each use case, which in turn requires a framework to be in place for securing large numbers of connected devices. This article briefly reviews three such approaches, one from **ARM**, with its Platform Security Architecture, a second from **u-blox**, with its Security Services Architecture, and a third from **Wind River**, with its Helix Security Framework.

ARM Platform Security Architecture (PSA)

Applying PSA consists of four key phases – analyse, architect, implement and certify, driven by threat models. How these four phases interact is illustrated in **Figure 1**.

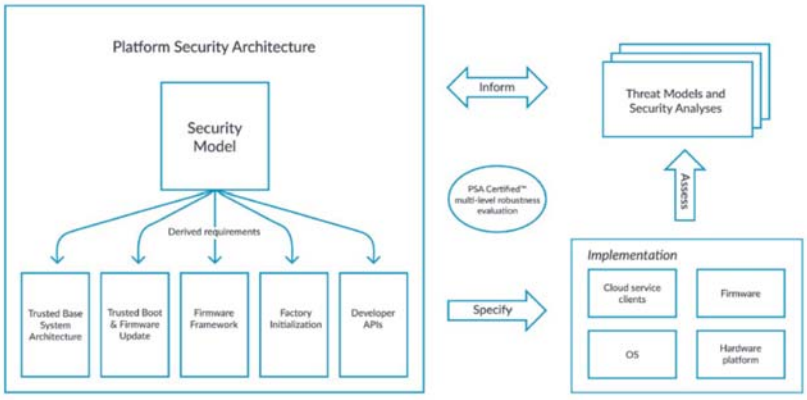


Figure 1: Components of the Platform Security Architecture (Source: ARM June 2019)

Within the PSA itself are the following components:

1. **Security model** This defines the overall security architecture for designing and deploying trusted devices. It includes high-level robustness rules and is based on the use case-driven recommendations of the threat models and security analyses.
2. **Trusted base system architecture** This encapsulates best practice security principles when designing systems. These principles support the design and integration of features rooted in hardware, including: Root of Trust, protected milestone, isolation between trusted and untrusted software components and a secure firmware update mechanism.
3. **Trusted boot and firmware update** This ensures boot integrity at start up and secure firmware update process, including authentication and authorisation of updates with cryptographic certificates and device keys.
4. **Firmware framework** Based on the requirements of the security model, this defines a standard interface and framework to isolate trusted functionality within constrained IoT devices, such as low power wide area (LPWA) network devices.
5. **Factory initialisation** The security and Root of Trust models are only effective if root secrets and device firmware are provisioned in the context of secure manufacturing processes. The manufacturing process extends into device management for robust distribution of device attributes and properties, firmware updates and then to service providers and device owners.
6. **Developer application programme interfaces (APIs)** These are APIs to enable software developers to have a consistent interface to hardware-based security functions.

U-blox Security Services Architecture (SSA)

The essential elements of u-blox's SSA are similar to ARM's PSA. This conforms to five security pillars, or principles: secure boot, secure firmware ▶

Security Services Architecture

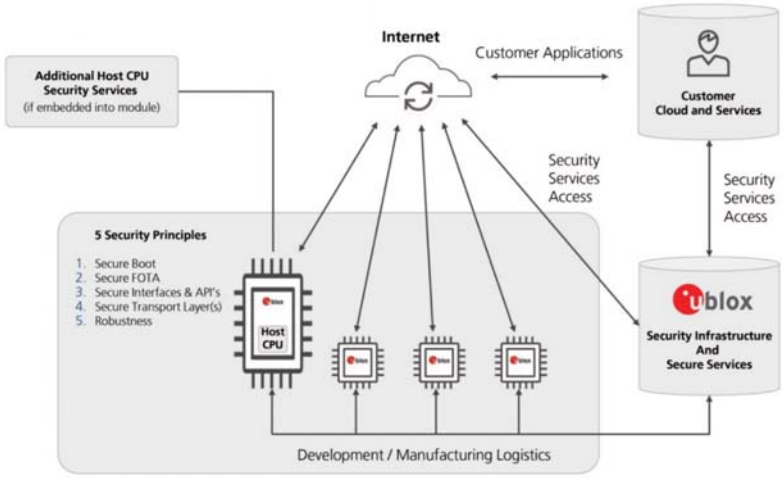


Figure 2: U-blox's Security Services Architecture

over the air (FOTA), secure interfaces and APIs, secure transport layer and robustness.

Exploring these five principles further:

1. **Secure boot** This is about the start-up software. It is the root of everything for booting up the system. It is essential that it cannot be tampered with, or else you lose the Root of Trust.

2. **Secure FOTA** This enables secure firmware updates. If there is a security problem in a device, this feature ensures the correct update is sent to fix that.

3. **Secure interfaces and APIs** This ensures authorised access for control and for debugging. This may be more than a developer interface, such as JTAG. For example, it can include a control element from an external host or other device.

4. **Secure transport layer, or secure communications** This is about securing the data from the source to the destination somewhere in the cloud. To secure the whole path, from data source to destination, requires both authentication and encryption of the link from one end to the other. That uses certificates to verify that the right server is being communicated with.

5. **Robustness** This relates primarily to external influences and whether the data being received from remote sources can be trusted or not. Examples include activities like attempted spoofing and jamming.

Wind River Helix Security Framework (HSF)

Wind River has been immersed in security since its founding, with early customers being primarily in the aerospace, defence and industrial sectors – all high security and high safety oriented. Compared with the other two approaches, there is a stronger focus on overall solution security rather than on individual devices. The principles behind Wind River's HSF are shown in **Figure 3**, starting with the industry standard confidentiality, integrity and availability (CIA) triad model for security.

The framework then decomposes those principles into security related categories and then decomposes those categories further into security-related implementations. It is then the collection of these security-related implementations that defines the security policy of an individual device.

The security assessment is the process of how to secure the embedded edge device. Identification of the assets, the vulnerabilities to those assets and security-related audit events are completed by the security assessment. Since there are always limits on time and money, the security ▶

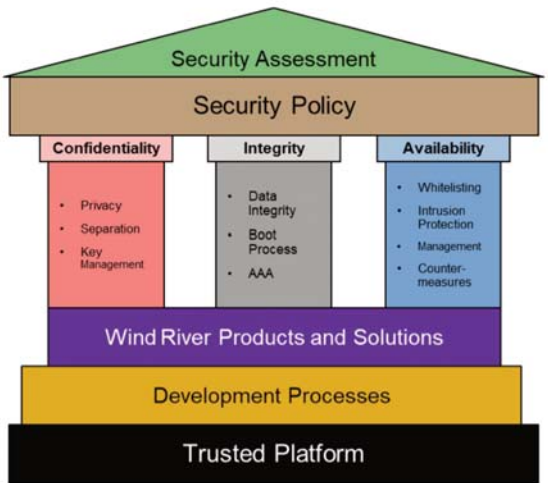


Figure 3: Wind River's Helix Security Framework

Robin Duke-Woolley,
Beecham Research

The simple definition of availability is maintaining access to the asset

assessment balances cost, performance and the environment the device operates in, with a prioritised list of recommendations provided to secure the embedded device.

The next stage - the security policy, which impacts the system - meaning both hardware and software, states what it means to secure the device. This includes the list of security implementations to use to protect the assets from the vulnerabilities along with the security-related events that need to be logged. No security is perfect, so there is a need to have a complete list of security-related events logged to perform forensics when an attack occurs – similar to the threat models in ARM's approach.

Confidentiality can be simply defined as maintaining the privacy of the asset. It is the equivalent of providing doors, walls and window coverings to provide privacy in a house. Decomposing the confidentiality principle down shows three categories – privacy, separation and key management. Of these, the privacy category is the use of cryptographic ciphers to encrypt data while it is going over a network - data-in-motion - or stored on the device - data-at-rest. The key management category is for generating and distributing the cryptographic keys needed to perform that encryption, while separation through partition is another means of protecting the privacy of the code running on a system.

Moving on to Integrity, this is defined as maintaining the content of the asset. It is the equivalent of an alarm system, a fence and locks on the doors and windows of a house, so that the contents are kept intact. It encompasses ensuring the integrity of data in all three states: over the network, stored on the device, or being processed by the device. Securing the boot process is fundamental to ensuring that the system starts with known, authentic software. There are many definitions related to secured boot, in common with all three architectures, for example verified boot, measured boot, high assurance boot, trusted boot and so on. Triple-A (authentication, authorisation, accounting) is similar to the Triple-A used by IT departments but needs to look at this internal to the embedded device.

The simple definition of availability is maintaining access to the asset. It is the equivalent of using passcodes and keys for accessing a house. This is different from in the IT arena where hot swap drives, remote failures and others are used to maintain access to your email. Availability for an embedded device gives it the ability to detect and combat attacks. It does this by detecting deviations in defined, bounded behaviour.

Surprisingly similar

Although organised differently, all three of these offerings are based on the same principles and could be regarded in a hierarchy. For an overall system, the recommended approach to security is to make an initial assessment at the overall system level, then work all the way down to each of the components in that system and ensure that each link in the chain is suitably secured. In this way, security architectures covering edge devices work together with those that cover the system level to ensure no vulnerabilities at each point, end-to-end.

One of the key issues for the IoT market is the constrained nature of some devices, for example in the LPWA segment. Depending on the type of public key infrastructure (PKI) certificate to be used for verification, this could be 2KB, 4KB or 6KB. This relates to the key length and level of security required for the application. However, this is a lot of data for a typical narrowband device that may only want to send a few bytes at a time. Ways around this are more likely to be specific to the framework being used.

Some frameworks are more complete than others regarding threat models, for example. In the ARM approach, these drive their security model. This includes a risk analysis and creating a threat model taking into account key factors, including: assets in need of protection, all potential threats for those assets, the scope and severity of those threats and the different types of attacker and the methods they may use to exploit vulnerabilities. From this research, security objectives can then be determined, and the security functional requirements established to mitigate the threats. This requires much additional research.

In addition to these frameworks, others are also available from companies like **Qualcomm** and **Intel**. In addition, a security compliance framework is available for free download through the **IoT Security Foundation** at **www.iotsecurityfoundation.org**. ■

Security of devices becomes a prime concern and needs to be addressed at the design stage

Billions of connected devices have caused participants in the Internet of Things (IoT) to reassess their approach to security. Jim Douglas, the chief executive officer of Wind River, tells Robin Duke-Woolley, the chief executive of Beecham Research, that developers of IoT applications and devices recognise they can no longer rely on patchwork approaches and instead must take a comprehensive view of security

Wind River software can be found in all major critical infrastructure sectors where security is paramount

Robin Duke-Woolley: At what point in Wind River's history did security become a key focus area for the company?

Jim Douglas: Security is embedded in everything we do. This goes back to the founding of the company in 1981. The company's first customers were primarily aerospace, defence and industrial organisations which were very security and safety oriented. So, from day one the foundational pillars of the company were security, safety and reliability. The product line and operational doctrine of the company has grown out of that. Wind River takes a holistic approach to security, which includes the following key elements:

- Secure software development lifecycle
- Built-in security features across our portfolio
- Security services and support
- Prudent security incident response

Our products, services and expertise provide our customers with a comprehensive security solution with a safeguard as new threats emerge. In addition, our development processes and security capabilities meet the rigorous requirements of the industries and governmental agencies in geographies we serve.

RD-W: Which markets does Wind River serve?

JD: Wind River software can be found in all major critical infrastructure sectors where security is paramount. From aerospace to industrial, defence to medical, and networking to automotive, our customers include the world's leading manufacturers, enterprises and governments.

RD-W: From a security perspective, what market changes are having the biggest impact on your customers?

JD: From a business and technology standpoint, connectivity in the critical infrastructure markets we serve has changed the security game dramatically. Historically, a majority of embedded systems were either not connected or were connected on proprietary networks that were not exposed to enterprise networks or the internet. Security concerns were always prevalent, but given the fact that embedded systems didn't have external exposure, security was more focused on physical intrusion. With IoT, customers have begun connecting devices using IP-based networking solutions to extract data more efficiently and use it to drive improvement in how systems operate, to improve their uptime, and to extend their product lifecycles. The ▶

IoT security breaches have brought to light the urgent imperative to protect devices and systems from external threats

availability of 5G will accelerate the proliferation of connected devices, creating a much bigger attack surface that will need to be monitored and defended, posing a significant increase in security risks. This will require customers to have rigorous, end-to-end system-level security strategies. In addition, we will see artificial intelligence (AI) based security solutions gaining traction to aid in finding and preventing malicious activity that threaten embedded systems.

