

NO. 4 – NOVEMBER 2017



THE FOURTH INDUSTRIAL REVOLUTION
HAS CONNECTIVITY AT THE CORE **P.5**

VIRTUAL REALITY RETURNS
TO INDUSTRY **P.18**

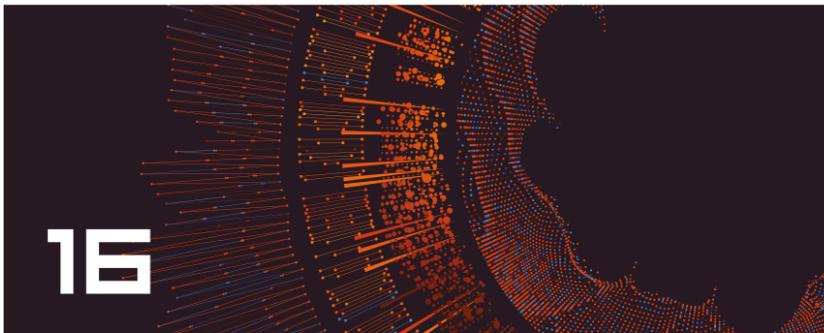


THE CONNECTED INDUSTRY





8



16



20



28

CONTENT

The Connected Industry

- 3** Foreword
- 4** The fourth industrial revolution has connectivity at the core
- 8** The three keys of the IIoT: timing, location, and communication
- 12** From farms to factories, artificial intelligence is coming of age
- 16** Engineering the IIoT mechanics of Industry 4.0
- 18** Virtual reality returns to industry
- 20** The demise of the dial

Markets

- 24** A global push
- 26** IIoT as an engine of growth in Taiwan

Expert Opinion

- 28** Towards a secure connected industry
- 34** Infographic: Network-connected industrial devices
- 36** Research summary

Products

- 38** Eyes in the container
- 42** u-blox connects the industries

Inside u-blox

- 44** Teams without borders

FOREWORD



THE FUTURE OF INDUSTRY

Dear Readers,

We are delighted to present to you already our fourth edition of the u-blox magazine, with a focus on the Industrial Internet of Things (IIoT) and how the Internet is drastically reshaping a multi-faceted industry, and its workforces.

Accenture estimates that the IIoT could add US\$14.2 trillion to the global economy by 2030. This is no wonder when we note that the wealth of connected industrial applications ranges from manufacturing, processing, instrumentation, energy management and survey monitoring to asset tracking, condition monitoring, remote control, and monitoring systems.

We are in the midst of a fourth industrial revolution, where sensors wirelessly send data over the Internet to machines or people where they are analyzed to automate processes and enable productivity gains and better products. At the core of this revolution is connectivity. With its wireless and positioning technologies, u-blox enables the underlying nervous system of this newly connected industry with more efficient and streamlined

resource management as well as increased economic and sustainable efficiency. In this context, security is very key. This is why u-blox has implemented its five security pillars: Secure Boot, Secure FOTA (firmware over the air), Secure Physical Interfaces and APIs, Secure Physical Transport Layer(s), and Robustness (spoofing and jamming detection).

So what will the connected industry of the future look like? With increasingly sophisticated technologies adding to our wireless and positioning technologies, such as artificial intelligence (AI), virtual and augmented reality (VR and AR) and new human-machine interfaces (HMIs), I believe we can only look forward to it and that it can ultimately only enhance the quality of our lives.

We wish you informative and smart reading.

Yours sincerely,


Thomas Seiler, CEO

IMPRINT
u – The u-blox technology magazine
Published by: Thomas Seiler
Chief Editor: Sven Etzold
Senior Editor: Natacha Seitz
Concept and Design: Identica AG, identica.ch
© by u-blox AG 2017
Circulation: 15'000, bi-annual
Reader-Service: magazine@u-blox.com

Contributors: Michael Ammann, Mats Andersson, Christina Bjorkander, Sabrina Bochen, Adrian Bridgewater (Technology Journalist), Rod Bryant, Ming Chiang, Robin Duke-Woolley (Beecham Research Ltd.), Klaus Erlinghagen, Peter Fuchs, Edoardo Guiotto, Paul Gough, Dylan Huang, Reza Kashani (Compology), Jessie Liao, Max Mazzawi, Jan Overney, Karin Steinhauser, Adrian Tan

Printed on: cover 300 g/m² Supersilk offset, polished super white
content 120 g/m² Supersilk offset, polished super white

THE FOURTH INDUSTRIAL REVOLUTION HAS CONNECTIVITY AT THE CORE

Forget business as usual: the Industrial Internet of Things is already disrupting how companies operate.

Thomas Newcomen, an ironmonger from Dartmouth on the south coast of England, installed his first working steam engine in a coalmine in 1712, where it was used to pump water out of the mine. It was a revelation, enabling mine operators to replace manual pumps, or the use of horses. By 1729, when Newcomen died, at least 100 of these expensive machines were in use around Europe. It was perhaps the first indication that a revolution was about to take place: an industrial revolution that would touch millions of lives and transform economies across the globe. Machines began to replace or enhance the work of people, delivering productivity gains in agriculture and manufacturing. Men, women, and children moved from rural farming to start working in factories, and mass production took hold. Communication began to play its part too. The first telegraph message was sent in 1844 and Alexander Graham Bell was awarded his patent for the telephone in 1876. Both these inventions provided virtually instant communications between physically separate locations.

The second industrial revolution took hold from 1908, when Henry Ford launched the Model T and demonstrated how manufacturing lines could deliver increased benefits and better product quality.

The third revolution started in the 1940s, with the advent of machine numerical control (NC), followed by computer numerical control (CNC) and the emergence of the first programming languages in the late 1950s.

Today, we're witnessing the fourth industrial revolution. The Industrial Internet of Things, or IIoT, is part of the wider Internet of Things (IoT) phenomenon, and embraces all aspects of the connected industry, including manufacturing operations, maintenance and services. In terms of commercial opportunity, McKinsey predicts¹ that IIoT will account for the largest proportion of the 'things' that will be connected to the Internet by 2025. Industrial installations will eclipse areas such as smart homes, smart cities, and health and fitness applications.

¹ The Internet of Things: mapping the value beyond the hype, McKinsey Global Institute, June 2015.

The IIoT will transform asset tracking from the container-ship to the warehouse.

IloT, Industry 4.0, and M2M communications

At this point, it's worth understanding some key terms. Industry 4.0 – or rather INDUSTRIE 4.0 – is a phrase often used interchangeably with IloT. However, it's actually a specific initiative launched by the German government, concerned exclusively with connected manufacturing. It's therefore just one (albeit very important) aspect of the IloT.

IloT is sometimes viewed as an extension of machine-to-machine (M2M) communications. However, IloT is broader than that. IloT delivers cost reduction and efficiency gains throughout the supply chain, using remote asset and network monitoring, real-time asset tracking, and remote diagnostics to enable predictive maintenance and minimize downtime. Accenture estimates that the IloT could add US\$14.2 trillion to the global economy by 2030².

How the IloT works

An IloT system uses sensors to detect what's happening in an environment. It then processes the data it receives from the sensors, analyzes it, and sends the resulting information over the Internet to machines or people. The processing and

analysis can be done close to the sensors (which are described as being at the 'edge' of the system, or 'edge computing'), in remote cloud computers, somewhere in between, or in all these places. Machines or people then decide if and how to respond.

Making the IloT work

Several technology advances are coming together to make the IloT viable. The cost of sensors, microprocessors, and microcontrollers has fallen to levels that make it feasible to deploy hundreds of thousands of these devices within systems. Processor performance and software advances have led to significant progress in implementing artificial intelligence (AI).

AI is about more than raw number-crunching – it's about programming computers to mimic the way our brains work when detecting and responding to external stimuli. Humans are much better at processing and reacting to streams of information from our surroundings. Neuromorphic computing, which seeks to emulate the workings of neurons and synapses in our brains, has made great progress in recent years, further enhancing the capabilities of AI in IloT systems.

Then there's progress in connectivity, without which the IoT could not exist. The sheer scale of the IoT phenomenon means it's impractical to connect devices using wires. What's more, many devices will be mobile or portable, and many of them powered by batteries or energy-harvesting. This means efficient and effective wireless connectivity will be key. Bluetooth, Wi-Fi, and cellular radio technologies account for the vast ma-

“AI IS ABOUT PROGRAMMING COMPUTERS TO MIMIC THE WAY OUR BRAINS WORK.”

majority of connections today, while a host of other specialist wireless protocols are used in niche applications.

As well as connectivity, many IloT applications rely on positioning and timing technology that enables the operator to see where an asset is (and where it's been). Standard-precision Global Navigation Satellite Systems (GNSS) are widely available and are now being complemented by high-precision location and timing capabilities and dead reckoning technology, the latter enabling precise location sensing even in places where satellite signals can't reach.

IloT is here already, but there's much more to come. Just 35% of manufacturers are using smart sensors today³, according to PwC. However, companies are embracing the concept that distributed networks of ultra-connected, intelligent machines will transform industry for the better. And, unlike previous industrial revolutions, it's not only productivity and quality that will be improved. IloT will also enable companies to create more personalized products, whether they're cars, clothes, or anything else. And it will mean that companies will

² Winning with the Industrial Internet of Things, How to accelerate the journey to productivity and growth, Accenture, 2015.



An engineer takes measurements inside the metal body of a Russian GLONASS positioning satellite at the Applied Mechanics Institute in Zheleznogorsk, Russia.

be able to bring new products to market faster to gain competitive advantage.

A few examples of the IloT in action

Irish utility Bord Gáis Energy has installed GE's Asset Performance Management software for predictive maintenance and to minimize power outages at its 445 MW power plant in Whitegate, Ireland. Sensors throughout the facility feed data to a cloud platform that carries out over 300 analyses to detect when components could be about to fail. The reduction in outages is estimated to have saved the company over US\$1 million in the first year, while another US\$1 million of potential savings has been identified.

Heating, ventilation, and air conditioning (HVAC) systems are also being transformed by IoT connectivity. In developed countries, buildings can account for as much as 40% of energy consumption⁴. By connecting HVAC installations to the Internet, smart sensors continuously monitor conditions and feed data to energy management systems, which facilitate real-time monitoring and control. The aim is, of course, to cut energy use. The world's largest HVAC company, Japan's Daikin Applied, makes extensive use of Intel's systems and end-to-end analytics to connect its Rebel rooftop systems to the cloud. Here, data is aggregated, filtered, and shared, resulting in 43% energy savings compared to the level required by the

main US industry standard for building efficiency (ASHRAE 90.1). These energy savings translate into environmental benefits too, thanks to reductions in carbon dioxide emissions.

German-based Bosch Rexroth makes hydraulic valves for mobile machinery, and has reduced costs by €500k per year by introducing Industry 4.0 practices into its manufacturing⁵. It uses 2,000 different parts to make around 250 variants of its products, and the number of small-batch runs means production has to be flexible. The production line was redesigned to create individual workstations equipped with RFID chips. These enable Bosch Rexroth to collect data and act on it. An interactive manufacturing system then continually analyzes data, presenting operators and management with real-time information that enables them to make informed choices. Within a year of implementing the new system, set-up time was eradicated, inventory requirements fell by 30%, and productivity increased by 10%.