RD-W: Enterprise users often view security as complex. How should they view this?

JD: I think people do perceive it as complex, and further, there tends to be a rather short-sighted view regarding security. Specifically, there is a tendency to focus on individual pieces of the system and ensure those individual pieces are secure, versus taking a comprehensive system view.

With such a wide variety of known security threat types and new ones emerging all the time, developers of IoT applications and devices can no longer rely on patchwork approaches to mitigate risk. They cannot continue using a piecemeal approach to security where one weak link in the chain can take the entire system down. They need to be thinking end-to-end rather than one-by-one. A comprehensive approach to security must take into account not only the entire IoT system - from edge devices to the network and the cloud - but also the entire system lifecycle, from development to deployment through operation and even to end-of-life.

RD-W: What do you see as the main challenges for your customers regarding security over the next few years?

JD: IoT security breaches have brought to light the urgent imperative to protect devices and systems from external threats. Security of devices has to be a prime concern of IoT system developers and device manufacturers, and needs to be addressed at the design stage.

Building security into devices poses both technical and business challenges. How much security is enough? You can over-engineer anything to be more secure, but at what price? Are you willing to compromise device performance, significantly increase the bill of materials (BOM) cost, or elongate your development cycle – all to implement security measures that you may not be able to monetise. This dilemma poses the biggest challenge facing customers when it comes to security. In parallel, experience shows that attacks on devices typically exploit multiple points of vulnerability. Closing even a few of these gaps can mitigate the damage. Technology such as the security features in VxWorks allows customers to take a scalable approach to security, adding as much or as little as the device requires for its purposes, making it possible to control costs and deliver devices on schedule while reducing the risks of security breaches.

We can't forget though about securing legacy software, which will also continue to be a challenge for our customers. To address this challenge, we enable customers to partition legacy software with capabilities like virtualisation and real-time processes found in VxWorks and Wind River Helix Virtualization Platform. This helps limit the attack surface of the device when major, externally facing functions are impacted. Partitioning is a great security implementation to mitigate the entire system from being attacked.

RD-W: How would you sum up how Wind River is helping customers address security?

JD: Security is so fundamental to IoT system development that it requires a well thought-out, end-to-end strategy encompassing all aspects of a target systems operational cycle including power on, boot up, runtime, network connection, sleep, power down, and all stages of the systems lifecycle, from development to decommissioning. This is why our customers turn to us.

First, we follow a strict security development process from design to coding, testing and build to ensure we deliver solutions that are highly secure and reliable for critical infrastructure IoT systems.

Second, with built-in security capabilities, our products enable customers to implement comprehensive security that minimises attack surfaces end to end, from devices through communications networks and gateways to the cloud.

Third, our professional services team offers security assessments to help customers understand the confidentiality, integrity and availability considerations of their system architecture, as well as sets security policies and guides their security investments. In addition, we deliver a consultative process to determine the type and level of security appropriate for any project and help build in security from step one and for every stage of the process.

Lastly, knowing we have billions of devices deployed with our technology and that savvy attackers could find vulnerabilities in even the most secure systems, Wind River has in place a best-in-class security incident response process that our customers rely on us for. Our stringent release process includes aggressive testing, and our team actively works with the research community and monitors a variety of security sources. Following responsible disclosure, we proactively notify customers of potential vulnerabilities, offering resolution measures in advance of vulnerability disclosure. Our response process helps protect devices from cyberattacks even after product deployment.

In summary, what's important to our customers is having vendors like Wind River with a long track record of developing, delivering and supporting secure development processes to ensure our products are developed as securely as possible, building in security capabilities across our product portfolio, providing security services and support, and responding immediately when new vulnerabilities are discovered.

www.windriver.com

Companies need a framework for implementing security in IoT systems and embedded devices

Security is foundational to the reliability of IoT systems and devices, writes Arlen Baker, the chief security architect at Wind River. Everyone from the developer to the operator to the end beneficiary needs to have confidence that an IoT solution will perform as promised, without putting anyone's privacy or safety at risk. Moreover, the ability to demonstrate effective security is increasingly critical for compliance with stringent standards such as the EU's General Data Privacy Regulation (GDPR), and for obtaining product safety certifications from various regulatory entities

Given the rapid pace of IoT adoption and the pressure on developers to bring solutions to market quickly, that's a fairly tall order. How can IoT developers address security efficiently across the solution lifecycle?

IoT developers would benefit from a systematic approach to security, grounded in a clear understanding of security needs and objectives. A prime example of such an approach is the Wind River Helix Security Framework, designed to help developers optimise the security capabilities built into Wind River embedded software solutions.

The Helix Security Framework starts with the industry standard model of Confidentiality, Integrity and Availability – the widely accepted CIA Triad. Then we take it a step further and deconstruct each of these three principles into tangible security implementations. In the context of the Triad, confidentiality encompasses implementations designed to maintain the privacy of an asset. Integrity refers to ▶

SPONSORED ARTICLE

IoT developers would benefit from a systematic approach to security, grounded in a clear understanding of security needs and objectives

measures that protect the content of the asset from disruption or corruption. Availability includes implementations that ensure accessibility of the asset. We then apply these implementations specifically to the requirements of the embedded systems our customer needs to secure.

That's the high-level explanation of the framework, but how does it work in practical terms? To put it more simply, security functionality is built into every product across our portfolio that we offer for embedded system developers. However, that in itself is not enough to ensure that devices built with these solutions will be secure. It takes an additional measure of expertise and analysis in a comprehensive approach to identify and implement the right security capabilities for each system's requirements. The Helix Security Framework enables users to determine which security features they need for their specific applications and how to activate those features.

Three stages of training

In practice the framework comes to life through a customised embedded security training class. The class is based on the specific Wind River solution the customer is using and the application they're using it for. Classes typically entail three stages over three days. Day one is focused on understanding the framework, breaking it down into security implementations, and laying the foundation for what is needed to secure an embedded device. Day two involves going through the various security features within the Wind River product that will put those implementations into effect. Importantly, no single security solution by itself will provide complete protection for an IoT device. Rather, it is the proper layering of these defences that will provide a much stronger, multifaceted protection, commonly referred to as defence-in-depth.

On the third day, we conduct a hands-on lab that enables the customer to bring it all together – to use the tools identified on day two to implement the security requirements identified on day one.

That's the educational component of the framework, essentially teaching our customers how to secure their devices using the tools built into the solutions they've acquired from Wind River. Another key component of the framework is a security assessment. It's similar to the training class in that it starts with laying the foundations, going through the implementations coming out of the CIA Triad, and making sure the customer understands what it means to secure the device. We follow that with a deep dive into the customer's specific need to define the system assets, the vulnerabilities of those assets, and the security implementations needed to secure them. We put all that in a written report that the customer can execute against.

Versatile deployment

In different scenarios with several customers, the Helix Security Framework has proven effective in empowering development teams to meet their security objectives. It has been applied in securing medical devices, head-up displays for military aircraft, industrial control systems, power plants, wastewater and sewage systems, and other IoT systems for critical infrastructure. We've applied it on behalf of customers building new systems from scratch, as well as for industrial and critical infrastructure operators faced with upgrading and connecting brownfield legacy systems and equipment.

The beauty of the framework from the customer's perspective is that it is repeatable and transferrable. One client with a major defence contractor told us his team was applying our process not just to the initial engagement, but to multiple projects across the corporation. We gave them the framework and taught them how to use it, and they ran with it.

Another customer in the medical device arena was looking for a commercially available operating system (OS) that provided continuous security monitoring and vulnerability protection. In fact, the company had incurred a great deal of negative press about the vulnerabilities in its devices, and was causing them financial impacts. Walking through the Helix Security Framework was a big factor in the company's decision to go with Wind River Linux, along with our continuous security monitoring and vulnerability protection, and the next release of its device incorporated the recommendations derived through our security assessment.

IoT and embedded system developers need a systematic approach to security that can be integrated into the development process. For users of Wind River technology, the Wind River Helix Security Framework has been proven in the trenches. It's a way for IoT developers and system operators to gain the upper hand against malicious actors, while enabling them to meet the marketplace and regulatory demand for safe, secure and reliable systems. ■

www.windriver.com

IoT security is a driver for your business objectives

IoT devices interact with the physical world all of the time and in rapidly evolving ways. Securing them is much more challenging than has traditionally been the case with information technology (IT). In the Internet of Things (IoT), physical things are in need of protection, whereas in information technology it is largely data – cyberspace – that is being secured. Countless such things that are already out there in the real world, in millions of locations, have all become part of an ever-growing attack surface

To ensure business success in the IoT space, the protection of devices and the data they transmit must be a primary objective. Safety is a preeminent concern, and there is no safe operation without security. The consequences of failing to sufficiently secure IoT devices is perhaps most obvious in connected health, where device safety protects lives: the protected asset is not actually a thing but a human being, such as a customer, employee, user or child. Inadequate safety can harm users by exposing their devices to hackers. Customers and employees can be impacted by the blowback in the wake of such attacks, through costly lawsuits and even jail time, especially if negligence can be proven.

Many companies view security as an insurance policy, something they need to have in case of an attack. This insurance policy protects them from the cost of replacing or upgrading breached devices and the cost of damages from exposed confidential user information.

But instead of viewing security as a burden – a cost centre – companies should view it as an opportunity to protect revenue. Having the ability to prevent denial of service attacks, ensure the accuracy of billable charges, or detect counterfeit devices all affect the top line and should thus be of concern to any senior corporate decision maker.

Examples from connected health

Connected medical devices are a rapidly growing market. According to **Berg Insight**, global revenue for connected medical devices will reach €18.7bn in 2023, as services traditionally offered by doctors and healthcare personnel are transitioning to automated interactions. This trend coincides with new ways of managing medical data in the era of big data: medical records are now largely digital, as an increasing number of healthcare facilities are deploying electronic health record (EHR) systems to additional data feeds and applications. While this increases the value that can be gained from the data, it also makes them vulnerable to attack.

And, as the cliché goes, it's not a question of if IoT devices will be attacked, but when – in particular when high value assets and data are involved. There have already been a number of well publicised ▶

The attack surface at many medical providers is significant due to the scale, diversity and advanced age of IT systems and medical devices

vulnerabilities and breaches. For example, the US Department of Homeland Security issued a warning concerning certain insulin pumps and pacemakers that allowed attackers with low skill level to make remote changes to patient implants. The one saving grace was the fact that attackers would require close proximity to the patient, due to the use of short range radio wave connectivity.

However, causing bodily harm may not be the objective of an attack. It is entirely conceivable that other motives play a role. A ransomware attack similar to the WannaCry virus that affected millions of PC users around the world in 2017 could threaten to disable equipment and endanger patient safety unless a ransom is paid.

In either case, such vulnerabilities need to be identified and addressed in the design and development of IoT devices. The integrity of any connected device must be ensured through functions such as an immutable Root of Trust (RoT) located within a secure element. From the RoT secure keys can be derived that ensure encrypted communication. Device access must be limited so that only authorised users can access devices and functions.

Medical records are another source of attack and trade on the black market, where they bring in several times the black market value of financial records according to a report by **Trustwave**. In many cases, they contain the same amount of personal information but are often less secure, and breaches are detected less quickly than those of banking records. The data can then be used to create false claims, allowing attackers to obtain medical equipment or drugs that can be resold on the black market for profit.

The attack surface at many medical providers is significant due to the scale, diversity and advanced age of IT systems and medical devices. As a matter of fact, one of the victims of the WannaCry ransomware attack was the UK's National Health Service, affecting up to 70,000 connected medical devices and IT systems in hospitals throughout England and Scotland. In parts of the country, any non-essential medical procedures had to be postponed as a result of the attack.

It is therefore imperative that the security of data sent back and forth between any devices connected to an IT system is ensured and that a breach will be contained and not bring down the entire system. The identity and authenticity of all connected devices needs to be known and their integrity must be protected.

The u-blox solution

u-blox Internet of Things security features and services are designed for critical applications delivering confidential data. The company integrates best-in-class hardware and software security to deliver holistic, ready-to-go security solutions.