Emerging IloT revenue models

Whenever data is generated, there are opportunities for new revenue models that

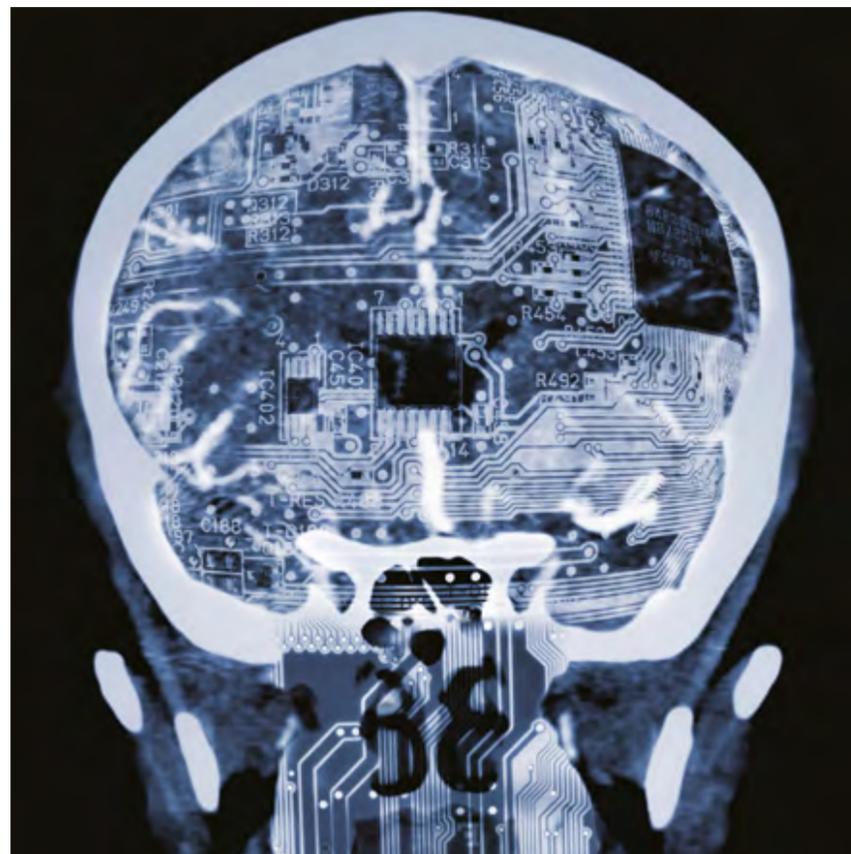
monetize the data. The sheer volume of data produced in some IloT applications will demand sophisticated analysis and presentation of results in a format people can understand easily. It will also require robust, reliable, and secure wireless data distribution, and dependable timing and positioning information. Software as a Service (SaaS) revenue models with industry-specific tools and processes may see significant growth within the IloT. What's more, the ability to monitor the usage of machines and other business assets, such as vehicles, will simplify the introduction of usage-based pricing, enabling manufacturers to reduce capital investment and up-front risk. Ultimately, this may even enable new businesses to emerge by removing capital investment barriers.

It is worth adding that current value chains are gradually becoming fragmented by all these new technologies. We might therefore see a horizontalization of industry and business, with for instance companies that would focus on data storage and analytics only. Such a shift might challenge businesses that are reluctant to innovate and develop new technologies. ●

³ The Internet of Things: what it means for US manufacturing, PwC, 2017.

⁴ A review on buildings energy consumption information, ScienceDirect, Elsevier, 2008.

⁵ Industry 4.0 in action, whitepaper by Dr Matthias Möller, technology and process planning director at Bosch Rexroth's Homburg plant, March 2017.



Neuromorphic computing seeks to emulate the way our brains process information.

THE THREE KEYS OF THE IIOT: TIMING, LOCATION, AND COMMUNICATION

With its portfolio of leading timing, location, and communication solutions, u-blox is uniquely positioned to power the Industrial Internet of Things.

A revolution is just beginning in the industrial world. It is a revolution that will rival the mass mechanization and the production-line innovations of the three previous industrial revolutions, though it may be harder to see – the changes will come through the increased flexibility made possible by real-time communications and local computing capability.

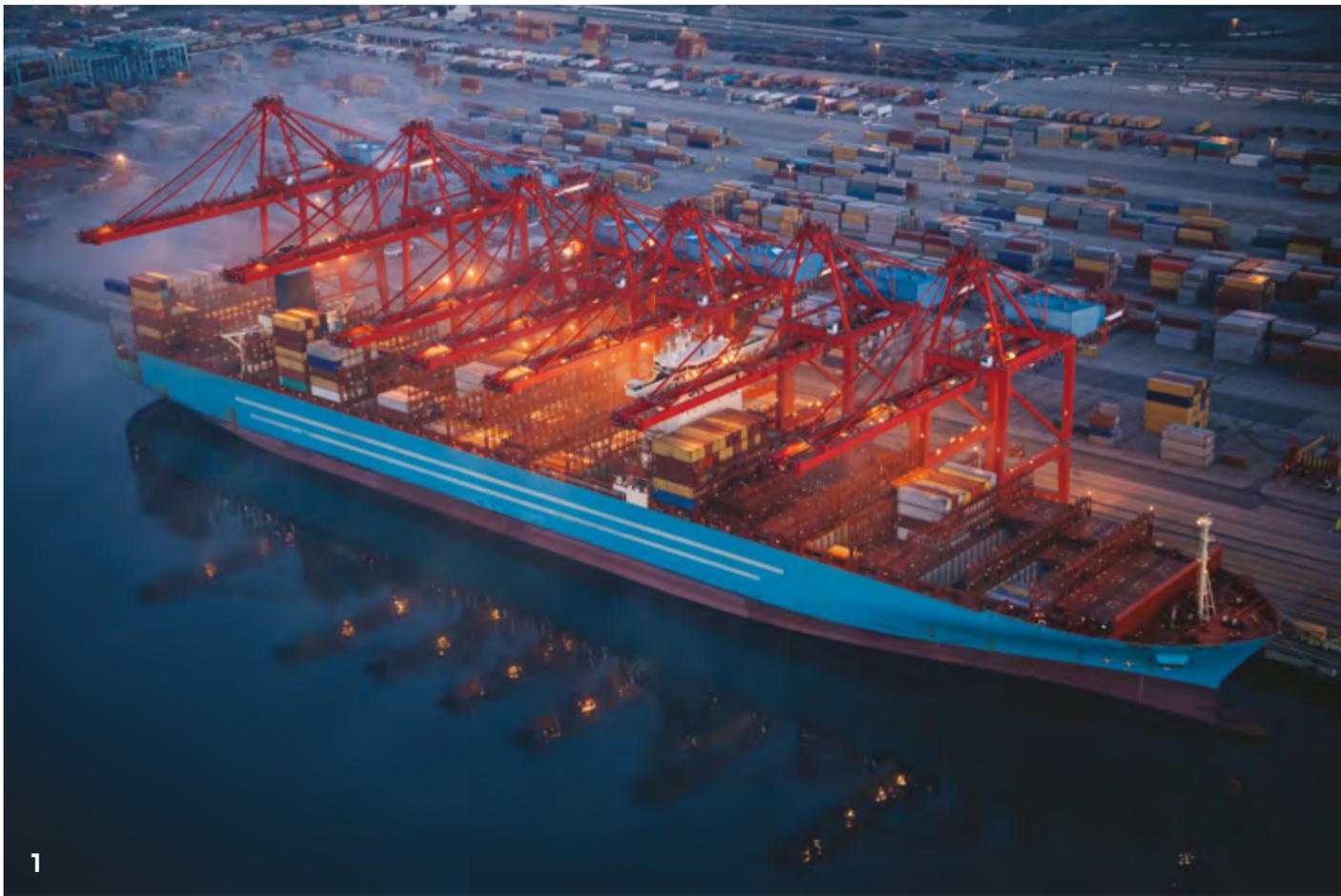
At the core of the Industrial Internet of Things (IIoT) is a network of uniquely identifiable devices, each producing and consuming data streams that are part of a highly cooperative and distributed processing environment. Through real-time data flows, operators and manufacturers can optimize their systems with the ability to control assets, processes, and supply chains at a much finer level of granularity than has been possible to date.

Sensor data from a manufacturing or utility grid can be aggregated at multiple locations, enabling

intelligent decisions that improve the efficiency of industrial processes. With more accurate sensor data, a control room can make smarter decisions about when elements of the system should be idle or asleep. Other systems can monitor the flow of goods to ensure efficient supply and demand planning. In a network of wind turbines, the sensor data may indicate looming problems with the machinery that call for maintenance before there is an outage. In logistics, fleets of vehicles can report their position and status in real time to give accurate information on when deliveries will take place.

There are a number of key technologies that are needed to make the IIoT work. Local computing capability is a given. But in order to make that computing capability effective, systems need to be able to transmit accurate real-time data on their status, location, and operations. Location, time, and communications are all essential components for the IIoT.

High precision clocks in cell towers keep mobile networks synchronized.



1

u-blox offers a complete portfolio of components that provide IIoT systems with the ability to communicate and determine time and position, using the most appropriate technology for the application. This enables control over the entire IIoT architecture.

Wireless communication technologies for the IIoT: short range radio and cellular

For communications, IIoT integrators are faced with a huge range of choices, especially for short range applications where the range to the sensor node is 100 meters or less. Wi-Fi and Bluetooth wireless technologies are widely implemented in industrial and consumer devices.

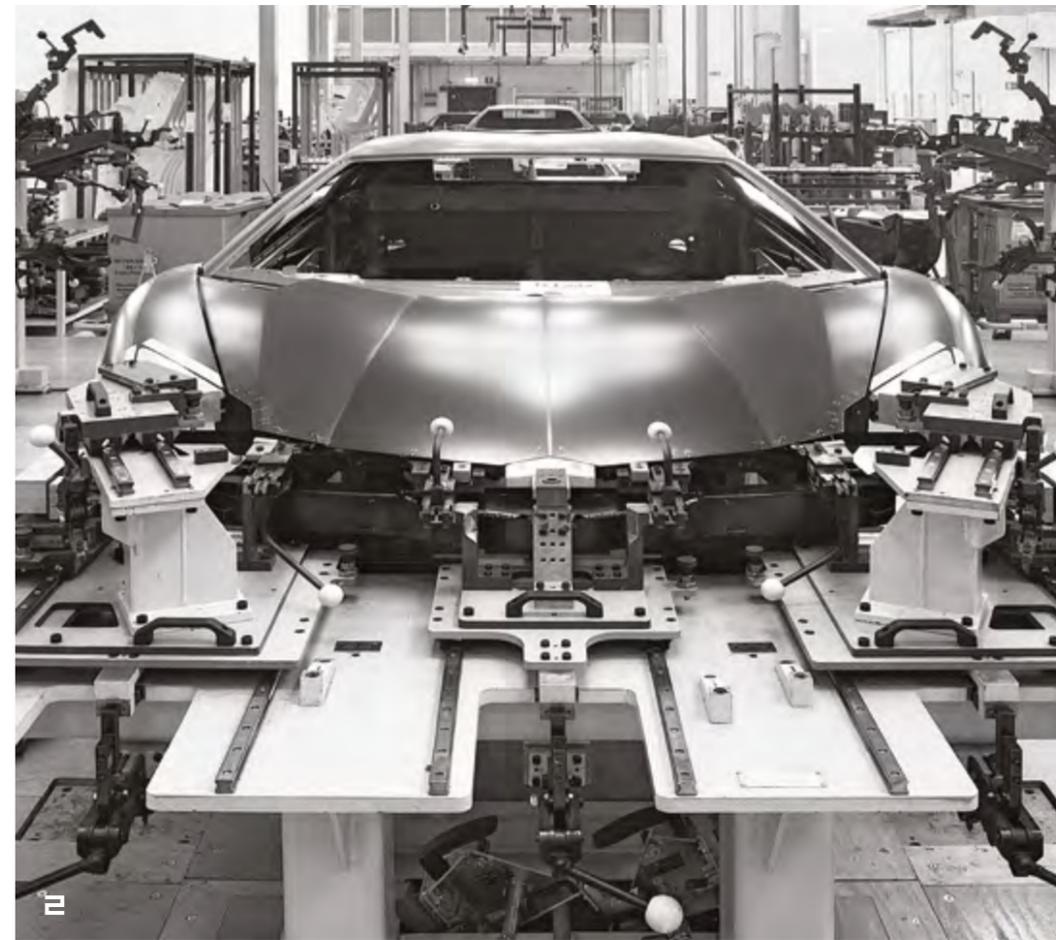
Wi-Fi continues to be an important technology for short range applications that need connectivity to the LAN infrastructure and high data rates. For applications that focus on security, u-blox has launched the compact NINA-W1 module series. Already established on the market is the ODIN-W2 series, which is the most versatile industrial IoT gateway module series on the market. The stand-alone modules feature Wi-Fi and Bluetooth and are ATEX and IECEx certified for use in explosive atmospheres.

Bluetooth is currently available in two variants: BR/EDR (basic rate/enhanced data rate) for audio and streaming applications, and Bluetooth low energy (BLE) for intermittent transmission of data in battery operated sensor devices. The latest revision of the Blue-

tooth Specification, Bluetooth 5, increases the range and speed of Bluetooth low energy and is featured in the new u-blox NINA-B3. With mesh networking, Bluetooth low energy nodes can form large-scale networks with extended reach. The NINA-B1 series of stand-alone Bluetooth low energy modules with NFC are advanced Bluetooth low energy modules that target industrial markets.