The u-blox SARA-R5 NB-IoT and LTE-M cellular module features industry-leading security, starting with an immutable, hardware-based Root of Trust that is embedded in a secure element. It provides a unique device identity and foundational security for all other functions, such as secure boot, secure updates and anti-cloning detection. A proven, lightweight key management system derives pre-shared security keys in device and cloud, which reduces power and data overhead while providing end-to-end and local data encryption.

www.u-blox.com

Elisa Costante, Forescout Research Labs

Philip Griffin, NetFoundry

Some IoT devices are too smart to be secure, say Forescout and Netfoundry

The Internet of Things (IoT) industry has awoken an age-old conflict, the power struggle between technology's two rival groups: The Doers and the Dilettantes, writes Nick Booth

The former get on with moving things forward. The latter love to sell themselves, often running in front of the parade and pretending to lead it. One camp quietly engineers things on everyone's behalf, the other is full of brash self-promoters. In the IoT world, you could classify the two technology camps as operational (OT) and information (IT).

OT is brilliant at creating an infrastructure. For example, telecoms operators built the framework for the mobile internet. But it was the IT people who got to go over-the-top (OTT).

The danger with those who over-reach and make extravagant claims is that these are the classic symptoms of insecurity. Which is ominous for IoT, because safety, surety and stability have now become the holy trinity of the connected world, according to Elisa Costante, senior director for industrial innovation and operational technology at **Forescout Research Labs** (FRL).

Security landgrab

Meanwhile, the landgrab by the IT people continues. Gartner research says that OT security is falling into the hands of the IT people. By next year 70% of security will be managed by CIOs and CISOs. That's up from 35% last year. That's got to be wrong. We want security to be managed by people with their feet on the ground, not blue sky thinkers with their heads in the cloud.

FRL was built to explore the security implications of hyper-connection and chart the types of threat presented by every device. The new set of ▶

variables presented by each new addition just acts to multiply the number of attack surfaces. Costante's calling is to identify the threats and call out the nonsense.

In FRL's latest report, *Rise of the Machines*, Costante identifies one of the age-old problems of IT: double speak. This is where technology promises one thing and delivers the opposite.

Too stupid by far

Smart systems, for example, are invariably so stupid they're a liability. Their lights are easily hijacked and smart buildings are taken in by hackers far too easily. The most popular targets for fraudsters are surveillance cameras, which are commandeered so readily they should be classified as insecurity devices.

FRL managed to replace a network video recorder's footage with previously recorded fake content. This proves that cameras are capable of helping the criminals, rather than aiding the prosecution. By extension, they make cyber-physical attacks possible too.

DEF CON 27

The finding, presented at the DEF CON 27 ICS Village in Las Vegas on 10 August, tells us that smart things are stupid when they over-reach, says Costante.

One way they are stretched is the use of thousands of devices with a myriad of operating systems and network protocols. Spreading yourself too thin means compromising on quality and most IoT devices are installed as default settings.

The security search engine **Shodan** lists 4.7 million devices that could be fooled by these unencrypted protocols.

The next big IoT challenge

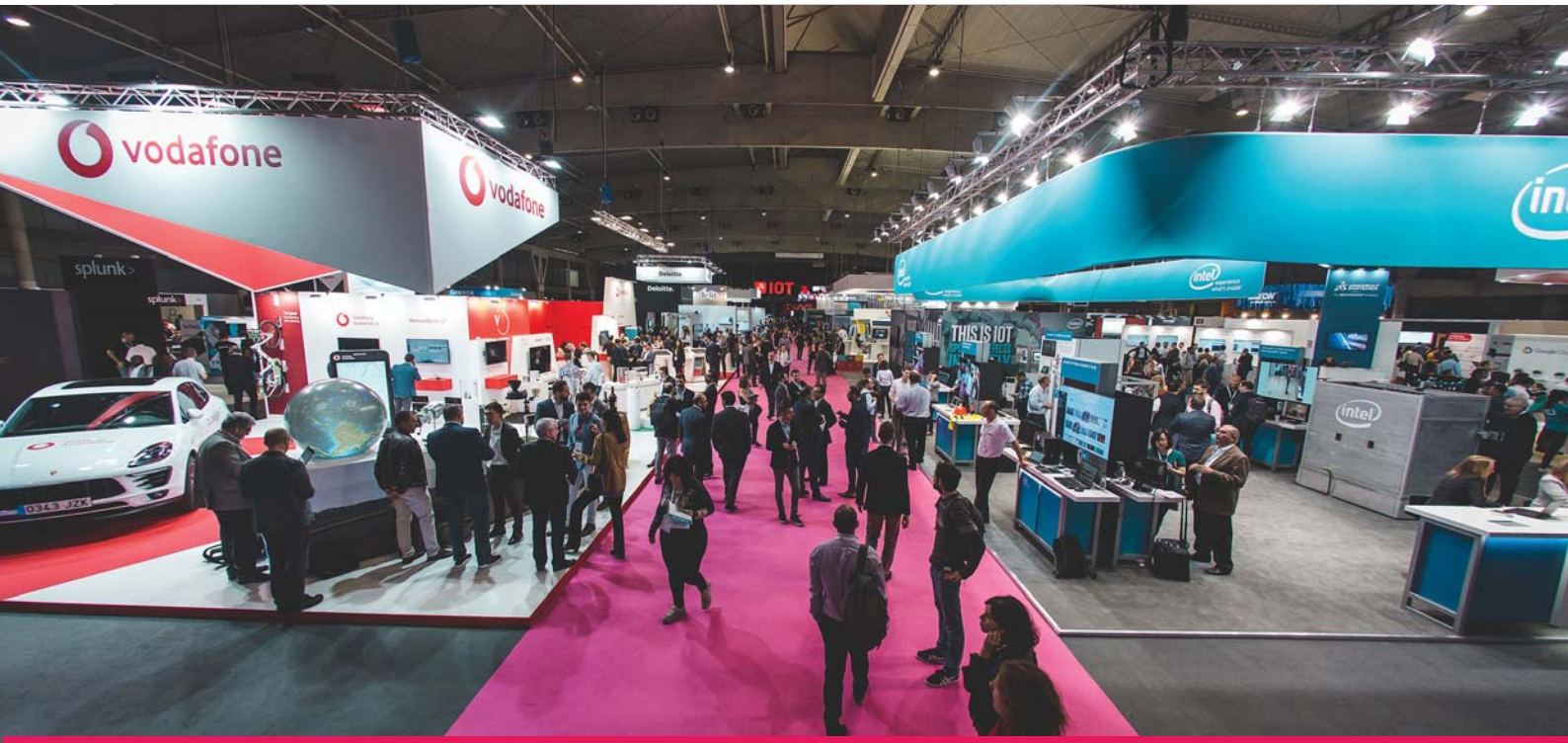
Simplifying all these disparate variables - operating systems, syntaxes, protocols - is the next big challenge for IoT and the inspiration for companies such as **NetFoundry**.

NetFoundry's solution is a single overlay – in the form of a managed software service – that takes care of all the complexity. The alternative is to run your own integration services – such as jump servers, data diodes and private access point names (APNs) – all of which are horrendously complicated, says NetFoundry's head of partnerships Philip Griffin. Attempting massive projects in-house usually becomes a legal liability too.

NetFoundry works with the likes of **Microsoft**, **CoreSite**, **Digital Ocean** and **Vapor IO** to simplify the interfaces between applications and operations.

Which sounds like it is rationalising the best bits of OT and IT and finally getting them to work together.

That could be hard to maintain. In the struggle between The Doers and The Dilettantes, the first casualty is the truce. ■



The IoT Solutions World Congress will bring together the leaders of the digital transformation of industries

The IoT Solutions World Congress (IoTSWC), the largest international event focused on innovation in the Industrial Internet of Things (IIoT), will return to Fira de Barcelona's Gran Via venue from 29 to 31 October 2019. In its fifth year, the IoTSWC will reveal the real scope of the digital transformation in different industrial sectors and businesses that are incorporating disruptive technologies such as IoT, blockchain and artificial intelligence (AI) into their activity. The exhibition area will bring together more than 400 exhibitors, including leading global providers of IoT solutions, AI and blockchain

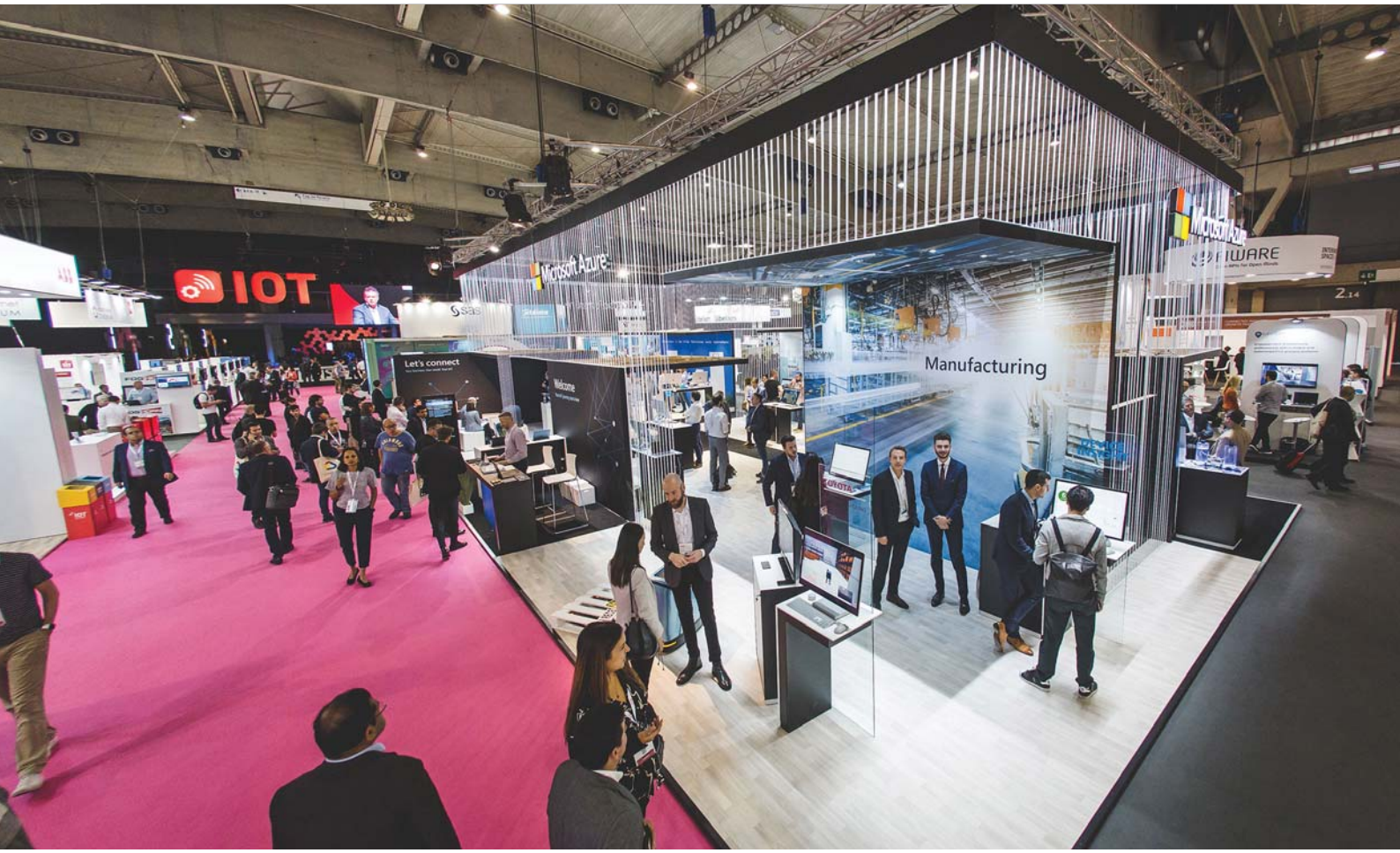
Organised by Fira de Barcelona in partnership with the Industrial Internet Consortium, this year's IoTSWC is expected to grow by 15% compared to 2018 in terms of the number of exhibitors. The companies set to attend include those from the information technology sector, software platform developers, cybersecurity companies, service and telecommunications providers, industrial automation firms, consultancy firms, hardware manufacturers, technological and R&D centres, incubators, associations and IoT-related entities.

The list of participating companies includes **Microsoft**, **SAS**, **T-Systems**, **Vodafone**, **Nutanix**, **Deloitte**, **Libelium**, **Kaspersky**, **Orange**, **Fiware**, **Hitachi**, **Relayr**, **Siemens**, **Thingstream**, **Zyfra**, **Emnify**, **ARM**, **Things O2** and **Linux Edge Foundation**. Leading companies from different sectors adopting IoT solutions will also attend via the industrial partner programme. The countries set to provide the highest number of exhibitors are Spain, the USA, China, France, Germany and the United Kingdom.