For longer range applications beyond the factory floor or warehouse, wide-area networks such as cellular come into play. Most recently, the options available to IIoT integrators have expanded through the wider availability of networks based on new cellular standards, such as LTE Cat M1 and Narrowband IoT (NB-IoT), also called Cat NB1. Both Cat M1 and NB-IoT are considered to be low-power wider-area (LPWA) technologies with deep in-building range that are ideal for IIoT applications. The u-blox SARA-N2 NB-IoT module and SARA-R4 multi-mode NB-IoT/Cat M1 module are able to support a large number of low-energy sensor nodes. SARA-R4 is also available on a single global hardware, making it the ideal candidate for large-scale, multi-regional implementations.

Cellular is not the only wide area option. RPMA® (Random Phase Multiple Access), an LPWA technology for the Machine Network™, is supported by u-blox modules such as the SARA-S2 and is ideal for systems that transmit small amounts of data infrequently, such as environmental sensors.



2

1
The RF signals from the orbiting satellites do not readily penetrate walls or containers used for transport.

2
With mesh networking, Bluetooth low energy nodes can form large-scale networks with extended reach on the factory floor.

Positioning technologies for the IIoT

Positioning technologies such as Global Navigation Satellite System (GNSS) provide the means to locate IIoT devices, while also providing accurate timestamps for data-to-server applications that synchronize activities. The ability to determine location automatically is important in many industrial activities, even for equipment that is designed to be fixed or stored in one place. By providing the device with its own positioning technology through small sized and low power modules such as the ZOE-M8 and EVA-M8, there is little need for high technical knowledge or additional components to program in the location by hand. And if a node goes missing or is moved without authorization, the gateways and servers will detect the problem.

However, GNSS signals may not always be available to the node. The RF signals from the orbiting satellites are weak, easily jammed, and do not readily penetrate walls or containers used for transport. This is why u-blox provides a number of technologies to augment GNSS data. An example is the CellLocate® technology in the SARA-G3, LISA-U2, and SARA-U2 cellular modules offering hybrid positioning. This technology uses data from cellular base stations to help determine the accurate location of the module.

Inside factories and warehouses, Bluetooth and Wi-Fi communications provide another means to improve the accuracy of

location data. Software running on the processors in communications modules can analyze Bluetooth signals such as angle of arrival (AoA) and angle of departure (AoD) to help determine position relative to other nodes or beacons. Time of flight analysis and fingerprinting of networks is possible using Wi-Fi signals.

Dead Reckoning (DR) technology, which makes use of multiple sensor inputs and fuses them with GNSS signal data, provides a further way to determine the location of road vehicles when there are low satellite signals such as in urban areas, tunnels, or parking garages. Modules such as the NEO-M8U feature Untethered Dead Reckoning (UDR) technology that does not need a connection to the vehicle, relying primarily on inertial sensors to process motion data to provide an accurate picture of the direction or position.

Because of our experience in supporting industrial applications of many kinds, u-blox recognizes the importance of the triumvirate of timing, location, and communications. This is reflected in the portfolio of modules that can now help drive industry towards the IIoT. ●

LEARN MORE:
<https://industry.u-blox.com>

FROM FARMS TO FACTORIES, ARTIFICIAL INTELLIGENCE IS COMING OF AGE

Artificial Intelligence will help us reap the full benefits of the fourth industrial revolution.

First postulated in the 1950s, the idea of artificial intelligence (AI) has been around for a long time. In science fiction, robots were often depicted as pseudo-humans with vast stores of knowledge, incredible powers of mathematical calculation, and the ability to understand voice commands. We haven't quite reached this level of AI yet, but as a field it's growing fast, and most of us come into contact with it every day, often without realizing it.

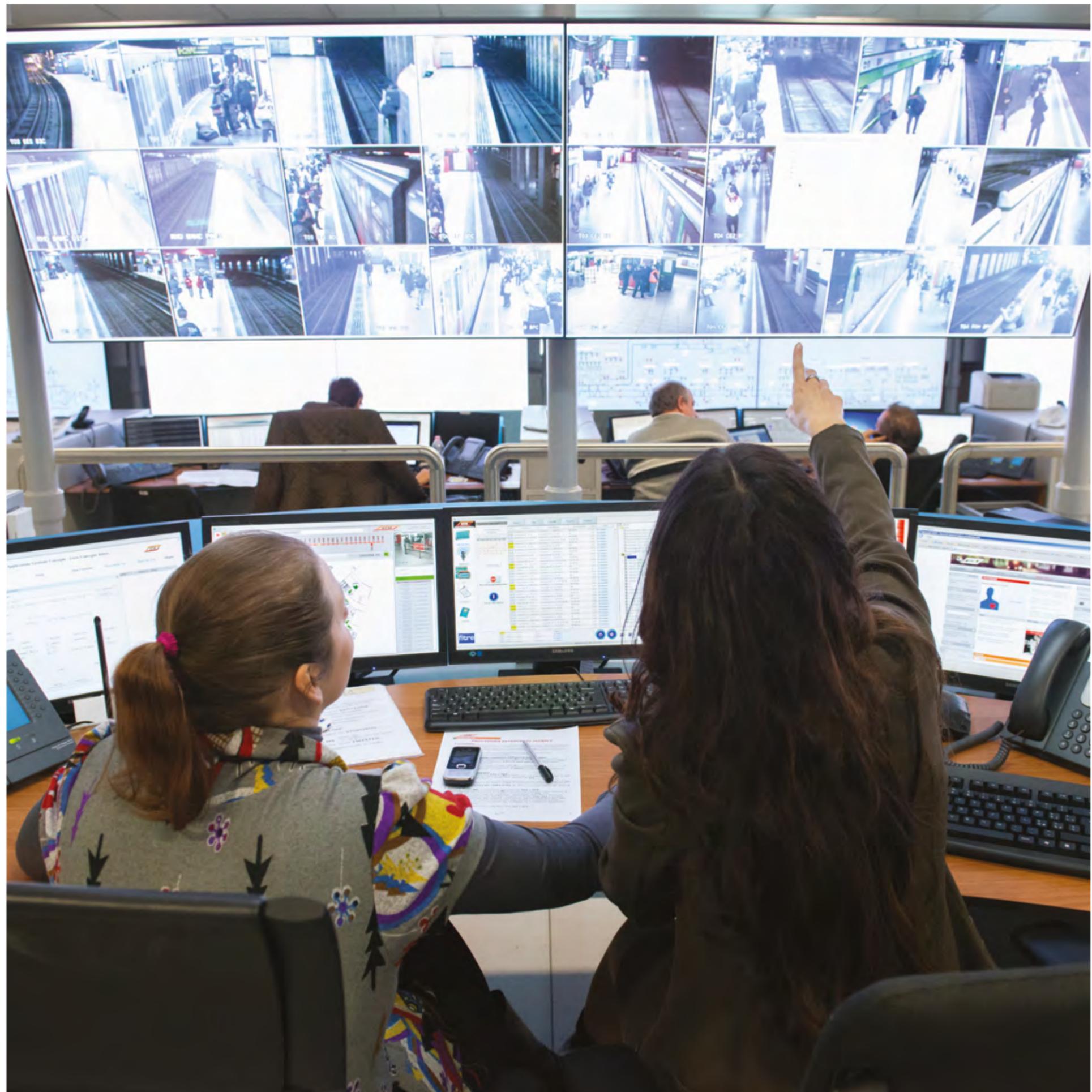
AI is about programming computers to emulate the way our brains detect and respond to things that happen around us. Approaches such as neuromorphic computing, which aims to replicate the way neurons and synapses work in our brains, have come on in leaps and bounds in recent years. This has been key in improving what AI

in Industrial Internet of Things (IIoT) systems can achieve.

The term 'AI' is sometimes used interchangeably with 'machine learning', but the latter is in fact a subset of AI. Machine learning is where a machine learns from its own outputs and improves its processes, but crucially, without human intervention. Then there's 'deep learning,' which is a specific branch of machine learning that uses multi-layered neural networks to perform tasks such as image recognition. Using the data you feed through the neural network, the machine is able to determine which are more relevant results and modify its algorithm accordingly to ensure future outputs are more accurate.

AI systems run on algorithms: sets of mathematical instruc-

Artificial intelligence can be credited for Hong Kong's punctual subway service.





1

tions that process inputs and deliver a variety of output types. These could be anything from signals to activate machine functions to data visualizations that support decision-making. In recent years, there has been great progress in how algorithms are written and implemented. The advances have been so great that Ray Kurzweil, Google's Director of Engineering, estimates that robots will achieve human intelligence levels by 2029. Meanwhile, research firm Gartner believes that a third of jobs will be replaced by robots and smart machines by 2025¹.

Of course, there are moral and ethical concerns about the rise of AI. Will it enhance or damage humanity? Will AI create machines with emotions? If

so, could they turn against humans? Will millions of jobs disappear overnight as machines take over? Naturally, every technological revolution, from steam engines to genetic engineering, has caused some fears and anxieties, but most have gone on to deliver enormous benefits to humanity. In the case of AI, most experts predict it will create more jobs than it eliminates. A study by Accenture, for example, identified several completely new categories of human jobs² that are emerging to support AI systems. And an IDC and Salesforce white paper focusing on the Customer Relationship Management (CRM) space predicted that artificial intelligence will create over 800,000 jobs and boost global revenues by \$1.1 trillion³.

To understand the recent pace of progress in AI, you only have to think about how quickly web browsers now interpret your search requests, or how much more accurate Google Translate has become. Also witness how self-driving cars are now able to undergo trials on roads used by traditional vehicles, and how you can use voice commands with reasonable accuracy when instructing the digital assistant in your phone, computer, or home speaker system. All of these examples rely on artificial intelligence to process and respond to information received from sensors.

The Internet of Things (IoT) and AI are intimately connected

IoT sensors create an enormous volume of Big Data that needs

to be ordered and analyzed. The quantities involved mean it's far more than humans could feasibly process manually. This is where AI comes in, enabling machines to automatically learn from the data and use these learnings to improve related processes.

In situations where action needs to be taken very quickly, there isn't always time to send sensor data to the cloud for processing. In these cases, AI is being deployed nearer the edge of IoT systems, which is where the sensors reside. Companies such as Arm[®] have recently designed new processor architectures that enable AI algorithms to run within small, low-cost, low-power chips that can be integrated into smart sensors.

In industry, AI is being implemented into organizations' workflows to enhance processes through automation, improve efficiency and provide workers with information that makes them more effective in their jobs. Agricultural equipment manufacturer John Deere, for example, is developing various ways to help farmers increase their productivity through the use of AI, with for instance driverless tractors

and sensors that interact with real-time data. Google has cut energy usage in its data centers by 40%, thanks to its DeepMind AI technology. And the Hong Kong subway uses AI to optimize the planning of engineering works. It models the network and creates a maintenance schedule that makes maximum use of its teams, including by identifying opportunities to combine multiple projects or share resources. As a result, AI is a major contributor to the subway's enviable 99.9% on-time performance levels and has given engineering teams an additional half-hour of maintenance time every night, saving the operator US\$800K every year.

Process manufacturing is one of the fastest-growing industries for robotics, as one branch of AI, according to a 2016 report from analysts IDC⁴, the other being healthcare. The use of robots in manufacturing has been growing rapidly for the last 20 years, and IDC predicts the industry will be worth US\$135.4 billion in 2019, with a compound annual growth rate of 17%. Robots rely on numerous sensors for their input data. When connected through the use of AI, with for instance driverless tractors

and sensors that interact with real-time data. Google has cut energy usage in its data centers by 40%, thanks to its DeepMind AI technology. And the Hong Kong subway uses AI to optimize the planning of engineering works. It models the network and creates a maintenance schedule that makes maximum use of its teams, including by identifying opportunities to combine multiple projects or share resources. As a result, AI is a major contributor to the subway's enviable 99.9% on-time performance levels and has given engineering teams an additional half-hour of maintenance time every night, saving the operator US\$800K every year.

So with growing numbers of manufacturers, utilities, logistics companies, and other service providers using smart sensors to collect ever-greater quantities of ever-richer data, AI is going to play an increasing role in helping us take full advantage of it. The benefits we've looked at above are just the start: in the same way that the first three industrial revolutions changed industries in ways few had imagined, so the IIoT, powered by AI, will positively transform the working lives of billions of people all around the world, and to some extent human life itself. ●

BOOK

Artificial intelligence will create over 800,000 jobs and boost global revenues by US\$1.1 trillion.