Similarly, IoTSWC 2019 will have internationally grouped participations and institutional halls. In this regard, the presence of stands from Greece, Austria, Germany, Spain, Catalonia and Barcelona have already been confirmed; these will contribute a large number of companies to the event, many of them small-to-medium sized enterprises (SMEs) and startups linked to the IoT ecosystem.

A new feature of this year's fair will be a specific area called **IoT Solutions .Font**, which will provide visibility for startups with original and innovative products and services based on IoT, AI and blockchain, tested in the market and with ▶

SPONSORED PREVIEW



IoTSWC will also host a testbed area to showcase ten experimental platforms designed to apply new solutions and test them under real operational conditions that will be addressing challenges

potential for internationalisation. In partnership with Conector Startup Accelerator, about twenty startups from all over the world have been selected, which, in addition to exhibiting at the trade fair, will take part in a competition to choose the best start-up along with a networking activity involving investors, sponsors and visitors interested in finding out more about their solutions. The winning startup will gain direct access to a Conector acceleration programme.

Testbeds and Congress

IoTSWC will also host a testbed area to showcase ten experimental platforms designed to apply new solutions and test them under real operational conditions that will be addressing challenges such as: How can wind turbines on wind farms be fixed remotely? Will there be variable insurance policies that adapt to our driving behaviour? How can cyberattacks affecting the safety of autonomous cars be tackled? How can the water pollution of a river be monitored? How can energy losses in gas distribution networks be detected? and How can one find out the condition of crops in real-time?

The Congress programme will focus on nine core themes: IoT enabling technologies; connected transport; manufacturing; energy and utilities; healthcare; buildings and infrastructure; open industry; artificial intelligence and blockchain. There will be 200 sessions, including talks, roundtable discussions and presentations, and more than 400 speakers are expected to participate. The Congress will focus mainly on the best practices and success stories of companies that have achieved significant competitive advantage.

Noteworthy among the list of speakers is the American analyst, Joe Barkai, directors from major technology companies such as **ABB**, **Dell**, **Ericsson**, **Google Cloud**, **Huawei**, **IBM, Hitachi**, **Microsoft**, **SAS**, **Wipro**, **Fiware, Honeywell**, **Amazon Web Services**, **Thingstream**, as well as companies who are already using IoT solutions such as **Hugo Boss**, **Uber**, **Airbus**, **Netflix**, **Sanitas**, **Carrefour Group**, **Daimler Motors**, **Ibercaja**, **Roca**, **SNCF Réseau**, **Maersk GTD** and **Brussels Airport**, among others.

IoT Solutions World Congress
From 29 to 31 October 2019
Fira Barcelona's Gran Via venue
Av. Joan Carles I n.58-64. L'Hospitalet de Llobregat (Barcelona) Spain
https://www.iotsworldcongress.com/


Ask Us What Is Possible
THE GAME CHANGER
THE INDUSTRY'S FIRST
IoT SPECIALIST
MARKETING AND ADVERTISING
AGENCY
NOTHING IS OFF LIMITS
www.wkm-global.com
contact@wkm-global.com
we know

Connect with the latest technologies from generation to grid

European Utility Week and POWERGEN Europe, a three-day event that spotlights every part of the energy ecosystem, is coming to Paris, France from 12-14 November 2019. The event will welcome the influencers, disruptors and innovators in Europe's energy sector to the Paris Expo Porte de Versailles to highlight the strategies and technologies that will deliver their shared vision of a fully integrated and interconnected European energy system

A packed conference programme will take a deep dive into the trends and future direction of each aspect of the sector – from generation to grid to end users – while a bustling exhibition floor will give visitors the opportunity to see the latest technologies first hand, exchange ideas and share knowledge.

Hot topics will include storage and integration, digitalisation, grid edge technologies and the challenges facing a changing power generation mix.

This unified event offers a one-of-a-kind opportunity to be at the heart of Europe's energy transition and join decision-makers and thought-leaders to plan the path to a zero-carbon economy.

A key focus of the show will be the way that the energy industry is embracing digital technologies. In recent years, power and utility companies have realized significant benefits from adopting solutions that involve IoT, big data and analytics.

In the Summit conference sessions, these key questions will be addressed:

- How do I maintain security in an increasingly connected and digitalised energy system?
- Where is digitalisation taking us?
- What is the current digital roadmap?
- What kind of problems can be solved by what kind of technologies on a strategic level?
- Which is the most prominent cyber threat?
- Is data in the service of the digital citizen?

There is no doubt that digitalisation is already improving energy systems in the sectors related to safety, productivity, accessibility and sustainability. With the use of digital technologies, the sector becomes more connected, smarter, more efficient and reliable. Collaboration between the various stakeholders becomes easier with the help of new technologies and the consumer is more and more included in the decision-making process.

Digitalisation Hub

In the Digitalisation Hub on the exhibition floor, the event will investigate the nature of these technologies and learn from innovative projects that are in the making, already running or which have finished their cycle, and the secrets of their success or failure.

Greater efficiencies in the power generation are being won by applying predictive analytics and machine learning to traditional methods of maintenance and optimisation for power plants and their equipment, particularly to enable a greater flexibility of operations.

European Utility Week and POWERGEN Europe will explore how these IoT-enabled technologies have helped the power and utility sector stay ahead of the game in the European energy transition – and it will also highlight the still-untapped opportunities that can be unlocked.

Another key aspect that will be spotlight by speakers is cybersecurity. As the power and utility sector employs an increasing number of digital solutions, so too does it make itself vulnerable to security incidents, not just from outside hackers but also from unintended incidents caused by employees.

European Utility Week and POWERGEN Europe will showcase the latest solutions for the industry, from generation to grid, and also present a number of case studies from experts working within the cybersecurity sector.

www.european-utility-week.com

SPONSORED PREVIEW

European Utility Week

POWERGEN EUROPE

JOIN US IN PARIS!

12 - 14 November 2019

Paris Expo Porte de Versailles, Paris, France

The end-to-end industry event for the energy sector.

European Utility Week and **POWERGEN Europe**, a three-day event that spotlights every part of the energy ecosystem.

Join the **influencers, disruptors,** and **innovators** in Europe's energy sector and hear about the strategies and technologies that will deliver a shared vision of a fully integrated and interconnected European energy system.

A packed conference programme!

Deep dive into the trends and future direction of each aspect of the sector – from generation to grid to end-users!

Walk a bustling exhibition floor to see the latest technologies first hand, exchange ideas and share knowledge.

Hot topics!

Including storage and integration, digitalisation, grid edge technologies, and the challenges facing a changing power generation mix.

A one-of-a-kind opportunity to be at the heart of Europe's energy transition!

Register for your free pass: **www.european-utility-week.com**

#EUW19 | #PGE19 #EUW19 | #PGE19

European Utility Week | POWERGEN Europe

Part of CLARION ENERGY POWER & ENERGY SERIES

15% DISCOUNT

10 REASONS TO SUBSCRIBE TO IoT NOW!

The next era is coming to the Internet of Things. Be the first to know what's happening. Since 2010 **IoT Now** has been read by business leaders in over 100 countries. Don't get left behind! **Subscribe to receive your hard copy of IoT Now.**

The glossy 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 every upcoming issue, subscribe here!

10 reasons not to miss out:

1. Exclusive face-to-face insights from the C-Suite
2. Independently-commissioned Analyst Reports
3. 'How To' features for your industry sector
4. Case Studies of connected world successes
5. Unrivalled Hot Lists of IoT/M2M Contract wins
6. All the key upcoming Events worldwide
7. In-depth Talking Heads Interviews
8. Outspoken Blogs and Opinions
9. News about Products, People & Companies
10. Special Supplements focusing on IoT Events

15% OFF – FOR A LIMITED TIME ONLY!

Subscribe to IoT Now • Price includes delivery to your address worldwide • 4 hard copies (NORMAL PRICE UK£60.00) NOW JUST £51 a year • Access our Digital Edition 24/7

Go to: www.IoT-Now.com and Click on "SUBSCRIBE"

5G Asia
Singapore
10-12 September 2019
get.knect365.com/5g-asia-pre-register-2019

IoT World Asia
Singapore
10-12 September 2019
registration.n200.com/survey/35v7xmli5dqfu

Edge Computing Congress
London, UK
17-19 September 2019
tmt.knect365.com/edge-computing-congress

Digital Transformation North America
Dallas, USA
23 September 2019
dtaw.tmforum.org

MVNOs Asia
Singapore
24-25 September 2019
tmt.knect365.com/mvnos-asia

Industry 4.0 Conference
Chicago, USA
23-24 September 2019
events.marketsandmarkets.com

5G Core
Madrid, Spain
24-25 September 2019
www.bit.ly/2Mh8DWT

AI World Summit
Amsterdam, The Netherlands
9-10 October 2019
www.worldsummit.ai

Internet of Supply Chain
Berlin, Germany
9-10 October 2019
iosc-de.internetofbusiness.com

MVNOs Europe
London, United Kingdom
15-16 October 2019
tmt.knect365.com/mvnos-europe

e-sim Connect
London, United Kingdom
15-16 October 2019
tmt.knect365.com/e-sim-connect

MWC19 Los Angeles
Los Angeles, USA
22-24 October 2019
www.mwclosangeles.com

AI World Conference & Expo
Boston, USA
23-25th October 2019
www.aiworld.com

HLTH 2019
Las Vegas, USA
27-30 October 2019
www.bit.ly/2Vy1kf8

IoT Solutions World Congress
Barcelona, Spain
29-31 October 2019
www.iotsworldcongress.com

Industrial IoT World
Atlanta, USA
31 October-1 November 2019
tmt.knect365.com/industrial-iot-world

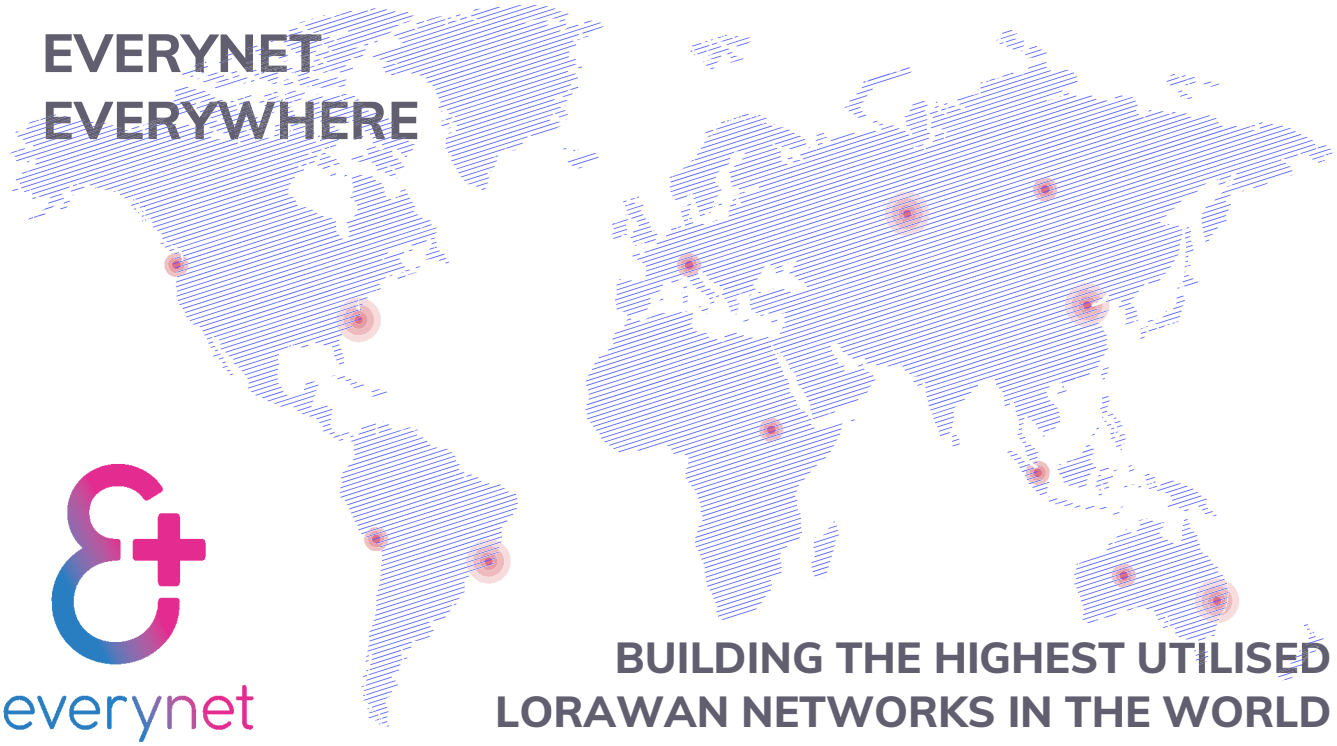
Smart Cities Summit
Atlanta, USA
31 October- 1 November 2019
tmt.knect365.com/smart-cities