1 Will AI create machines with emotions?

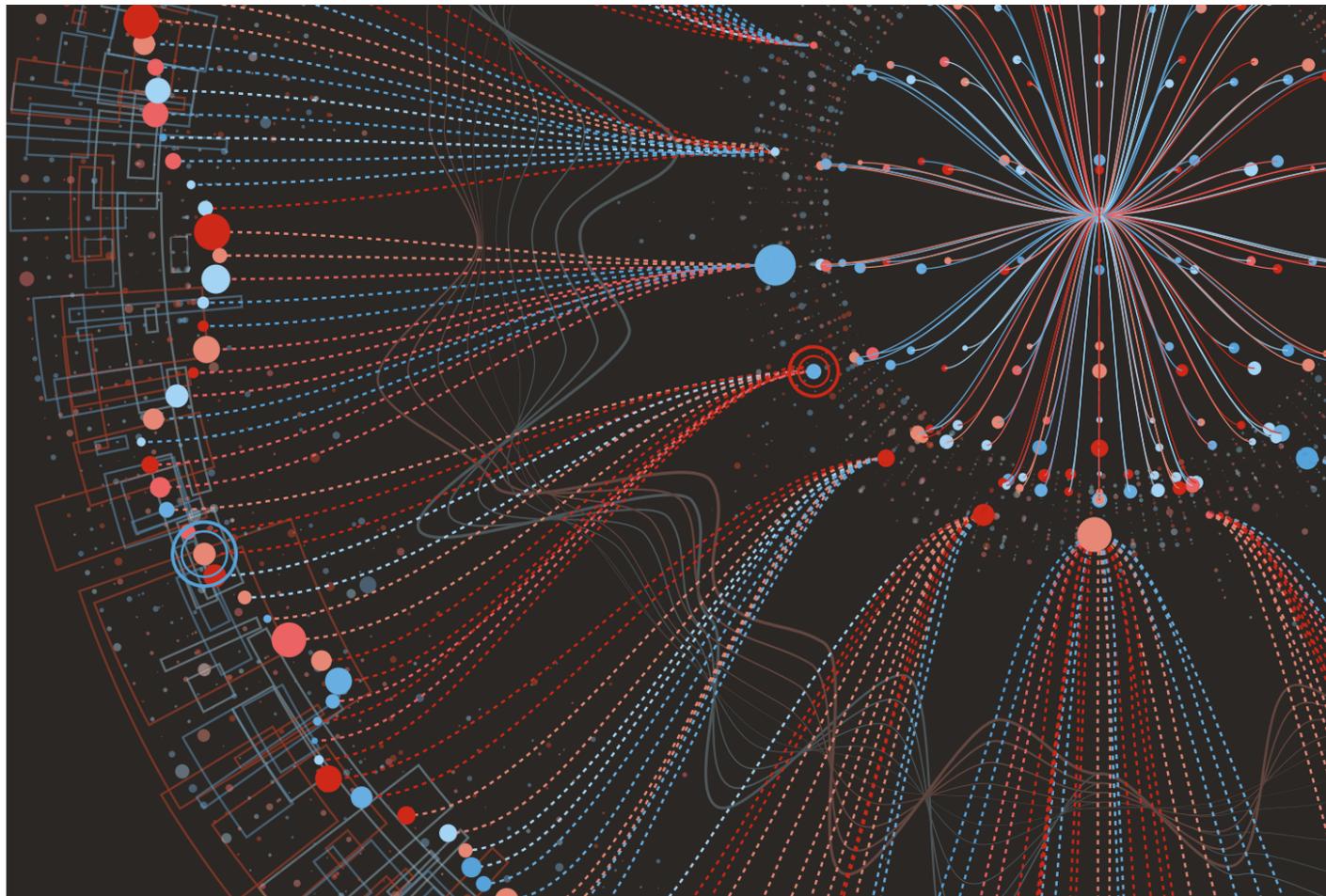
2 Full agricultural automation is no longer a fantasy.



2

ENGINEERING THE IOT MECHANICS OF INDUSTRY 4.0

Striking the right balance between too much and too little IoT at the workplace will take a new breed of Industry 4.0 savvy engineers.



Our notion of Industry 4.0 is meant to explain what we now understand to be the fourth industrial revolution populated by cyber physical systems and the Internet of Things (IoT). But what we really need to do now is know where we apply the so-called innovation points emanating from Industry 4.0 and how we truly leverage the power of the IoT and big data analytics to make our work systems run better. Perhaps most crucially of all, we need to know how we actually physically architect Industry 4.0 advancements into our platforms, applications, devices, and data streams.

How much is too much IT?

Firms now looking to apply the new age of cloud-centric services-based analytics-empowered automation-enriched technologies to their operational foundation need to look for what we might call the IT wastage point. This is the point where the additional application of technology will not necessarily bring any perceivable or measurable improvement to efficiency or performance and the bottom line.

But how do we find that cut off point? Let's use a non-technical example to clarify here.

Modern professional sports teams use player movement tracking technologies to analyze movement and performance. Teams themselves are on strict diets with calorie-controlled food and drink intake measured down to an exact and minute scale. Playing areas are often temperature controlled and atmospheric moisture might even be tracked.

But (in the above example) is the water supply used in hydration drinks analyzed for mineral content? If the sport is played on grass, is the grass growth being tracked and analyzed? Are daily oxygen levels being monitored? The answer is probably not. This is because these details are (at the time of writing at least) generally considered to be too infinitesimally small to make a difference to performance.

The same approach to performance can be applied to companies operating in any industry vertical. The IT wastage point is the socket or widget in the firm's engineering systems (or the function in the services layer) that may not necessarily benefit from the additional application of Industry 4.0 technologies at this stage. Of course the landscape here moves fast and today's IT wastage point is tomorrow's target area for digital transformation.

As we now apply these IoT Industry 4.0 mechanics to our business models, a new substrate layer opens up with wireless communications and semiconductors specifically tuned to support new more intelligently automated tasks, enabling time and cost efficiencies. These tasks can now be more digitally defined, controlled, and managed into data workflows. The digital business starts to come of age across industrial, automotive, and consumer markets.

Rise of the robots?

The opportunity is huge, but there is still a challenge here in terms of how we responsibly engineer these automation advancements into the fabric of our operational models. People often worry about robots, drones, and IoT devices taking over human jobs, but this misses the point, i.e. we can use these innovations to shoulder

the repetitive and dull tasks (but essentially quite clearly definable) that we would rather not do.

So it is not a question of some dystopian rise of the robots scenario at all. Instead it is a question of looking for that IT wastage point and then looking upwards to see where we want to bring the power of semiconductor-driven intelligence to bear in our business models.

It's not about jobs being taken over by computers, it's all about taking the definable drudgery out of some of our processes and then moving forward to more human-driven value-added work that makes a difference to our lives.

How to get an IoT engineering brain

What it really all comes down to is appreciating that we need to become IoT engineers (or at least try to think with an engineering brain) if we are going to be able to apply these new Industry 4.0 technologies in the workplace.

Engineers like to look inside a box to see how it works. Engineers like to open things up and find out how they connect to other things. Engineers like to see if they can use the things around them to make other things and processes work better. This is an all-inclusive engineering call to action that every company stakeholder can embrace from the admins staff to the C-suite.

Get involved with some industrial grease and be an IoT Industry 4.0 mechanical engineer today for all of our sakes. Now, please wash your hands. ●



Adrian Bridgwater is a technology journalist with over two decades of press experience. Primarily he works as a news analysis writer dedicated to a software application development 'beat'; but, in a fluid media world, he is also an analyst, technology evangelist, and content consultant. As the previously narrow discipline of programming now extends across a wider transept of the enterprise IT landscape, his editorial purview has also broadened. He has spent much of the last ten years also focusing on open source, data analytics, and intelligence, cloud computing, mobile devices, and data management.

VIRTUAL REALITY RETURNS TO INDUSTRY

After an excursion into entertainment, VR is once again getting serious.

For the past 20 years, virtual reality (VR) headgear has been a staple of the winter Consumer Electronics Show (CES) in Las Vegas. The image of the gamer wearing a visor has become so familiar it's easy to forget the professional and industrial applications that influenced the earliest ideas around VR and where it is likely to emerge as a powerful technology once again.

A little less than 50 years ago, computer scientist Ivan Sutherland and student Bob Sproull unveiled The Sword of Damocles, the first head-mounted computer display intended for their novel concept of VR. One of the first applications Sutherland envisaged for the head-mounted display was to visualize the working of prosthetic heart valves. Realizing that it would take many years for technology to catch up with the needs of the head-mounted display, Sutherland worked on a more achievable form of VR: the full flight simu-

lator (FFS). Based on a combination of a physical cockpit with simulated graphics for the view from the cockpit and a system of hydraulic rams to simulate the motion of an aircraft, the FFS revolutionized pilot training. It made it possible for trainees to log hours of practice with no risk of damage to aircraft if things went wrong. A crash in the FFS might lead to a jarring bump for the trainee and their instructor, but nothing more serious.

Virtual and augmented reality for industrial applications
Now VR and the closely related technology of augmented reality (AR) are moving into the design and manufacture of aircraft and countless other types of product and machinery. VR makes it possible to visualize the 3D structure of complex mechanical systems such as the rotating fans and pipework that make up a jet engine. Engineers can use headsets or interact with each other in a cave automatic virtual environment (CAVE) – a room



Virtual reality and artificial reality are moving into the design and production of machinery.

Computer scientist Ivan Sutherland and student Bob Sproull unveiled the first head-mounted computer display in 1968.



VR is widely used in aviation, from the construction of fuselages to flight simulators.



fitted with large video displays on the walls – to better understand how parts will fit together and behave in the real world.

Manufacturing, maintenance, and service will increasingly rely on AR technologies. Aircraft maker Airbus is already experimenting with AR to improve quality in the construction of its fuselages. Workers wearing AR-enabled visors and glasses get real-time help to ensure fasteners are tightened to the correct amount, removing the need to check each one separately. Cameras and sensors in the tools used to assemble and tighten the fasteners keep an eye on torque to make sure the nuts are fitted properly and not over- or under-tightened.

When it comes to servicing machinery, headsets can guide workers on how best to disassemble equipment safely and put it back together again – and check for damaged components to streamline the repair or maintenance process.

The biggest changes for AR and VR though will come with the introduction of 5G mobile services expected to arrive at the end of this decade. 5G is much more than a further improvement in download speeds for video and audio. It changes the architecture of the network to become much more responsive to real-time data. One of the most important factors for AR and VR is a massive reduction in latency to the order of several milliseconds.

The reduction is such a big change from previous wireless generations that people are taking into consideration the speed of light when planning where to put the servers needed to sup-

port VR applications. Every 200km of distance adds more than another millisecond of delay in a typical optical core network, where silica makes the speed of light about 30% slower than in a vacuum, before including amplification or routing. This means that highly demanding computer processing can be offloaded to offsite server farms, which also allows VR users to easily take advantage of improvements to software and computing resources.

High-performance servers also make it possible to remote control industrial robots via VR, such as in hazardous environments.

The robots will be able to handle nuclear or chemical waste, repair live machinery, and provide sensory data with the required resolution and responsiveness to make mechanical limbs extensions of the human body.

Low latency also ensures that users will not suffer from motion sickness any longer, a common side effect of using VR applications. Motion sickness is the result of too much latency when rendering virtual scenes in the headset.

As advances in technology create new application environments, we can expect VR and AR to return to the industrial world and help drive a new wave of product design, manufacture, and maintenance. ●

THE DEMISE OF THE DIAL

From touch screens and voice recognition to virtual dials that hover invisibly mid-air, new human-machine interfaces could render interfaces as we know them today obsolete.

Consumer electronics have been the key driving force in changing the way we interact with machines in industrial applications. The high volumes of products made for consumers have made it economical for manufacturers to invest heavily in R&D in order to create interfaces that make their products more attractive and easier to use, giving them competitive advantage. The same goes now for industrial manufacturers, with the advent of the IIoT and the growing need for easy-to-use interfaces for industrial applications.

Just two decades ago, few would have imagined the way we interface with electronic devices today. Back then, mechanical switches were the norm, and while some products had primitive 'touch' technologies, in certain cases 'press and hope' would have been a more accurate description. Then capacitive touch interfaces began to appear, with the original iPhone arguably the catalyst that saw them become truly mainstream. Believe it or not, that was ten years ago.

The continued use of mechanical switches

Today, mechanical switches still have a role to play in Human-Machine Interfaces (HMIs), albeit a diminished one. Sometimes, they're the most cost-effective option, particularly in heavy-duty applications, such as switching power on and off. Sometimes, they're used because people still prefer their simplicity and the feeling of operating a physical switch. For example, cars will often have touchscreens, steering wheel controls, and mechanical knobs, all of which enable the driver to adjust the volume of the audio system. People like to have a choice.

The legacy of physical buttons lives on in other ways too. While the means of sending a command from the human to the machine may be evolving away from mechanical buttons and switches, many modern touch controls still seek to mimic them. This is perhaps because so many people were brought up with buttons and are familiar with how to operate them. But this is changing. Younger generations are gradually becoming used to touch interfaces that don't seek to replicate switches and buttons. As these new norms become more widely understood, we're likely to see whole new ways of interacting with machines, unhindered by deep-rooted expectations.

The evolution of touch

Touch controls have developed rapidly since the early days of pressing a point on a screen to make something happen. Multi-touch technology recognizes the presence of more than one contact point on a surface, while gesture controls, such as pinch-to-zoom, extend this concept. Force-sensitive touch is now also becoming commonplace.

Multi-touch panels have already made the transition from consumer electronics into industry. A good example is Siemens's SIMATIC HMI technology for visualization applications, which offers operators more efficient control and monitoring of industrial plants.

There's also been a blurring of the lines between consumer and industrial products, including the use of industrial monitoring and control apps that run on consumer smartphones or tablets and communicate with equipment via

First popularized by the iPhone, touch interfaces are becoming increasingly common in industrial settings.

technologies such as Bluetooth low energy (BLE). They can manage a range of devices, such as heating control systems or local medical devices, for instance. A Bluetooth low energy app offers a full graphical user interface (GUI) with many interaction possibilities using multi-touch technologies. It allows to present historical data in graphs, represent the data from the device in a user friendly format, and support multiple languages. This ability to use proven consumer products is lowering the cost of bringing new interfaces into the industrial world.

The need for feedback

Some have been concerned by a lack of feedback from touch panels, and product designers have attempted to address this in a variety of ways, many of which are still evolving. Visual feedback is commonplace, delivered either by the image on a screen changing or via an LED indicator on a touch panel. Others have used audio feedback, while most recently, haptics – or tactile feedback – is growing in popularity. Where conventional keyboards provide a response through springs under the key caps and flat-membrane keyboards employ domed pieces of metal under their surface overlays, designers of capacitive touch panels have come up with other ways to deliver a physical sensation in response to touch. Small motors or piezoelectric devices are sometimes used to make a panel vibrate when it's touched. However, at present, it's difficult to make this response location-specific on a touch panel.

Other technologies are being developed to

solve this problem. Bending wave haptics, for instance, is a low-frequency surface wave technology that can focus haptic feedback from specific touch points on a panel or screen. Different effects can be delivered simultaneously to different fingers.

A more recent innovation, mid-air haptics, uses ultrasound to create virtual objects such as control knobs in the air. Consumer electronics companies and car makers, including BMW, are evaluating mid-air haptics, so while it hasn't yet appeared in industrial applications, it may only be a matter of time.

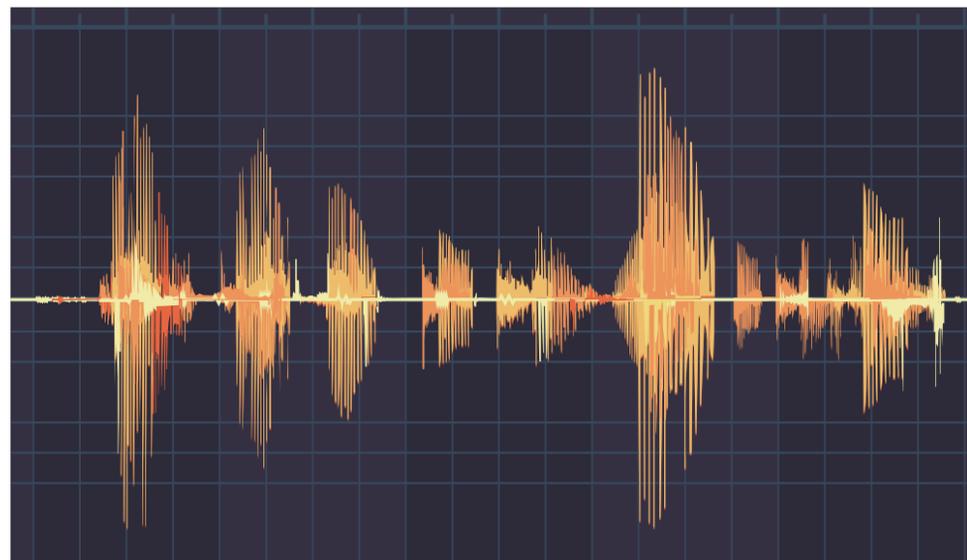
Augmented reality and virtual reality

Both augmented reality (AR) and virtual reality (VR) are growing in popularity in the consumer marketplace. Pokémon Go brought AR to the masses, while after several false starts for VR over the past few decades, the likes of Facebook, Google and Microsoft are now investing heavily to develop the technology.

As a way of interacting with industrial machinery, neither is particularly new, but nor are they yet widespread. However, as the technologies develop, we expect them to become more commonplace in industrial applications, enabling some truly exciting new use cases. You can read more about AR and VR on page 18.

Voice interfaces

Perhaps the most interesting HMI developments are in voice user interfaces (VUIs). We are increasingly using voice commands on our smart-



Multi-microphone setups, smarter processor chips and artificial intelligence (AI) make it possible to separate voices from industrial background sounds.



phones and other digital home assistants, such as Alexa in the Amazon Echo.

The Voice over LTE (VoLTE) cellular standard, which is currently being implemented by leading mobile network operators, is a new way to carry conversations over LTE networks. In the industrial sector, it will make it possible to use a call center or even voice recognition services, hosted centrally, to reshape the user interfaces of IoT devices that are rarely accessed by people. For example, rather than including a costly touchscreen on a building control system, why not use a voice channel to ask someone (or something) to adjust its controls for you? VoLTE supports simultaneous voice and data connections, which are required for roadside assistance systems or medical alert devices. This allows users to talk to a call center operator, while data about their emergency or medical status is uploaded to the response center.

Industrial environments, however, present additional challenges, most notably noise. How do you separate voices from background sounds, particularly if the person giving the command is some distance away from the microphone on a noisy factory floor? Multi-microphone setups, smarter processor chips, and artificial intelligence (AI) are making this possible. For example, a multi-microphone system can track people as they walk around a machine, while artificial intelligence can enable machines to recognize individuals by their voices, just as other humans would.

Holography

Arguably the most advanced of all current interface technologies, holography, may also be about to appear in industrial settings. In 2016, Iconics, a US-based control and instrumentation company, announced the 'world's first holographic machine interface.' It uses Microsoft's HoloLens, a self-contained holographic computer, to visualize real-time analytics data in 2D and 3D holograms. The company says this rich presentation of data is a time-saver for maintenance operations and field service personnel.

The end of the interface as we know it?

The digital transition of industry is gaining momentum. The coming decades are likely to see whole new ways of interacting with machines that go far beyond what's imaginable now. Interfaces as we know them today may even become obsolete.

We'll see greater interconnection between machines and powerful cloud-based computers, which will create new ways to monitor and control equipment, bringing in other general data on trends from the environment and mining it for further efficiency using analytics and artificial intelligence. All of this means that the workforce of tomorrow will benefit from higher-quality machines that ultimately increase productivity and help to deliver more personalized, high-quality products. ●

Holograms provide new ways of interacting with 3D virtual objects.

A GLOBAL PUSH

Hundreds of millions are being spent on the Industrial Internet of Things (IIoT) around the world. We look at what governments and businesses are doing and at the technologies being employed.

Linking large numbers of industrial sensors or controllers to a central monitoring or control system that enables smarter and quicker decision-making is high on the agendas of governments and businesses around the world.

It's easy to see why: forecasts suggest the resulting IIoT will create jobs, improve productivity¹, boost innovation, and thereby add significantly to companies' bottom lines and the global economy. Research by Accenture² into the predicted impact of the IIoT on 20 major economies (that together account for more than 75% of global output), suggested the IIoT could add between US\$10.6 trillion and US\$14.2 trillion to their cumulative GDP by 2030.

It's these sorts of figures that are encouraging governments and business leaders to plow significant funds into IIoT-related research and development.

Lack of standardization – a key challenge

A broad range of technologies is being used in early IIoT projects, and this lack of standardization has been highlighted as a major barrier to wider IIoT adoption, according to research by Morgan Stanley. The communications and location-awareness technologies – both key to the IIoT – highlight this issue.

With all IIoT kits needing some means of energy-efficient (usually wireless) communication, there are numerous technologies available – some competing, others complementary. For short range, options include Wi-Fi and Bluetooth (and Bluetooth low energy). When distances are greater, LTE Cat M1 and LTE Cat NB1 sit alongside traditional cellular technologies.

On the positioning side, there are the four major Global Navigation Satellite Systems (GNSS):

GPS, Galileo, GLONASS, and BeiDou.

As a product designer, which technologies or GNSS one chooses will depend on the nature of the solution one is creating – and on where in the world it's going to be used.

Given this, let's take a whistle-stop tour of the global IIoT market, looking at what's happening in each of the major regions and what technologies are being rolled out.

Europe

In Europe, perhaps the highest-profile government-led initiative is the German INDUSTRIE 4.0. This program, which has been allocated up to €200 million, is putting in place policies and funding aimed at making Germany a 'lead market and provider of cyber-physical systems by 2020.' Its influence is being felt beyond Germany too: the European Union has pledged

¹ Why IIoT spells J-O-B-S, by Allan E. Alter and Paul Daugherty, Accenture, 2017.

² The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity, by Mark Purdy and Ladan Davarzani, Accenture, 2015.

³ The Internet of Things and the New Industrial Revolution, Morgan Stanley Research, 2016.

to build on it its Digital Single Market drive. Meanwhile, it's hoped that IIoT collaborations, such as those between Germany and China and between Germany and Australia, will see a convergence of standards in the IIoT space.

Other European countries have also thrown their weight behind IIoT-related initiatives. The UK government's innovation agency, Innovate UK, is running numerous funding competitions related to IIoT, including in healthcare and transportation. Meanwhile, French Secretary of State for Industry, Christophe Sirugue, set out his country's plans to support digital industry starting in 2016.

On the tech side, LTE Cat NB1 and 2G cellular have so far been the preferred long range communication choices in EMEA. These deliver the broad coverage required, while LTE Cat NB1 is an ideal choice for the many smart utility metering programs being delivered, given its ability to reach meters buried underground or encased in concrete. On the positioning side, the recently launched Galileo GNSS is key, as it is created by the European Union.

A great example of NB-IoT technology in action is in Lisbon, where Huawei has been piloting its pioneering NB-IoT-enabled smart electricity meter. Looking at short range radio technologies, HMS Industrial Networks has launched its Anybus Wireless Bolt, enabling industrial facility operators to control existing equipment remotely using Wi-Fi, Bluetooth, or Bluetooth low energy.

Asia-Pacific

Europe isn't the only region

where governments are getting behind the IIoT. In Asia-Pacific, the Chinese, Indian, Japanese, and Taiwanese governments are all developing or supporting IIoT-related initiatives.

There are plenty of projects happening as well. In South Korea, Cobilsys has launched the ultra-compact ATPACK asset tracker, which can be used to keep tabs on moving objects such as vehicles and containers in IIoT environments. It's underpinned by two u-blox products: a GNSS module capable of concurrently using three satellite navigation systems, and an HSPA/GSM cellular communications module.

In the Indian region of Odisha, the Forest Minister has unveiled a new handheld GNSS device, the Sxtreo T51 PDA, that promises to transform forestry management and protection. To be used by thousands of rangers, the unit combines traditional GNSS with India's own GNSS Aided GEO Augmented Navigation (GAGAN) system to enhance accuracy. The resulting precision enables rangers to geotag the locations of individual trees and animals.

In terms of low-power wide-area (LPWA) technology, APAC has been broadly in line with EMEA, with LTE Cat NB1 being the preferred option.

Americas

Much is going on in the Americas as well, though the communications technology has followed a different path, with LTE Cat M1 being the preferred LPWA network.