Telco AI Summit Europe
London, UK
5-6 November 2019
tmt.knect365.com/telco-ai-summit-europe

Digital Transformation Asia
Kuala Lumpur, Malaysia
12-14 November 2019
dta.tmforum.org

AfricaTech
Cape Town, South Africa
12-14 November 2019
tmt.knect365.com/africacom/iot-world-africa

EVERYNET EVERYWHERE



everynet

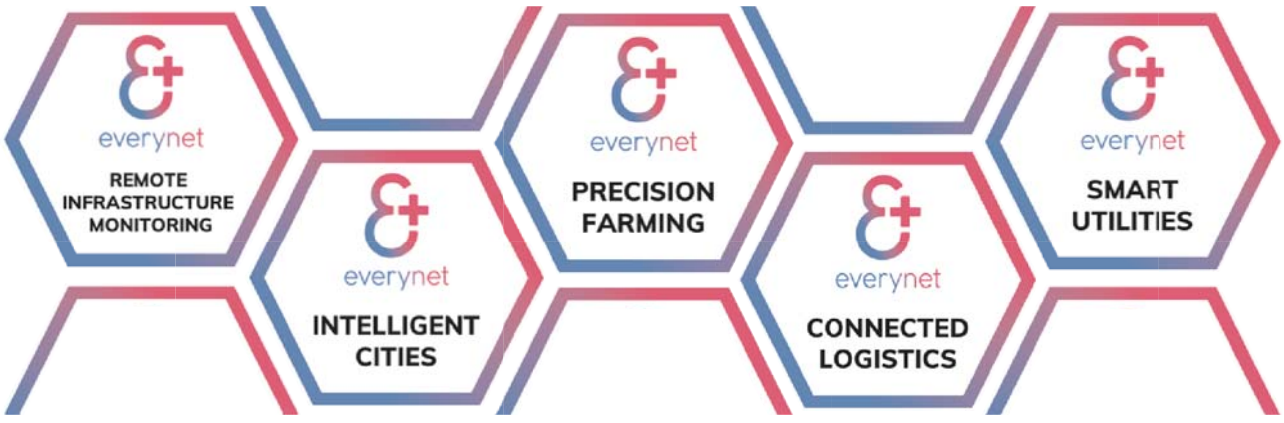
BUILDING THE HIGHEST UTILISED LORAWAN NETWORKS IN THE WORLD

Everynet has pioneered the concept of Everywhere: to build and operate the world's largest neutral-host LPWA networks for low-cost, low-power, long-range IoT, enabling the rapid digital transformation of existing global markets. Everynet's innovation focuses on massive scale, by balancing ultra-low-cost solutions with carrier-grade service levels

With a curated ecosystem of partners providing ready solutions to the most valuable use-cases in the market, Everynet accelerates time-to-revenue while fostering an in-country ecosystem of developers for long-term sustainability

With this unique shared-economy model Everynet offers the lowest capex, lowest opex, and shortest time-to-revenue for IoT network operators

Connect with Everynet today



IoT Now: ISSN 2397-2793

Q3 2019 • VOLUME 9 • ISSUE 3

IoT now

HOW TO RUN AN IoT ENABLED BUSINESS

TALKING HEADS

Romil Bahl of KORE explains why 80 billion connected devices demand an open, modular and scalable platform

IoT Now Guide to MWC19 Los Angeles

PLUS: Rust never sleeps as 42 Technology accelerates low cost, secure cellular IoT • IBM and AT&T detail their new strategic alliance in edge platforms and 5G • The Contract Hot List • How to avoid getting burned by bad platform selection • The top five things to ask of a connectivity management system • Inside the era of intelligent connectivity at MWC19 Los Angeles • Latest news online at www.iot-now.com

Secure Your IoT Devices Against Predators

DON'T LET YOUR DEVICE DATA BE FOOD FOR CRIMINALS.

Keeping your data secure is business critical. Reduce the risk of compromised application data with ConnectionLock™ – a core feature of the Aeris IoT network. This software-based IoT firewall restricts device communication to a set of customer-defined endpoints, significantly reducing the risks of catastrophic data theft and malicious device takeovers.

ConnectionLock brings an additional layer of security, providing an integral step in the effort to keep the IoT secure in a simple and economical way.

aeris

FUTURE PROVEN
IoT Connectivity

It's a jungle out there.
Make sure your devices are
out of danger's reach.

Learn more at: aeris.com/tiger

IoT Now Guide to MWC19 Los Angeles

IN THIS ISSUE

PUBLISHED BY: WeKnow Media Ltd. Suite 138, 70 Churchill Square, Kings Hill, West Malling, Kent ME19 4YU, UK Tel: +44 (0) 1732 807411

NEWS IN BRIEF

PTC enhances connectivity to industrial automation assets

PTC has released the newest version of its Kepware industrial connectivity software. Kepware is foundational to the industrial connectivity capabilities of PTC's ThingWorx Industrial IoT platform. The KEPServerEX 6.7 solution aims to make it easier for users to connect to all industrial automation assets via a single, secure application.

Connectivity to industrial automation equipment is critical to improving operational efficiency. Engineers often rely on a mix of commercial and home-grown connectivity tools to navigate complex and heterogeneous production environments. The increased complexity, cost and bandwidth spent retrieving industrial data, instead of interpreting and using it, has created a business need for a single, secure solution through which enterprises can connect all of their production assets. PTC says KEPServerEX 6.7's breadth of connectivity, reliability and security features empower engineers to focus on process efficiencies and product improvement. ■

Semtech releases new LoRa smart home device for IoT applications

Semtech, a provider of analogue and mixed-signal semiconductor products and advanced algorithms, has announced a new LoRa smart home device to extend LoRa's market applications from industry-class low-power wide area networks (LPWANs) to smart home, community and consumer applications. The transceiver, called LLCC68d, provides low power and extensive coverage for Internet of Things (IoT) devices in indoor and adjacent areas to connect sensors and actuators for security, environmental monitoring and convenience applications.

"This new LoRa smart home chip is compatible with the LoRaWAN protocol for low-latency smart home applications such as smart locks and lighting, enabling low-cost network expansion and many LoRaWAN-based B2B and in today's IoT market. The B2C solution provides a bridge," said Marc Pegulu, the vice president of IoT business at Semtech's Wireless and Sensing Products Business Unit. ■

42 Technology aims to accelerate secure, low cost cellular IoT environment as it claims 'first use' of Rust on Nordic SiP

Jonathan Pallant, 42 Technology

The Rust programming language application for a single-chip Internet of Things (IoT) device, which is claimed to be the first in the world, has been announced by **42 Technology,** the product design and engineering consultancy.

This software achievement could accelerate the development of more robust and secure low cost, low powered cellular IoT products and systems, and play a critical role in unlocking significant new markets for smart industrial and consumer products. For example in areas such as real-time asset tracking and monitoring, utility metering and smart city technology.

Rust is a very high-performance alternative to systems programming languages such C and C++, which avoids the memory safety issues that plague those languages, and without the complexity and overhead of Java. 42 Technology has developed the world's first Rust-based single chip IoT application using Nordic Semiconductor's nRF9160 development board. This software could help drive a new generation of more robust and more secure low cost IoT products.

In recent field trials, 42 Technology's Rust application made secure encrypted connections to **Amazon** cloud services via an early LTE Cat-M network that is being rolled out across the UK by **O2**, the mobile network operator. The board also supports NB-IoT which is being launched by **Vodafone** and other operators.

"42 Technology has specifically developed its Rust-based application to demonstrate an easier and faster way for companies to develop new products for the cellular IoT revolution but without inadvertently compromising on security," said Jonathan Pallant, the senior consultant who led the application development programme at 42 Technology and is also a founding member of the Rust Embedded Working Group. "Our aim is to help eliminate the security vulnerabilities that too many people have seen, for example, with low cost home security cameras, smart hubs and with medical equipment such as insulin pumps." ■

Claroty extends visibility of industrial cybersecurity platform to IoT

Claroty, the global provider of industrial cybersecurity, has introduced several enhancements to Continuous Threat Detection (CTD), its operational technology (OT) security solution. The latest release of CTD now enables enterprises to discover and monitor their Internet of Things (IoT) devices, provides customers with greater network visibility, reduces deployment time, and eliminates the noise of non-critical alerts. The company also announced it has joined the **Industrial Internet Consortium (IIC)**, the organisation that transforms business and society by accelerating the adoption of the Industrial Internet of Things (IIoT).

Claroty's announcements come as enterprises increase their use of IoT devices to drive digital transformation and increase the efficiency of their operations. **Gartner** research has forecast more than 65% of enterprises will adopt IoT products by 2020.

With the latest update to CTD – version 3.5 – customers now enjoy the benefits of Claroty's deep packet inspection technology across both IoT and OT devices. The solution automatically discovers IoT devices on the network and classifies each device based on both static and behavioural attributes. It then identifies known vulnerabilities and other risks associated with those assets, and continuously monitors the environment for threats and policy violations.

"Claroty's natural expansion into the IoT space enables us to empower customers with an unparalleled breadth and depth of visibility across their networked OT and IoT environments," said Amir Zilberstein, the chief executive of Claroty. "By using our comprehensive IoT-OT platform, customers can now embrace digital transformation initiatives with a higher level of confidence than ever before." ■

IBM and AT&T announce multi-year strategic alliance

IBM and **AT&T** have announced a multi-year strategic alliance. Under the agreement AT&T Communications will use IBM's expertise to modernise AT&T Business Solutions' internal software applications, enabling migrations to the IBM Cloud. In addition, IBM will provide infrastructure to support AT&T Business's applications. AT&T Business will utilise **Red Hat**'s open source platform to manage workloads and applications. The improvements will allow AT&T Business to better serve enterprise customers.

IBM will also make AT&T Business its primary provider of software defined networking. AT&T Business will help transform IBM's networking solutions with their latest technologies including 5G, Edge Compute, and IoT as well as multi-cloud capabilities using Red Hat. This builds on the existing relationship where AT&T Business is IBM's strategic global networking provider.

"In AT&T Business, we're constantly evolving to better serve business customers around the globe by securely connecting them to the digital capabilities they need," said Thaddeus Arroyo, the chief executive of AT&T Business. "This includes optimising our core operations and modernising our internal business applications to accelerate innovation. Through our collaboration with IBM, we're adopting open, flexible, cloud technologies, that will ultimately help accelerate our business leadership."

The two companies will also collaborate on edge computing platforms, which will help enterprise clients capitalise on the power of 5G network speeds and the internet-connected devices and sensors at the edge of the network. Using 5G, enterprises will one day be able to rapidly transmit data to and from multiple clouds and billions of edge devices with increased reliability and security, reduced latency and dramatic improvements in bandwidth. This will eventually help businesses transform the user experience for their customers and optimise processes across industries from retail to financial services, transportation to manufacturing, to healthcare and beyond.

Arvind Krishna, IBM

"Building on IBM's 20-year relationship with AT&T, today's agreement is another major step forward in delivering flexibility to AT&T Business so it can provide IBM and its customers with innovative services at a faster pace than ever before," said Arvind Krishna, the senior vice president for Cloud and Cognitive Software at IBM. "We are proud to collaborate with AT&T Business, provide the scale and performance of our global footprint of cloud data centres, and deliver a common environment on which they can build once and deploy in any one of the appropriate footprints to be faster and more agile."

Verizon lights the way for future smart grid technology with Peninsula Light Company

Verizon has been chosen to update Washington State's **Peninsula Light Company** (PenLight) power distribution system with Verizon's Grid Wide Utility Services Intelligent Energy platform. Electric meters equipped with Verizon cellular connectivity will replace end-of-life meters in the homes and businesses of over 33,000 PenLight members. The meters can then be managed using Verizon's Grid Wide platform.

Grid Wide is a managed, cloud-based, Internet of Things (IoT) platform-as-a-service solution developed by Verizon to help utilities modernise their systems. The solution allows utilities to remotely configure, monitor and manage end-points within their service areas, creating operational efficiencies and improving customer service across the board.

Members of PenLight – a member-owned electric cooperative serving the communities of Gig Harbor and the Key Peninsula in Washington – will benefit from improved meter reporting and billing accuracy and better power outage management, including improved outage identification, confirmation and response time.

"Utilities want to offer customers the benefits of IoT technologies, but can face costly infrastructure upgrades to do so," said Steve Szabo, head of Verizon's Global IoT products and solutions group, adding that, "Verizon's Grid Wide Platform-as-a-Service is a highly scalable and robust environment that combines a rich, world-class IoT application suite with the nation's largest, most reliable 4G LTE network. With near real-time data, Peninsula Light will gain the insights it needs to improve operational efficiency, control costs and offer an even higher level of service for its members."

NEWS IN BRIEF

Stone Technologies selects Sierra Wireless IoT solutions to expand into industrial monitoring

Stone Technologies, a supplier of intelligent monitoring solutions, has chosen IoT device-to-cloud solutions provider **Sierra Wireless**' Uplink remote monitoring solution and connectivity services to expand beyond its traditional alarm monitoring business to generate new revenue streams.

Art Stone, the chief executive of Stone Technologies, said, "Sierra Wireless' Uplink solution and connectivity services have allowed us to expand into new markets and open new revenue streams with a managed service for industrial monitoring. We're giving customers greater visibility over their remote equipment, whether they're in wastewater monitoring, tower lighting or emergency generator management. By partnering with Sierra Wireless, we were able to deliver a new service for our customers and increase our monitoring revenue by 32% from 2017 to 2018."

Dover Fueling Solutions and Microsoft collaborate to provide Azure-based edge

Dover Fueling Solutions (DFS), which delivers advanced fuel dispensing equipment, electronic systems and payment, fleet systems, automatic tank gauging and wetstock management, has announced a planned strategic partnership with **Microsoft** to bring new cloud and IoT solutions to market, utilising Microsoft Azure.

Through the alliance, Microsoft will help enable DFS' vision to deliver next generation retail site architecture and solutions that will digitally transform the fuelling experience for end customers, while delivering retail site operating efficiencies, enhanced consumer experiences and new revenue streams.

Microsoft and DFS will collaborate to develop, deploy, promote and support DFS Azure based solutions including the **Wayne** iSense Remote Monitoring and management solution. The iSense remote solution provides real-time updates of fuel dispenser and other support equipment at a retail fueling forecourt.

May and June 2019

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
Altair	ERM Advanced Telematics, Israel	Partnership agreed under which Altair optimised cellular IoT chipsets will be used to provide installation-free solutions for IoT, asset management and stolen vehicle recovery	5.19
ALPS Europe & Sigfox	DHL, global	Long-term partnership agreed to deploy tracking system for 250,000 DHL roll cages	6.19
Arqiva	UK Power Networks, UK	Deal to provide new broadband global area network (BGAN) M2M solution for electricity distributor's SCADA network	5.19
Ayla Networks	Hamilton Beach, USA	Ayla IoT Platform chosen by make of FlexBrew coffee machines to develop system for automatic re-ordering of coffee and brewing supplies	5.19
Bearing Point// Beyond	Tata Communications, global	Bearing Point selected to provide its Infonova Digital Business Platform to allow customers to manage and monitor how they use Tata MOVE IoT and enterprise mobility service	5.19
Comcast	Universal Parks, USA	Comcast MachineQ enterprise IoT service chosen to provide LPWAN technology for IoT projects at its Orlando, Florida park	6.19
Globalstar	PrismaQuality, Finland	Deal to provide satellite connectivity to provider of ReindeerApp and collar for tracking herds of reindeer in northern Finland and Sweden	5.19
Kerlink	Sensoterra, The Netherlands	Kerlink Low Power IoT Reference Design platform chosen for production of new class of soil moisture sensors	6.19
Navigil	City of Helsinki, Finland	Deal to provide Navigil smart wristwatches to approximately 200 customers suffering from memory loss diseases	6.19
SAS	Lockheed Martin, USA	Selection of SAS analytics to analyse streaming data from sensors on Hercules C-130 aircraft and enable predictive maintenance	5.19
SAS	Ulbrich Stainless Steel, USA	SAS analytics chosen by maker of engineered stainless steel products to ensure consistent high quality	5.19
Semtech	Birdz, France	Continuation of usage of Semtech LoRa devices and radio frequency technology for future smart meter deployments	6.19
Semtech	Istanbul Airport, Turkey	Semtech LoRa-based sensors deployed to track location, usage and condition of thousands of devices	6.19
Sierra Wireless	Stone Technologies, USA	Selection of sierra Wireless Uplink remote monitoring system to help expand business beyond traditional alarm monitoring	5.19
Telefónica	Schindler, global	Deal agreed to provide IoT connectivity for smart elevators and escalators worldwide	5.19
Traxens	CFL Multimodal, Europe and China	Selection of Traxens cargo tracking IoT system for rail freight wagons throughout European corridor and New Silk Road to China	5.19
Vodafone Business	Perch, UK	Digital displays and retail marketing specialist selects Vodafone Business to provide engaging digital experiences in stores via IoT services	6.19

Industry backs eSIMs but needs to learn the benefits of iSIM deployment, says Arm survey

The top three obstacles to large commercial embedded subscriber identity model (eSIM) deployments are resistance from traditional stakeholders (69%), complexity to deliver eSIMs (40%) and lock-in concerns (40%). These are among the key findings of a new survey by **Arm**, according to Vincent Korstanje, the company's vice president and general manager of Emerging Businesses.

The survey also showed that 90% of respondents are aware of eSIM, however education is needed to grow the industry's understanding of integrated SIM (iSIM), with 43% unaware of the technology. And only 44% of those surveyed believe iSIM is as secure as a traditional SIM.

As the IoT industry continues towards one trillion connected devices by 2023, one of the most critical steps towards enabling Internet of Things (IoT) connectivity is the evolution of the underlying SIM (subscriber identity module) technology. The evolution primarily involves embedded SIM (eSIM) and integrated SIM (iSIM) systems for authenticating users on existing and future 5G mobile networks.

A total of 67% view eSIM technology as a positive development and more than 80% agree it will overtake traditional SIMs. However, the industry still needs further education on the benefits that iSIM technology will deliver.

When asked about the main obstacles to large eSIM deployments, feedback from respondents already aware of eSIM was as follows:

- 69% of respondents cited resistance from traditional stakeholders
- 40% noted lock-in concerns
- 40% mentioned complexity to deliver

"This resistance may be linked to a desire to capitalise on existing solutions and investment, but Arm believes this resistance will diminish, particularly as **GSMA** and other standards bodies are playing an active role accelerating the evolution of SIM technologies," said Korstanje. "And based on my own conversations with decision-makers, I expect those resistance numbers will rapidly diminish as more of them experience the flexibility eSIM and iSIM offer across the entire connected device value chain."

Vincent Korstanje, Arm

"Acceptance will soon become more pervasive among traditional stakeholders unable to ignore the innovation, new business models and fresh opportunities enabled by eSIM and iSIM technologies as billions of IoT devices are deployed," he added. "An example thisis its recently announced partnership with **Vodafone** to combine iSIM, IoT software and network services with an aim to reduce complexity and enable standards-compliant remote provisioning of any IoT devices."

GSMA MWC19™ Los Angeles | IN PARTNERSHIP WITH ctia™

October 22-24 2019

WELCOME TO THE ERA OF

INTELLIGENT CONNECTIVITY

MWCLOSANGELES.COM

MWC Los Angeles 2019 is where tech industry influencers gather to explore Intelligent Connectivity – a combination of 5G, IoT, AI and Big Data – and how businesses can harness it to better compete and win.

Experience the first live 5G networks rolling out in North America, and see how Intelligent Connectivity can work for you.

#MWC19

GLOBAL PARTNER

MOBILE WORLD CAPITAL™ BARCELONA

IoT demands an open, modular and scalable platform to manage 80 billion IoT devices

Romil Bahl is the chief executive of KORE, the global, independent Internet of Things (IoT) solutions provider. He joined the company in 2017 to build on the company's seven million global connections, which have grown to 11 million in less than two years, and to drive its growth as IoT itself continues to mature. Here, he tells IoT Now how the recent launch of KORE One, the company's new IoT platform, brings together capabilities across seven modular engines that address next generation networks, security and enterprise and cloud applications

IoT Now: How do you see the overall landscape of IoT changing in the next five to ten years?

Romil Bahl: As the IoT marketplace matures, businesses across industries will continue to adopt IoT solutions to achieve digital transformation, an endeavour that is leading to billions of devices and sensors being connected to the internet over the coming decade. According to most analyst estimates, some 75-80 billion connected devices are expected by 2030, and that number is staggering – it will mean seven-to-eight connected devices per human being. In this era of digital transformation, companies will increasingly utilise real-time data and analytics to derive real-time insights from commercial and industrial assets and equipment to facilitate rapid improvements in business processes and core business applications. It is critical for organisations to understand that achieving transformative business performance with IoT means truly making use of the resulting data, rather than just talking about it. I believe that data will become the most valuable resource for connected businesses during the next five years, if not sooner.

IoT will not only deliver invaluable business intelligence, though, as it is expected that a growing number of original equipment manufacturers (OEMs) will bring new, IoT-enabled products, services and applications to market to achieve competitive differentiation and generate diversified revenue streams and business models. In fact, Gartner predicts that by 2023, 25% of commercial or industrial OEMs will offer IoT-connected products. These new offerings will be driven by advancements in IoT technologies such as embedded subscriber identity modules (eSIMs), which not only massively streamlines manufacturing and logistics processes for global or multinational deployments, it ▶

SPONSORED INTERVIEW

ensures affordable, local coverage for devices out of the box. eSIM technologies, with their power of futureproofing our customers' IoT investments, are expected to grow exponentially in terms of adoption over the next few years.

Underpinning the growth of IoT – regardless of the use case – will be advancements in security capabilities. In order for IoT to reach its full potential, organisations must be confident their connected solutions are protected, and in turn, IoT providers will need to step their game up to deliver advanced, innovative security solutions.

IoT Now: What is KORE doing to keep up with the changing requirements of the IoT world? What is your growth strategy for the future?

RB: KORE has transitioned from almost two decades of experience as an IoT network connectivity provider to a truly global, independent, IoT solutions provider. We understand that our customers need much more than connectivity to deploy, manage and scale their IoT implementations and as such we are continuously expanding our services portfolio to deliver comprehensive, integrated solutions to help businesses streamline their vendor ecosystems, accelerate speed-to-market and maximise returns on IoT investments.

Our aggressive growth strategy is focused on delivering innovative products and services related to our foundational offering of connectivity management - including eSIM and advanced connectivity, device management, and location-based services. Further, building on my previous statement regarding our transition to an IoT solutions provider, we are now delivering a variety of professional IoT services, IoT security, data-as-a-service and data analytics. Just one example of an entirely new service is our intelligent network monitoring service, SecurityPro, which helps customers effectively monitor device activity and protect IoT connections from potential threats.

All of that said, we are proud of our connectivity management heritage and we believe we understand the IoT ecosystem better than anyone else as the only truly global independent provider. Our 'multi-multi-multi' value proposition of multiple devices, multiple networks and technologies, in multiple regions of the world is the foundation of our future growth. After all, without fundamental connectivity services, there is no IoT.

IoT Now: What are the key enablers of this growth strategy?

RB: Our growth strategy revolves around three key pillars: (i) we continue to provide the best combination of connectivity management, device management and location based services as we have done for almost two decades, with a constant focus on advanced connectivity including leading with eSIM technology; (ii) helping our customers deploy ▶

KORE One is a true IoT platform comprised of seven modular technology engines that each play a unique role in facilitating the next generation of network services, security services, as well as enterprise and cloud applications

IoT applications with a host of services that simplify complexity and choices, and shorten time-to-market; (iii) an increasing focus on security and data management, including analytics and fraud protection.

Just as connectivity management remains the foundation of our three-pronged growth strategy, the foundation of our connectivity management service remains a world-class platform. Our new, state-of-the art IoT platform, dubbed KORE One, is being officially launched at MWC Americas after three successful phases of implementation, and several rounds of alpha and beta testing with some of our largest customers. KORE One enables the next generation of carrier, device and cloud-agnostic IoT deployments, delivering best-in-class technology, tools and services to allow innovation, business agility and speed-to-market for long-term IoT success. KORE One will be the platform from which KORE will build all new service and solution offerings, facilitating our leap into the future of IoT.