Project-wise, there's plenty of variety. The United States government's Centers for Disease Control and Prevention, for example, ran a pilot to assess

how IIoT could be used for monitoring and control systems in the mining industry. The work involved assessing radio frequency identification (RFID), wireless communications, wireless sensors, and real-time location-sensing.

Above ground, agricultural equipment manufacturer John Deere has been rolling out a variety of products and services to improve its customers' efficiency. This Precision Agriculture Technology connects equipment together to enable remote management, equipment guidance, and more.

And California-based Xirgo Technologies is using a range of technologies in its industrial tracking and monitoring products, with each solution tailored to the environment it's required to operate in. Applications include shipping container tracking and vehicle trailer tracking, the latter using energy-harvesting to enable operation without an external power source.

The need for hybrid solutions

The incredible variety of possible IIoT use cases, combined with the different technology options, demonstrate the growing need for technical flexibility and interoperability. This is why smart product makers are choosing GNSS modules such as the u-blox EVA-M8, which can concurrently link to more than one satellite system, communications components such as the u-blox SARA-R4 module series and ODIN-W2, which support LTE Cat M1 and Cat NB1, respectively Wi-Fi and Bluetooth. This approach is the best way to tap into the numerous government- and business-led initiatives gathering pace across the globe. ●



1 The INDUSTRIE 4.0 program aims to make Germany a 'lead market and provider of cyber-physical systems by 2020.'

2 Xirgo Technology's new vehicle trailer tracking system can be operated without an external power source.

3 Location trackers such as the Cobilsys ATPACK tracker help keep tabs on mobile assets.

IOT AS AN ENGINE OF GROWTH IN TAIWAN

Taiwan is harnessing the power of the fourth industrial revolution through a series of industrial initiatives.

We've seen that the IIoT is poised to transform industries. But when designated a key pillar of national policy design, it has the potential to transform entire countries. With its sights set on the future, Taiwan is seeking to keep up its competitive edge and boost its economy through a series of ambitious industrial initiatives. These include forging its precision machine industry into an intelligent machine industry, encouraging the development of smart cities and the technologies that enable them, and promoting IoT-related innovation through its Asia Silicon Valley Development Plan. Jointly with the eight-year DIGI+ Economic Development Plan, geared towards growing Taiwan's digital economy, these government-led initiatives aim to spur on R&D and create an innovation and entrepreneurial ecosystem that will ultimately develop exportable solutions for the global market.

Many companies offering smart solutions for the IIoT from within this ecosystem have u-blox technology at their core. One of them is Moxa, whose products connect devices on the ground, where the IIoT is spreading rapidly, reaching deep into factory floors and transportation and utility networks. Another is HEX, a company that is expanding the IIoT in the air, producing solutions for a growing global fleet of drones dedicated to a broad range of industrial applications, from precision farming to powerline inspection.

Moxa

A global player in industrial automation for over 30 years, Moxa has evolved into a leading enabler of connectivity for the Industrial Internet of Things. Specializing in the development of RISC-based mobile computers, they offer solutions for a wide range of complex industrial communications needs, such as energy monitoring systems. With a focus on the tomorrow's smart grids, Moxa has developed smart substation controllers to ensure the robustness of smart power grids worldwide. And recently, the company rolled out a RISC-based solution providing reliable train-to-ground data communication for the smart railway networks of the future.

LEARN MORE:

www.moxa.com/IIoT
www.moxa.com/Industrial_Computing/Index.aspx

HEX

Global demand for drones and in terms of their performance are growing in tandem. HEX is dedicated to create core drone accessories to meet these needs, providing cost effective and open source technologies enabling drone developers to build better and better solutions. With Pixhawk 2.1, it released what has since become the world's leading open source drone autopilot. Now, it is bringing centimeter level positioning accuracy to the ArduPilot open source autopilot suite, powered by u-blox's NEO-M8P high precision RTK GNSS module, taking the open source drone industry to the next level. ●

LEARN MORE:

www.hex.aero



The UC-8100-ME-T is designed for embedded data acquisition applications from -40°C to 70°C with LTE enabled.



Pixhawk 2 is an affordable and lightweight open source drone autopilot.

TOWARDS A SECURE CONNECTED INDUSTRY

Security is vital to any connected enterprise. But who is responsible for ensuring it and how is it best achieved? Two security experts discuss how to enable trust in complex IIoT value chains.

Gartner, Inc. forecast that 8.4 billion connected things would be in use worldwide in 2017, up 31 percent from 2016, reaching 20.4 billion by 2020. This will also affect the Industrial Internet of Things (IIoT). In addition to the increased number of connected things, the ability to collect more data from geographically dispersed field assets in remote locations has driven the need for enhanced communication technologies. As the number of sensors and data points with improved

connectivity and new technologies continues to increase, so too does the network's exposure to attacks, making robust security paramount.

What are the challenges in securing IIoT applications such as in health-care or manufacturing?

MATS ANDERSSON – No matter the application, it all begins with knowing that the right software is running in the

module. This is the very basis for a secure connection to the Internet, which you need to completely secure data all the way from the device to the end point in a cloud service. There are also interfaces within the systems that you must secure, to ensure that only authenticated access is possible. And end-to-end security also means securing the connection all the way from the source of the data to the Internet by authenticating and encrypting it.



Robin Duke-Woolley
CEO, Beecham Research



Mats Andersson
Senior Director Technology, Product Center Short Range Radio, u-blox

ROBIN DUKE-WOOLLEY – Indeed, many different elements of security are needed, irrespective of the type of application. With some of them, there's a need for more security in the individual elements; with healthcare, for example, there's a need for privacy of the information. This means that slightly different techniques have to be incorporated to make that work.

M.A. – Privacy is key in areas where people are involved, true, and we need to

that can affect production performance, in particular in industrial systems that contain really small embedded systems. The way we try to address this is to use different types of hardware accelerators in our devices.

Today a lot of industrial devices are connected locally inside the factory via the company's intranet. Therefore industrial customers have very little knowledge on how to move the data up to the Internet. But now with things such as preventive

out from. That's the basis that I think u-blox is working with as well.

M.A. – Yes. It's very important to secure the system from the root and to have a secure identity on the device to know that you are talking to the right one.

Given these dangers and as more devices and objects become connected within industrial IoT systems, are we doing enough to implement security measures?

R.D-W. – The root of trust is really important, and it provides the opportunity for creating secure elements within a bigger environment. But we need to think about how urgent it is to get on with this. In the surveys that we do of adopters, security always comes out as the top issue, but I think that there is, equally, not much knowledge about how to address it.

M.A. – I agree and I think it's really urgent. One already sees devices slipping out today that are not really secured. Historically, mostly consumer-oriented things have been on the agenda, but now we see more serious threats. Do you remember the Stuxnet, the malicious industrial computer worm that actually interfered with computer systems in Iran's nuclear plants? The main problem there was the communication link between devices, which made it possible to interfere with the link, get into the systems, and install malicious software on the devices.

An IIoT network typically consists of small embedded devices with long lifespans that are rarely, if ever, updated. How can you guarantee security when updates are minimal or don't exist?

M.A. – Yes, many of these devices don't talk to the world that much and are therefore difficult to update when needed for security reasons.

R.D-W. – That's really an interesting point.

“IN THE SURVEYS THAT WE DO OF ADOPTERS, SECURITY ALWAYS COMES OUT AS THE TOP ISSUE, BUT I THINK THAT THERE IS, EQUALLY, NOT MUCH KNOWLEDGE ABOUT HOW TO ADDRESS IT.”

ROBIN DUKE-WOOLLEY

have means in our products to ensure that when a device is communicating over the air, it cannot be traced back to an individual. For example, there is a feature in Bluetooth called Privacy, where the address of the device changes constantly so no one can listen in and find out a person's whereabouts. At u-blox, we set higher requirements on the authorization and authentication capabilities for health-care applications than for other applications, and this also helps achieve privacy.

R.D-W. – Manufacturing has much more to do with real-time information than healthcare, which changes the requirements for security. How would you see that?

M.A. – One thing we've found out with our industrial customers is that real-time information can be a problem, because adding a lot of authentication or extra encryption causes delays in the data flow

maintenance, they start to see a need to store more data, combine data with other external sources, and so on via the Internet or the cloud. With these possibilities come new challenges and security risks related to authentication and encryption that they aren't prepared for.

Ensuring signal integrity is crucial for the safety and operational reliability of any IIoT application. How should the IIoT value chain achieve data security and privacy?

R.D-W. – It's not just about maintenance, although that's obviously important; there's also the interaction between different parties, which is part of the overall process. This leads to a lot of potential attack points for miscreants. How do we address these types of situations? I think it starts with a secure root of trust, so you have a secure start point. Then you've got the islands of trust which you can move

“I THINK THAT A LOT OF THE SYSTEMS
IN THE FUTURE WILL BE
A COMBINATION OF CELLULAR AND
SHORT RANGE. ERICSSON TALKS ABOUT
CAPILLARY NETWORKS.” MATS ANDERSSON

If you've got something that is pretty much isolated from the network, how do you update it? If it's connected all the time like cellular, it's much easier – unless you've got a very low-power cellular device where you'd have a battery issue if you started to download lots of updates.

M.A. – Exactly, new low-power cellular will run into a similar problem as we see in short range. But at least they are Internet-connected. What if you have a Bluetooth low energy device that runs in a network without being connected to the cloud? We are looking into introducing firmware updates to them via a proxy, for example a phone app or gateway that talks to the central FOTA server for firmware-over-the-air updates and talks back to the device using Bluetooth to find out if an upgrade is needed and securely performs it. FOTA capability not only makes it possible to keep track of the firmware, but also of all the devices. We can then conduct wireless update campaigns on all our customers' devices. And all of this with a high level of security.

Who in the IIoT value chain should take ownership to ensure security across the various verticals and what are the obstacles?

R.D-W. – You can't assume that a customer will take ownership and have the buck stop with that person or that part of business. Maybe we are not in a situation yet where the person who should take responsibility actually knows enough to be able to do so.

M.A. – I think it's a bit different with enterprises, because they should be more aware of security when installing a new device in a factory or in a hospital. We already see new or updated standards emerging and expect future requests for

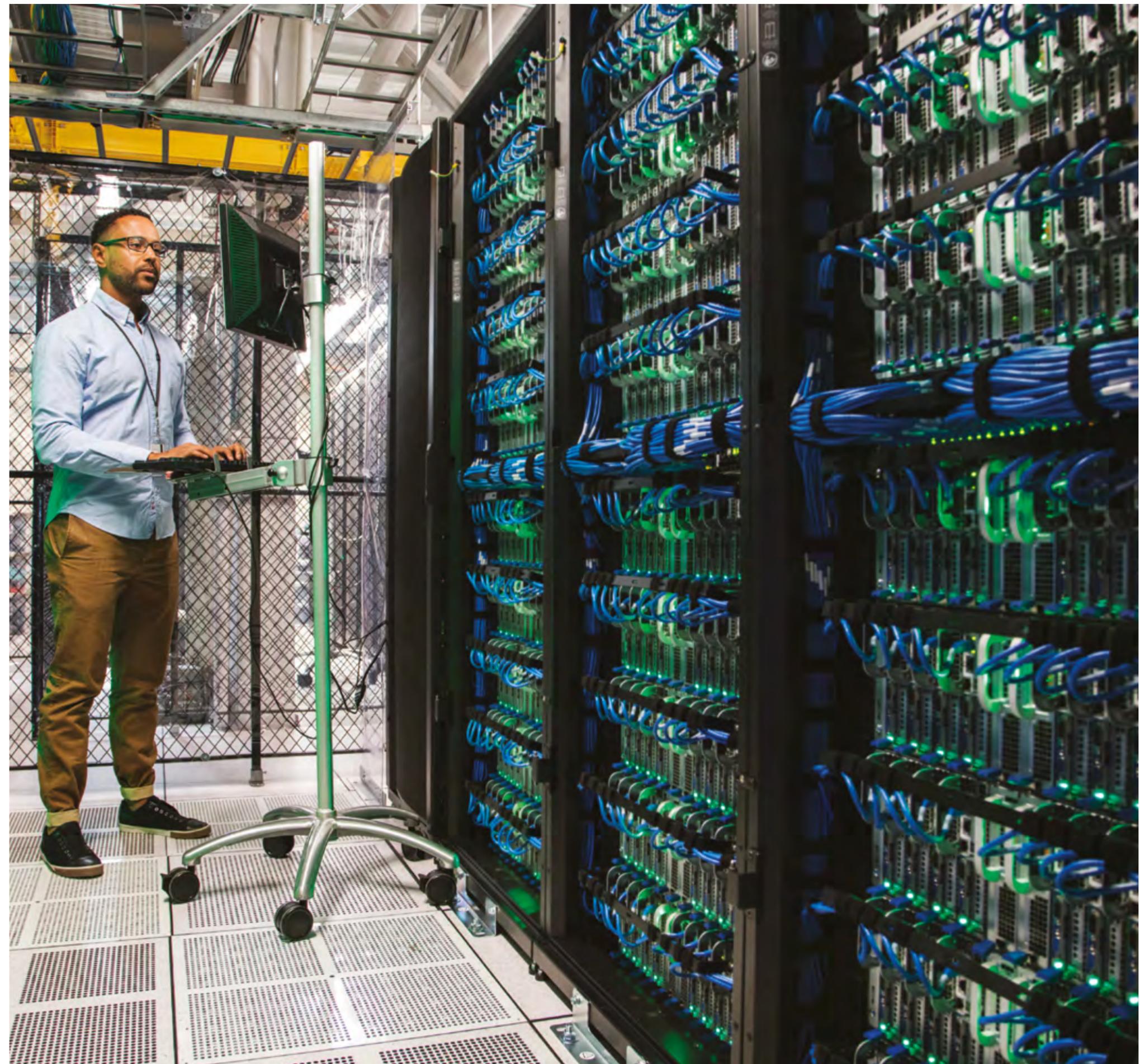
quotations from our customers asking for specific standards and therefore taking ownership.