IoT Now: Tell us a little more about KORE One and its platform capabilities.

RB: KORE One is a true IoT platform comprised of seven modular technology engines that each play a unique role in facilitating the next generation of network services, security services, as well as enterprise and cloud applications. Engine functionalities include secure, universal data processing, integration and workflow capabilities to connect network providers to enterprise applications, as well as real-time billing and rating functionalities.

Through the integration of these unique engines, KORE One enables pre-provisioned connectivity for traditional SIMs, eSIMs and unlicensed spectrum options to provide total flexibility; powerful data management capabilities to harness all levels of sensor data, meta data and usage data; as well as seamless and robust application programme interface (API) integrations to improve response times, eliminate costly provisioning errors, and decrease total cost of ownership.

The microservices architecture of the KORE One platform also facilitates the individual deployment of each engine. For example, the aforementioned integration and workflow engine delivers a normalised and templatised interface to cellular carrier platforms, which is a key component for managing switchable eSIM profile provisioning and can be used in bring-your-own-carrier scenarios as a licensed software deployment. Another example would be using our network intelligence engine to understand device behaviour from network meta data.

We have already launched several innovative tools and services on the KORE One platform to improve our customer experience and enable customer success

Bottom line, we have built a platform that goes above and beyond just connectivity management. We have leap-frogged our competition with an entirely modular, API-first, IoT platform for connectivity management, security management, application enablement, and that is just what we are launching now. There is much more to come as we continue to add features, functions and services to make it easier for our customers to launch their IoT applications on our platform.

IoT Now: With the launch of KORE One, what benefits are you anticipating your customers will experience?

RB: Fundamentally, the modular foundation of KORE One has allowed us to pick modern, world-class technologies that are the best fit for the function each engine delivers. This gives our customers the advantage of knowing that they are working with the best technology platform in the world, picking and choosing the engines and services/APIs they need, knowing that we can add features and functions at will over time, without fear of technology obsolescence or scalability issues. On this foundation, we will continue to build features and services that will significantly differentiate KORE One from most all IoT platforms in the industry, especially as we now support well over 11 million connections globally and are learning ever more every day.

We have already launched several innovative tools and services on the KORE One platform to improve our customer experience and enable customer success. The first is ConnectivityPro, our next generation connectivity management service. Replacing our legacy connectivity management platform, ConnectivityPro provides a streamlined user interface with service-oriented APIs supporting full automation of connectivity management activities, including support for our eSIM offerings. Customers also benefit from fully-featured provisioning, diagnostics, reporting, support, and billing; proactive monitoring in real-time to events, usage and costs with rule-based actions and alerts; as well as integrated, a la carte microservices supporting solution components that be added based on unique business requirements.

As previously referenced, the second service we've built on the KORE One platform is SecurityPro, an intelligent network monitoring tool that allows customers to detect changes in network behavior that may indicate a security breach has occurred at the device level. For example, the service can be configured to notify a customer when one or more of their devices is communicating with an unauthorised IP address or is sending an anomalous increase in data traffic.

KORE One also lays the foundation for our data-as-a-service (DaaS) and analytics capabilities. KORE One enables storage and analysis of a variety of different data sets in the IoT arena. This not only includes payload data but also usage and meta-data associated with the device as observed through the network. This provides KORE with the unique ability to provide valuable analytics to our customers. As an example, this would include observing meta-data as a proxy to device behavior or network traffic patterns which could enable customers to act proactively in certain situations.

In summary, the future opportunities that KORE One will bring to our customers are nearly endless, as it provides an industry-leading architecture from which enterprises can build and deploy their own unique applications and services more quickly and efficiently, and at a fraction of the cost, should they had started from scratch.

IoT Now: What are some of the KORE One elements or functionalities that differentiate KORE in the marketplace?

RB: The differentiators of KORE One can essentially be summarised in three words: open, modular, and scalable. Open API access utilising fully documented external APIs supports agnostic application enablement and rapid delivery of new applications, providing unparalleled levels of flexibility with no need to ever modify source code. Modular, micro-services architecture enables a simplistic approach to creating new solutions and services through the rapid integration of desired services, accelerating time-to-market and ensuring evolution of best-in-class technologies. Scalable, auto-elastic capability provides for a future-proofed foundation to grow, manage, and meet increased demand.

IoT Now: How do you think the launch of KORE One will continue to position KORE as the leading, global independent IoT provider?

RB: We pride ourselves at KORE in being a trusted IoT advisor that is solely focused on customer results and enabling maximised returns on IoT investments. Our commitment to our customers' success has gotten us where we are today, and we are confident that the introduction of KORE One is the next evolution of this commitment as it further empowers organisations to simplify IoT complexities and streamline solution deployments, while ultimately providing a platform for innovation, growth and scalability.

www.korewireless.com

Don't get burnt by your IoT platform decisions

As IoT scales up growing pains are inevitable. George Malim asks what the industry needs from platform providers not to make technology operate well but to generate valuable insights and, ultimately, revenues

A platform can means many things including a springboard to new opportunities, a point from which a journey starts or a base to build upon. It can also be burning, as former **Nokia** chief executive Stephen Elop prophetically warned.

In IoT, the definition of a platform suffers from the wide spread of organisations that offer parts of a platform or a platform that addresses part of a use case. These are all valid and, as the industry's growth accelerates, it's important not to get bogged down in terminology and semantics. However, it is now clear that IoT platforms need be more than packages of technology. They need to help organisations manage the slew of data connected devices generate and help them extract value from that.

"The use of relevant and useful data is the ultimate value from IoT platform providers," says Darron Antill, the chief executive of **Device Authority**. "Being able to ensure the relevant data is secure end-to-end from the edge device and on its journey to an IoT platform or even further than its interactions with the platform such as people, organisations or other applications is of extreme importance. Automation will be key to the scale challenge, and frankly removing any human interference or error. Ensuring compliance is often the name of the game, and protecting your insights from your data assets and/or IP for many will be critical data."

For Wayne Stallwood, the head of AWS at **KCOM**, the scalability of an IoT platform is the entry level requirement. "The IoT industry needs seamless - or near-seamless - scalability from platform providers," he says. "A good example is the need to scale up for surge days. Events such as Christmas, Black Friday and Amazon Prime Day see a sudden peak in sales for IoT devices, followed by a peak in registrations. Their supporting platforms must be able to cope with the surge, allowing device manufacturers to preserve a positive customer experience for everyone, by avoiding failed registrations that could result in warranty returns or increased calls to support teams.

"On the other hand, it doesn't make economic sense for an IoT device manufacturer to build out capacity for unsold devices," he adds. "This means that utility-based computing, such as Cloud Native Serverless infrastructure provided by the likes of AWS, if properly architected, yield immediate scalability with the lowest financial risk. In this situation, the

platform provider only bills for utilised capacity, and the cost of the IoT platform remains proportional to the sales success of the IoT device."

The pay-as-you-grow model is well understood in IoT but cost isn't the only consideration. Monetisation enablement is of growing importance. Collecting the data and storing it is one step, turning it into value is the next.

Peter Ruffley, the chairman of **Zizo**, feels this is now the focus. "With the explosion in IoT sensors, companies across virtually every sector have been encouraged to collect and store vast quantities of data," he says. "And while some are effectively harnessing that data to improve business operations, there is a growing recognition that this data could have a broader value. Indeed, as companies scrabble to realise a return on the investment in IoT sensors and vast data storage resources, there is a growing push towards utilising these data resources by selling them to the highest bidder."

"But let's be realistic here – is there any actual value in that data set?" he warns. "Simply loading every piece of IoT sensor data into a vast cloud-based database and mashing it up is not enough: data without context inherently has no value. So where is the context? Where is the additional data source, or sources, that when combined unlock real insight?"

Ruffley gives the example of edge computing in relation to a refrigeration unit where sensors are increasingly used to avoid food wastage by continuously monitoring temperatures and taking action should a fault occur. Predictive analytics of historical performance data is used to identify potential points of failure, enabling remedial action. This performance data is also incredibly valuable to the refrigeration unit manufacturer, especially when combined with contextual information about different locations and operations. Manufacturers could also use this insight during the design process to improve efficiency and address problems within specific operational areas.

"Think laterally and the opportunities are incredibly exciting," adds Ruffley. "The whole is definitely greater than the sum of the parts when it comes to data – but achieving that requires a clearly defined business model and full understanding of issues, from ownership to security and data delivery. With the right approach, and by layering data sources over the IoT delivered insight, IoT can be truly monetised, and can become an incredibly compelling new value stream."

For Antill, it may not be the platforms that uncover this new value. "The platforms play their role, but many of the systems integrators and the IoT data managed applications or services will be key to managing this for clients," he says. "Some will be homegrown. Again, the key is only to consume securely the relevant data from the edge, not all of it. IoT software security platforms like KeyScaler from Device Authority can help solve the operational scale and security challenges for relevant data consumed with IoT applications platforms, as well data management services like Assetminder from **InVMA** and similarly from **DevicePilot** help customers collect, analyse and provide the insights needed from relevant data."

Others similarly see the need to be selective. "When it comes to storing data, the cloud offers huge scalability at a relatively cheap rate. However, it's only worth storing if there is long term value," says Stallwood. "Successful organisations are going to have to become ever more inventive in how they use the installed base of IoT devices and the data they collect without undermining data privacy."

"To enable long term success and financial sustainability, IoT device providers need an ongoing revenue stream," he adds. "This could be through service subscriptions, advertising, ongoing sales enablement or seeking value within the collected data – while remaining compliant with GDPR. The IoT solutions that achieve long term success will be the ones where the device provides mutual benefits to both the device owner and the platform operator."

A significant challenge for organisations is that they face substantial jeopardy if they back the wrong horse and select the wrong technologies and approaches when it comes to their IoT platforms, their costs and their performance. This risk of making the wrong choice has the potential to create paralysis among decision makers.

This can be avoided. "The key is to ensure you adopt a platform that can be integrated via application programme interfaces (APIs) or other open interfaces to ensure integration, flexibility and portability," explains Antill. "Many organisations will use and choose multiple platforms – and both cloud and an on-premise deployments have their place and purpose depending on the business model and use cases. In either case make sure the data is secure, and any devices or people that interact with the platform are authorised, regularly authenticated and secure, whereby ongoing lifecycle management of credentials and automation will be key. If you can't trust the device, you can't trust the data."

Undoubtedly it's hard to specify an IoT platform against the backdrop of continuously accelerating landscape but there are steps organisations can follow to minimise risk. "When using an IoT platform, continual improvement and development through an agile methodology significantly lowers risks," says Stallwood. "The IoT landscape is constantly developing, so platforms and device functionality must evolve at the same time to stay relevant and successful. Organisations should accept the fact that even the most optimal approach today may need to be revisited, improved or entirely rearchitected in the future and design in as much flexibility as possible from the outset."

Darron Antill, Device Authority

Peter Ruffley, Zizo

"The key is to ensure you adopt a platform that can be integrated via application programme interfaces (APIs) or other open interfaces to ensure integration, flexibility and portability"

The top five things to ask of a connectivity management system

IoT solutions are truly revolutionising our world and the way we operate on a daily basis. With every new development, improvement or function, IoT solutions have more opportunities to make an impact for end-users. And for every IoT solution – from personal healthcare devices to sustainable, smart living plant walls – you need a reliable, agile system to easily manage your connected devices

This need for reliability, ability and ease of management is why so many companies are looking to implement a single hub to manage their global network connections. The ability to monitor and adjust rate plans and connections across multiple carriers for all of your devices, worldwide, is no longer a nice to have – it's a requirement. That's why it's crucial to engage with a trusted IoT partner that provides a single, seamless connectivity management system as a part of their IoT solution bundles. When evaluating which partner has the right platform for your IoT solutions, here are some questions to ask:

1. Is it user-friendly?
One of the first things you need to consider is how easy the connectivity management tool or platform is to use – if it's difficult to use, it's going to be difficult to operate and optimise your IoT solution. A successful connectivity management system should have a clean, user-friendly design that makes monitoring and managing your connectivity simple. The goal should be to help automate many of your daily connectivity processes so that your team of experts can continue to innovate and grow your business. But good intentions and goals are useless if the system isn't easy to use. In your evaluations, make sure your team attends demos or walkthroughs or has the ability to physically test the different functionalities you'll need and that it performs as advertised.