R.D-W. – We work very closely with the IoT Security Foundation in the UK. They are coming out with guidelines and creating a trust mark for people who conform to them. That gives the user the confidence that guidelines that make sense are actually being implemented. I've always felt that the IoT market grew up through individual sales, opportunistically, and that the technology was pushed on enterprise users. What we've ended up with are little islands of use, even within one organization, that don't necessarily aim to work in an interconnected way. If they would, they could share data and get more value out of it.

M.A. – In terms of security, if they develop security differently by using different algorithms, they can't even talk to each other. Wireless links like Wi-Fi and Bluetooth have defined their own standards supporting high link level security. But they aren't necessarily used, often by lack of knowledge. Actually, the IIoT is a key area nowadays where high requirements on link layer security are requested. We have, for instance, customers in the automotive tools area, where there are mandatory requirements on supporting enterprise level Wi-Fi security using the Extensible Authentication Protocol, also known as Protected EAP, and Transport Layer Security, TLS.

R.D-W. – Interestingly, when you have service-level agreements or you've got guidelines that are generally understood, people can start to request the security that they are actually looking for. Then, the job of the vendor becomes not so much promoting new methods, but more of a tool box from which things can be

Connecting more and more devices raises the stakes for security and privacy.



chosen. This is actually very consistent with u-blox's five principles used in different proportions for different things. Maybe that's the way forward with users as well: once they can specify, then it becomes easier. It also depends on the levels of security required, doesn't it? You could be ultimately secure, but it would probably cost so much that it wouldn't be worth doing. It's a balance between cost and need.

M.A. – We can see that for some smaller devices, it's not affordable to have the highest level of security.

R.D-W. – Ultimately, the customer or the enterprise user needs to decide just how much security they need for their application. However, they don't really know enough to be able to say how much security they need or don't need. When we talk about a value chain and the security of the value chain, it's important that each component supplier within that value chain is looking at the security needs. But if we just leave it up to the value chain to decide or that user, I don't think that that will work, will it?

M.A. – No. Our approach is to provide security functionality on all levels, starting from authenticating the code running in the IIoT device all the way up, including the link to the cloud service. A high level of authentication and encryption on all levels, on communication links as well as end-to-end, is a way to ensure both data integrity and privacy.

When we consider the legacy systems and the need for retrofitting, how long will it take to implement a secure industrial value chain? Does it depend on the market or the regions? Do you have an example of a success story?

R.D-W. – Should we actually do retrofitting? There is a view that to retrofit into existing applications is fraught with difficulty and that it's better to start fresh. Ultimately, I can't think of any situation where it's actually been successful.

M.A. – I agree with you that retrofitting is a big problem. If you take industrial system automation, in many cases these systems have been running for many years,

with limited computing power and using protocols on the local network level. They are very difficult to retrofit. Industrial systems are also vulnerable to downtime. Therefore, to avoid having to touch a running system, some customers install a new infrastructure, for example a preventive maintenance system, in parallel with the control system.

R.D-W. – The difficulty is also that you very seldom replace all of the elements of a control system at once, but more piece by piece, perhaps when they wear out after 50 years. So actually implementing a new security system for an industrial control can take forever. It's got to be, as you say, like an overlay. Or when you build a new factory.

M.A. – Yes, or you add a subsystem. We have a customer that makes industrial tools for the automotive sector. They replaced all the assembly tools thanks to a new wireless Internet-connected subsystem that doesn't interfere with the other systems in the factory. This makes it possible for them to analyze the data generated over the cloud to monitor how efficiently the factory works in order to enhance maintenance and planning.

R.D-W. – And you don't necessarily need to connect to the Internet to get that data analytics information, so long as you can find a way of storing it and capturing it locally.

M.A. – Yes, the IoT can also connect devices via an intranet inside a factory, because the same technologies are applicable. But you still need to have a higher level of se-

curity than in the past because there are new attack points, especially with wireless connections.

R.D-W. – For example, for an external maintenance company, it makes more sense to use a wireless link into the factory, than to try and go through the firewall.

M.A. – Yes. If you rent an industrial device, the renter will want to be able to look into it for maintenance purposes. If he wants to connect the device not using the internal industrial system, he will use his own wireless network, for instance using a cellular modem installed directly on the device.

R.D-W. – In the past, you never connected

“IN THE PAST THERE HAS BEEN THIS TENDENCY... TO ASK CUSTOMERS WHAT THEIR TECHNICAL NEEDS WERE. I THINK WE SHOULD ASK THESE QUESTIONS FROM A BUSINESS POINT OF VIEW.”

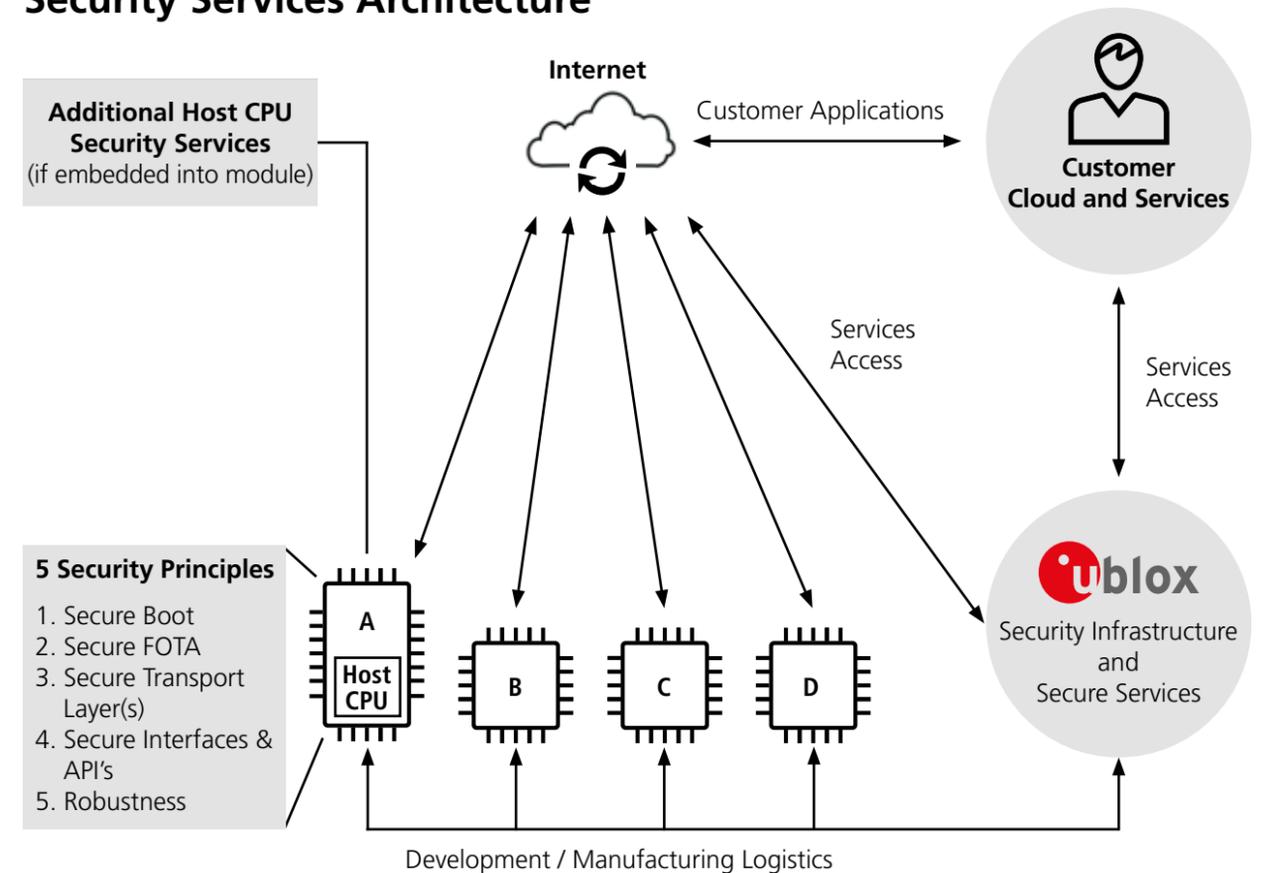
ROBIN DUKE-WOOLLEY

anything in the industrial environment using cellular or wireless because it's a noisy environment, and you couldn't really get the cost justifications right. But now, the security needs seem to justify use of cellular and wireless technologies.

M.A. – Yes, but how much will be cellular and how much will be something else? I think we can agree that a lot of the systems in the future will be a combination of cellular and short range systems. Ericsson talks about capillary networks. There will be lots of small sensors, valves, etc., all connected locally via a short range network and then connected via a cellular gateway to the Internet.

But when it comes to security, this actually means that you have a new problem. You might have devices connected on a short range link to a gateway and a cellular

Security Services Architecture



link from the gateway to the Internet, all with different levels of security. Ideally we would like to have the same level of security throughout the network. But if you authenticate and encrypt the link from a short range device to a gateway, it will perhaps limit the real-time behavior, so you might decide not to secure that first stage, but only when it gets to the hub, where there is much more capacity. This will of course limit the level of security, but this is what is done in many cases. At least the link going outside the factory or building is secured.

It would cost more to secure end-to-end throughout the systems, both in terms of resources and money. You might even need to move to full TCP/IP-based communication end-to-end instead of using domain specific protocols that are much more constrained and difficult to secure. Still, if you think about the security attack we had a couple of months ago, where a lot of devices were sending data and disturbing more or less the whole Internet, it might

be worth considering more expensive and resource-consuming solutions to prevent this from happening.

Can you tell us a little about the u-blox approach to enhance hardware security?

M.A. – We've defined five principles or pillars of security as a framework that covers all levels of security. It all starts with knowing that you have the right firmware running in your device. We define this as secure boot and secure firmware. We make sure to use encryption and authentication to ensure that a valid code, either ours or the customer's, is running in the device.

R.D-W. – That's the secure root of trust, isn't it?

M.A. – Yes. Then we talk about end-to-end security. The radio link as such and the end-to-end security from the end node, so that the whole link up to the cloud is secure. We also need to support certifi-

cates provided by the customers that we securely store in the device. Then, another pillar is secure APIs and secure physical interfaces. We have a lot of interfaces in our system today, and it's very important to secure them as well.

R.D-W. – There is a need to update it all and not have it go wrong.

M.A. – Exactly, so another pillar we have is a secure FOTA to make sure that you download the right firmware in the right way to the right device. And finally we have to avoid jamming and spoofing. At least we need to be able to detect jamming and report it back to the customer's application. Spoofing is even trickier in some cases as it can literally fool a system.

In what ways is u-blox supporting its direct and further downstream customers to demonstrate the supply chain of trust expected of any digital enterprise in the future?

M.A. – What we see is that a lot of industrial customers understand the need for security but don't know how to handle it. They might even hesitate to connect to the Internet. I think that one of our goals as a company is to provide the proper support and infrastructure, also directly in our products, so that they can securely connect to the cloud.

R.D-W. – Indeed, if people fear connecting to the Internet, the benefits that they can get from that are missed completely. In the past there has been this tendency for us in the industry to ask customers what their technical needs were. Actually I think what we should do is ask the questions from a business point of view and then interpret them to make it as easy as possible for our customers.

M.A. – In security, we ask customers to tell us what they want, and most can't even answer that question because they don't know.

R.D-W. – It seems to me that we need to do more in the industry to reinterpret the technical requirements into business requirements and make it clear to people what the business choices or issues are, rather than the technical issues. If we measure it in downtime, saying: "You can save this amount of downtime by doing this," people understand that.

M.A. – Yes, and you can lose face if your systems are hacked. That's the challenge for us as a company providing the components. We must make sure that we do it the right way, by raising awareness and being able to prove to our customers that we have enough security features in our modules and chips to support a secure future. ●

NUMBER OF NETWORK-CONNECTED INDUSTRIAL DEVICES:

1.8^{BN} BY 2020

North America
359.669^M

Western Europe
397.192^M

Eastern Europe
97.603^M



Source: ABI Research, 2015

Note: The network connections can be wired (like Ethernet) or wireless and do not necessarily mean the device is connected to the Internet.

WHAT DRIVES THE GROWTH OF THE INDUSTRIAL INTERNET OF THINGS?

Here are some facts & figures.
Would you have known?



35 %
of manufacturers use smart sensors today
(Source: Business Intelligence)

60 %
of global manufacturers will use analytics to sense and analyze data by 2017
(Source: IDC)

25 %
of the 13 million new IIoT connections in 2017 will be wireless
(Source: ABI Research)

547 ^M
US\$ IoT security spending in 2018
(Source: Gartner)

14.2 ^T
US\$ added by the IIoT to the global economy by 2030
(Source: Accenture)

298 ^{BN}
US\$ in industrial automation device revenue by 2025
(Source: ABI Research)

45 ^{BN}
US\$ in robotics revenue by 2025
(Source: ABI Research)

66 ^M
global IIoT connections in 2017
(Source: ABI Research)

5.4 ^M
IoT devices will be used on oil extraction sites by 2020
(Source: Business Intelligence)

178 ^{BN}
US\$ total operational spending in 2016 makes manufacturing the largest industry in the IoT and the IIoT
(Source: IDC)

EYES IN THE CONTAINER

With the u-blox SARA-R404M LTE Cat M1 module, San Francisco-based waste-tech company Compology improved its wireless container sensors for smart waste management, cutting production costs, increasing battery life, and expanding cellular reception in hard-to-reach locations.

Traditionally, waste haulers working on tight margins have been less likely to adopt new technology unless it is both highly reliable and positively impacts their bottom line. However, Compology's product is a unique and effective application of the Industrial Internet of Things (IIoT) meant to save haulers money. With accurate, up-to-date data on their fleet of containers, waste haulers are able to turn containers faster and eliminate unnecessary pick-ups. By more efficiently utilizing trucks and containers, haulers can increase profits through reduced fuel usage, less truck wear and tear, and increased turns, all while improving environmental-friendliness through reduced traffic and fewer greenhouse gas emissions.

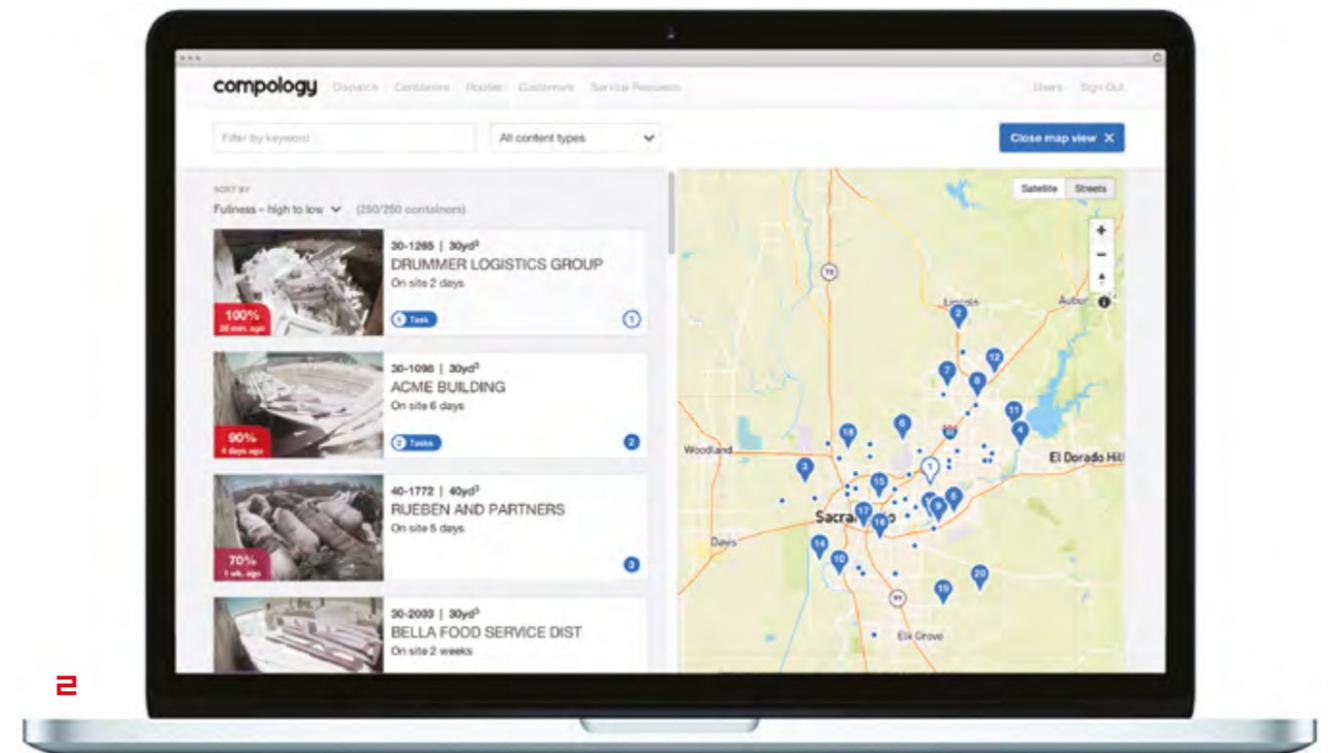
So how did Compology strike the right balance of creating an affordable, low maintenance sensor, while also providing a high-quality product waste haulers would benefit from? In part, through implementing u-blox's SARA-R404M LTE Cat M1 module for cellular communications.

In April 2017, Verizon introduced its LTE Cat M1 network across the USA, a low-power wide-area (LPWA) cellular technology using LTE low speed, paving the way for countless IIoT applications. As one of Verizon's Cat M1 partners, u-blox was ready, early on, to give its customers access to

the network with its SARA-R404M LTE Cat M1 module. Designed for low-power consumption, the module's long battery life effectively minimizes maintenance operations. Extended range in buildings and basements further ensures that data can be transferred from almost anywhere. With its competitive price, the module offered Compology the low-cost, high performance solution necessary to meet their wireless communication needs.

For their latest sensor, the R12, Compology traded in the high speed LTE Cat 4 cellular module they had been using to transfer data for the newer LTE Cat M1 technology. This, says Ben Chehebar, Co-Founder and Chief Product Officer at Compology, brought significant improvements to the services they were able to provide to their customers, while also reducing Compology's costs:

"Our goal is to consistently improve the performance and reliability of our sensor, while also reducing our overall hardware costs. The move to the SARA-R404M LTE Cat M1 module made sense for us as it allowed us to save 50% on the cost of the module and drop a D-cell from our previous battery pack – thanks to the 40% reduction in power usage from the module – without losing performance. And, we now have improved reception in hard-to-reach locations." ●



1 Compology's container sensors send data on the fullness of waste containers to the cloud.

2 Using Compology's smart waste management platform, waste haulers can eliminate unnecessary pick-ups.

LEARN MORE:
www.compology.com
www.medium.com/@compology

U-BLOX CONNECTS THE INDUSTRIES

Combining leading industry-quality, robustness, sensitivity, and performance with innovative features, u-blox offers components and solutions for your designs. We focus on business critical applications for which our customers need our products to perform 24/7 with exceptional reliability and to handle exceptions in a way that minimizes disruption to the overall system. As a result we can offer our customers improved productivity, fast response, and new business opportunities... to locate, communicate, accelerate.

Sapcorda Services GmbH

In August, 2017, Bosch, Geo++, Mitsubishi Electric, and u-blox announced the creation of Sapcorda Services GmbH.

The partners recognized that a new way of offering Global Navigation Satellite System (GNSS) positioning services is required to enable high precision GNSS services for mass market applications. u-blox contributes with extensive knowledge in the field of satellite reception. Sapcorda will offer globally available GNSS positioning services via the Internet and satellite broadcast and will enable accurate GNSS positioning at centimeter level for automotive, industrial, and consumer markets.

LEARN MORE:
www.sapcorda.com



Positioning and wireless technologies for the IIoT

SARA-R4

The ultra-compact 16x26mm SARA-R4 module provides multi-mode LTE Cat M1/NB1 connectivity, as well as the ability to define preferred modes. It is software-configurable to support any global band combination based on a single hardware unit.

Featuring power save features that extend battery life up to 10 years, the module also provides extended in-building and underground coverage. With the u-blox uFOTA client/server solution, critical firmware updates can be delivered using LWM2M. Nested design provides easy migration from 2G and 3G modules to the latest generation of cellular technologies.

LEARN MORE:

www.u-blox.com/product/sara-r4-series



NINA-W1

The ultra-compact NINA-W1 series of stand-alone Wi-Fi and Bluetooth modules offer superior performance and application flexibility. The NINA-W1 professional-grade series consists of NINA-W131/NINA-W132 (antenna pin/internal antenna) featuring Wi-Fi 802.11b/g/n and NINA-W101/NINA-W102 (antenna pin/internal antenna) featuring Open CPU with hardware capabilities, Wi-Fi 802.11b/g/n, and Bluetooth dual mode.

NINA-W1 offers the u-blox connectivity software for out-of-the-box connectivity. The globally certified industrial modules have important security features embedded, including secure boot and enterprise security. This makes NINA-W1 ideal for critical IoT applications where security is important.

LEARN MORE:

www.u-blox.com/nina-w1



Virtual teams are becoming increasingly common in global organizations.

TEAMS WITHOUT BORDERS

Prospering despite the distance.

In global companies, virtual teams, whose members are more likely to meet online than in person, are becoming more and more widespread. u-blox is no exception: acquisition-driven growth and our desire to retain talent have led to 58 of our 148 currently active teams being spread out across multiple sites. Rather than simply dealing with the distance, many have learned to reap its benefits. Obviously, the right technology is critical to making it work. The right personality traits are equally important, not just in leadership but across the entire team. We reached out to two employees who are geographically far removed from their teams to find out how they have learned to prosper despite the distance.



Rod Bryant

Senior Director Technology, Product Center Positioning at u-blox
Line manager based in Canberra, Australia

"I'm literally sitting on the other side of the planet, so when I joined u-blox, the question whether we could make this work did come up. To be successful, remote team members have to be more proactive and to go after the information they need, rather than waiting for it to come to them. Technology makes it easy to keep in touch, which we do in weekly face-to-face meetings and fortnightly group meetings. We also get everyone to sit around the same table for a few days each year to brainstorm on technical problems and deal with the technology roadmap. As everybody else's touch point, I can spot areas that need better coordination. And the fact that I'm in a distant time-zone means I have funny working hours, but it also gives me some quiet time to whittle down my to-do list before people in Thalwil get to the office."



Rick Camarillo

Principal Engineer, Product Center Cellular at u-blox
Technology team member based in San Diego, USA

"About two and a half years after founding Fusion Wireless in San Diego, we were purchased by u-blox, which was great for us. The team I am part of now is mainly spread across Europe. It's been four years since my last trip there, but I stay in touch through a monthly team meeting and one-on-one bi-weekly meetings with my manager. If you are by nature an outgoing person, this type of arrangement might come easy. If, like myself, you are more reserved, you really have to change your mode of operation, actively put yourself out there, and share information or you won't be heard. It's grand that here at u-blox Senior Management gets on a conference call every month to share the company's status. It keeps people informed on how the company is being managed and what is being considered."

LEARN MORE:

www.u-blox.com/en/our-employees



u-blox.com