2. Can it adapt to my changing needs?
Simply put, your IoT solution can – and should – evolve over time. As new capabilities become possible, you'll include more functionality as part of your solution. Your connectivity management system needs to be agile enough to support adding and removing services as your solution needs change. Look for a connectivity management system that's built on modular architecture, allowing you to add new services to your system quickly. This will also impact the speed with which you can get your solutions to market as well as the overall scalability of your offering. You need to find a platform and provider that can grow and change as quickly and easily as your solution.

3. Is it flexible?
This question goes hand-in-hand with adaptability. Not only do you need to consider the future of your solution, but also the current state of your environment. A holistic connectivity management system needs to seamlessly integrate with the various technologies in your own infrastructure. To adequately assess this, you need to first audit your existing set-up. Then ▶

you can begin looking for a system that functions seamlessly with yours. An open application programme interface (API), allows all your various systems to communicate with each other – if there's no flexibility, there's no reason to implement a solution. Look for a system that supports agnostic application enablement and makes it easy to integrate your technologies rapidly – without the need to modify source codes on either end.

4. How many networks does it integrate with?
Possibly the biggest benefit of a centralised, single connectivity hub is the ability to provision multiple network carriers depending on your regional or global deployment needs. A connectivity management system is only valuable if it integrates with a wide network of carriers in the areas you need coverage. It's important to ask for not only the provider's current carrier partnerships but also their future plans.

If you're investing in a connectivity management platform, you want to make sure that your partner's future vision aligns with yours – sparing you the challenge of moving to a new platform after you've outgrown your current one. The benefit of choosing a provider with a large number of geographically diverse carrier partnerships is that, no matter where you decide to take your IoT solution in the future, you're more likely to have exceptional coverage.

5. Does it support emerging technologies?
Technology changes – rapidly. In the past ten years, alone, IoT has exploded in both popularity and capabilities. So it makes sense that you'd need to look for a platform and a partner that is forward-thinking and innovative in the technologies it supports. Take eSIM, for example – you may or may not have a need for this technology currently, but the ability to remotely provision carrier profiles to your devices, whether they're deployed in various global destinations or they're mobile and need to seamlessly switch from network to network, affords you an immense amount of flexibility as you innovate and iterate on your IoT solution. Finding a connectivity management platform that supports emerging technologies and working with an IoT enablement partner that stays ahead of these trends is crucial to the future success of your solution.

Using these questions to guide you as you search for a connectivity management portal or system will allow you to ensure the right fit for your business needs. Ultimately, a connectivity management system is only valuable if it can help simplify your daily IoT solution deployment needs. From a high-level overview of your device and connectivity health, security and statuses to arming your team with the future-proofed technologies you need, the right system should free up your team and allow them to focus on innovative new ways to use your IoT solution and maximise your return on IoT investment. ■

Possibly the biggest benefit of a centralised, single connectivity hub is the ability to provision multiple network carriers depending on your regional or global deployment needs

That was the goal and these were the questions the KORE team asked of itself as the organisation laid the strategy for its new connectivity management service. KORE is thrilled to officially launch ConnectivityPro, powered by the KORE One IoT platform, which is a revolutionary way for customers to manage every aspect of their network connectivity. The modular, flexible, scalable platform architecture of KORE One enables the robust functionality of ConnectivityPro, empowering customers with a central hub to easily monitor and manage the health and usage of their various connections while providing best-in-class intelligent network monitoring and security tools. To learn more about ConnectivityPro and other services supported by KORE One, please visit:
www.korewireless.com/KOREOne

Welcome to the era of intelligent connectivity

MWC19 Los Angeles will be held on 22-24 October 2019 at the Los Angeles Convention Center in California, USA. The organisers, GSMA have taken the theme of Intelligent Connectivity, detailing that now is the time in which speed, convenience, and intelligence converge; inspiring new technologies that keep us connected to everything and everyone, while delivering highly contextualised and personalised experiences, when and where you want them. Here, IoT Now previews the event

5G deployments in North America are empowering advances in IoT, artificial intelligence (AI), immersive content and disruptive innovation. MWC Los Angeles 2019 will bring tech industry influencers together to explore this transformation and discover how they can harness it to impact their success.

"This year's MWC Los Angeles event is bringing together the greatest minds and companies to showcase the transformation the mobile industry is undergoing," said John Hoffman, the chief executive of **GSMA**. "In the era of intelligent connectivity, 5G is powering AI, IoT and data to reach new heights in never before imagined ways. By 2025, there will be 5.8 billion unique mobile subscribers and over 25 billion IoT connections. MWC19 will examine the possibilities in this new frontier – you won't want to miss it."

Over the four days in Los Angeles, we expect to see big name exhibitors, partners, enthusiastic sponsors and press.

The mayor of Los Angeles, Eric Garcetti, added: "Technology can serve as the great equaliser of opportunity for people everywhere - a vehicle to enhance education, deepen ties of commerce and culture, and improve the quality of life for young people and families around the world. Los Angeles decided to become a smart city, lead the way in 5G adoption, and host MWC19 for a clear reason: we know the power of innovation to level the playing field for our workers and forge solutions to our most pressing social, political and economic challenges."

Keynote speakers announced

GSMA has announced several new keynote speakers, with executives representing a wide range of organisations across the technology and telecommunications industries, including:

- Ajit Pai, chairman, United States **Federal Communications Commission** (FCC)
- Asha Keddy, corporate vice president and general manager, Next Generation and Standards, 5G, **Intel**
- Ricky Corker, president of Customer Operations, Americas, **Nokia**
- Joseph Essas, chief technology officer, **OpenTable**
- Stéphane Richard, chairman and CEO, **Orange Group** and chairman, **GSMA**
- Amy Emmerich, president North America and chief content officer, **Refinery29**

These executives join previously announced keynote speakers from leading companies

including **CTIA**, **Ericsson**, GSMA, **U.S. Cellular**, **Verizon** and **Viacom**.

4YFN start-up programme details unveiled

The 4YFN (Four Years from Now) start-up programme will attract more than 200 investors and 150 start-ups to MWC19 Los Angeles. Two pitching competitions will run on the 4YFN Discovery Stage in the LACC, organised by 4YFN sponsor **Indiegogo** and 4YFN partner **TrepCamp**.

SPROCKIT, a global startup community, has signed up as the first 4YFN theme sponsor and will curate media and entertainment content onstage illustrating the impact of mobile on the entertainment industry. For more information on 4YFN, visit: **https://www.4yfn.com/los-angeles/**.

GSMA Innovation City

The GSMA Innovation City will return to MWC19 Los Angeles inviting visitors to experience how intelligent connectivity, the fusion of 5G, AI, IoT and data, is positively impacting society and helping to create a better future for businesses and citizens alike. This year, joining lead partners **LivePerson** and **Mastercard**, there will be more than 25 interactive demonstrations across various categories including entertainment, industry, transportation, public services and the environment. Innovation City will be in booth #1750 in the South Hall. For more information on Innovation City, visit: **https://www.mwclosangeles.com/exhibitor/gsma-innovation-city/.**

www.mwclosangeles.com

Photos: Scott Chernis Photography

Be a part of MWC20

With this year's event only a few weeks away, attention is turning to the MWC20 Los Angeles event and GSMA has released some advance information. Mobile connectivity is transforming the planet and shedding light on future innovations that will change how we think about technology. The event brings together the latest trends from leading companies in the tech industry, with a highly-rated conference programme assembling today's visionaries to explore the hottest topics influencing the industry.

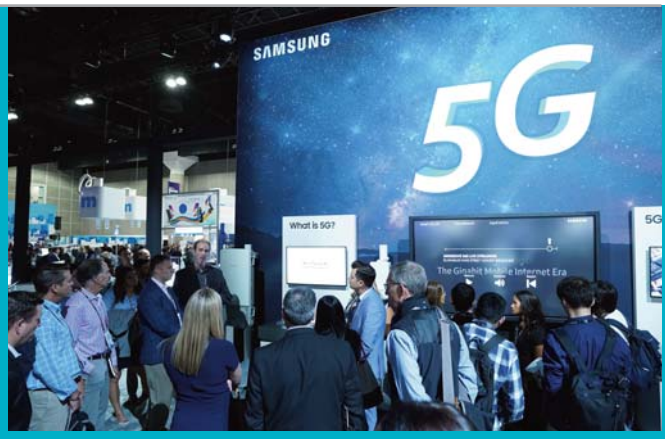
MWC20 Los Angeles is set to feature extensive learning opportunities from dozens of partner-led programmes, GSMA summits and more. Everything you need to know about the industry, today and beyond, can be found here. With important key decision-makers expected to attend, MWC20 promises to expand your professional network and help you achieve your goals.

Over the four days in Los Angeles, we expect to see big name exhibitors, partners, enthusiastic sponsors and press.

MWC20 Los Angeles will provide a glimpse into the future of mobile. Get involved and gain valuable insights from some of the most prominent leaders in the industry from various platforms:

Conference will feature presentations from tech's most influential executives, who will share their visions of the industry while providing essential insights on current and future trends.

Conference sessions are available to Gold and VIP pass



holders. For more details, view the full conference agenda online. As you look through the sessions, you will notice icons representing event themes, these will help you sort through what is most relevant to you.

Women4Tech features three days of in-depth analysis of topics shaping gender diversity. Open to all registered attendees, this programme aims to strengthen the overall mobile ecosystem through increased gender equality. In 2020, you can join the Women4Tech Summit, Speed Coaching session, Equality Tour and more.

4YFN enables start-ups, investors, corporations and public institutions to discover, create and launch new ventures together. The 4YFN Start-up Event will include workshops, networking opportunities, and speaker programmes and more. The 4YFN Los Angeles Awards applications are now open for online entry.

Cities made of dreams, how smart can enable sustainable

Smart City Expo World Congress returns to the Fira Gran Via venue in Barcelona, Spain on 19-21 November 2019 and is set to welcome more than 25,000 visitors and over 1,000 exhibitors. Since the first event, smart cities have come a long way, the organisers say in this preview of the event

Someone once said that "the future belongs to those who believe in the beauty of their dreams." When Smart City Expo World Congress started back in 2011, it did so with a clear dream in our minds: To make the world a better place for everyone. Almost a decade ago, we started with a vision, wondering whether smart initiatives could make sustainable cities flourish. Not because it was a nice thing to do, but because many indicators such as the increasing environmental footprint, growing urban population and resource consumption forecasts indicated that it would be the best and maybe the only opportunity to tackle such critical challenges. Smart cities appeared to be a vital tool here.

We now know that roughly two-thirds of the global population will be living in urban areas by 2050. From an environmental standpoint, the special report on global warming, issued by UN-IPCC warned us that we needed to act fast. We only have a dozen years to limit global warming to 1.5ºC and cut risk of extreme heat, drought, floods and poverty.

We have come a long way since 2011 and the smart city opportunity has turned into reality. Cities and companies are moving from small proof-of-concept projects to smart implementation at scale. New governance models and new approaches to equity and a circular economy have also emerged along with IoT, artificial intelligence (AI), drones, self-driving cars and new forms of micromobility. New ways of processing and distributing information such as blockchain and IOTA distributed ledger technologies have also come into the picture.

Cities have become socio-economic and political actors on both national and global stages and have a major impact on the development of nations. Yet we need to keep on exploring new paths, reinventing places and scenarios, drawing new cartographies of imagination, as we still have the opportunity to make things happen just the way we need them to be. And if we want to reach that destination a key element of this equation is and will be mobility.

Cities around the world face many obstacles but if there is one that is clearly shared across the globe is how to enable the inhabitants of large metropolises to move within their cities and also connect to other ones. That is the main reason why, since 2017, we have also hosted the parallel event Smart Mobility Congress. This 2019 event will welcome international experts such as Janette Sadik-Khan, the former NYC Commissioner of Transportation and Laura Tenenbaum, **NASA**'s scientific communicator, as well as leading companies from all over the world. These will come together to reveal the latest innovations addressing the biggest challenges that cities face today: digital disruption, sustainability, clean and efficient mobility, open governance, and inclusive and collaborative solutions. Industry leaders, policy makers, entrepreneurs and academia from around the globe will shape together an all-round approach that will help us find answers and pave the way towards the cities we dreamt.

www.smartcityexpo.com

SPONSORED PREVIEW

SMARTCITY
EXPO WORLD CONGRESS

Fira Barcelona

19 - 21 NOVEMBER 2019
BARCELONA

www.smartcityexpo.com
#SCEWC19

CITIES MADE OF DREAMS

#theEventforCities