

# The Future of IoT



# —Contents

- 3. Foreword written by Nick Earle, CEO, Eseye**
- 5. IoT is transforming industries and starting to make its mark on the workforce**  
Navin Arora, Executive Vice-president, TELUS and President, TELUS Business Solutions
- 10. Bringing together people, data, and IoT to deliver the untapped promise of Industry 4.0**  
Vernon Turner, Principal and Chief Strategist, Causeway Connections LLC
- 15. Context, costs, complexity, connectivity and COVID**  
Eric Conn, CEO & Founder, Leverage
- 20. IoT is enabling a whole new business model: vertical value integration**  
Josef Brunner, Entrepreneur, Investor, and Advisor
- 25. If we want the benefits of interconnected IoT, the user needs to be at the centre**  
Ibrahim Gedeon, Chief Technology Officer, TELUS
- 30. We need to talk more about IoT**  
Leonard Lee, Managing Director and Founding Member, neXt Curve
- 34. IoT is key to the super resilient organisation**  
Ade McCormack, Digital Transformation Advisor and Associate, The Møller Institute
- 38. Unlocking the potential of cellular IoT**  
Mikael Persson, Chief Technology Officer, Sigma Connectivity
- 42. Overcoming the challenges of global IoT deployments with eSIM and localisation**  
Steffen Sorrell, Chief of Research, Kaleido Intelligence
- 46. eSIM: creating the perfect storm to accelerate digital transformation**  
Nick Earle, CEO, Eseye
- 52. Visibility and understanding – securing the IoT**  
Peter Doggart, Chief Strategy Officer, Armis

# —Foreword

Written by Nick Earle, CEO, Eseye

I am fond of noting that IoT is responsible for one of the biggest missed predictions in tech. Ten years ago, the industry – myself included – loudly said there would be 50 billion connected things by 2020. In reality, this fell short with only 11 billion and only around 2 billion were cellular connected, the rest were tablets and mobile phones.

This is not for lack of possibility. Many of those 11bn are doing amazing things – transforming businesses and user experience – and many companies are eager to do more.

But having a vision of what is possible in IoT is one thing. Solving the complex challenges that allow you to deliver that vision on a global scale, is quite another.

Transformational IoT means deploying thousands of devices into products and assets, which must then operate in messy real-world environments, outside the enterprise (fire)walls, all around the globe: in people's homes, on remote infrastructure, in transit. They must work seamlessly, conveniently, and without compromising privacy or security.





We have been proud to lead the way in delivering the cellular connectivity that enables many innovative global IoT deployments. But we are only one part of the picture of IoT innovation. We co-exist in an ecosystem of interesting organisations – both providers like ourselves, and enterprises designing IoT deployments – who come together to break down the barriers holding IoT back.

As such, we wanted to take this opportunity to capture the insights of these industry leaders and share them with the IoT community, in the hope they will benefit others, and spark ideas to help solve problems and unlock disruptive innovation.

Our contributors are a diverse group, from technologists to analysts to pioneers and futurists. Their ideas vary, but some things come through time and again.

Innovative thinking remains key both in designing IoT deployments and benefiting from the data they capture. We need to consider the new possibilities and business models that IoT presents, not just how it can make existing things incrementally better.

On the more practical side, our contributors emphasised the need for global deployments to be truly global – i.e., to design IoT devices that work wherever they find themselves in the world, from a convenience, connectivity, and security perspective. To this end, there was much excitement about the eSIM, which promises to address many global deployment issues.

I could rave about the insights in this report, but I will let the contributors speak for themselves. We hope you find these insights useful for your own IoT programme. And if you need help and would like to discuss the issues raised, then I'd love to hear from you.

A handwritten signature in black ink, appearing to read 'Nick', with a stylized flourish underneath.

Nick



# — IoT is transforming industries and starting to make its mark on the workforce

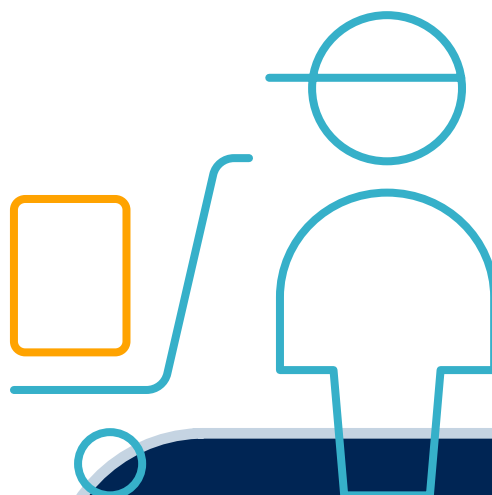
Navin Arora, Executive Vice-president, TELUS  
and President, TELUS Business Solutions



Many businesses have embarked on IoT programmes to improve efficiency and innovation – for example tracking assets, automating checks and maintenance and creating customer-centric products. Some have also recognized how much IoT will be instrumental in ensuring business continuity whilst enhancing employee safety. As the pandemic accelerated virtual work and a more distributed, but also a connected world, IoT will become not just an enabler of productivity, but an enabler of whole new ways of working.

One of the things we're excited about is how IoT can enable a fully integrated 'Connected Worker' strategy. If we could turn workplace devices into connected IoT devices, then people can access many of these remotely. Just as laptops and phones have enabled much of today's "office" work to be done remotely, IoT will offer similar capabilities in manufacturing, logistics and eventually even transport. We're exploring how to leverage technologies, such as AR glasses, which connect workers with experts to facilitate training and improving productivity for activities like vehicle safety checks, factory line procedures and warehouse stock picking. Ultimately, IoT remote assistance tools can help improve employee safety, while reducing the need for in-person or on-site visits.

All of this is a win-win for employers looking to drive greater productivity and efficiency within their operations, and for workers who want greater flexibility in how and where they work. It also ties into another post-pandemic trend, employee safety. If we can reduce the number of people needed in higher-risk environments, such as working with chemicals or machinery, then we can better protect our workforce.



## A more efficient world

IoT has the ability to change the game for every business and industry, and there are lots of exciting IoT deployments underway.

For example, manufacturers are using IoT data to track their parts and finished products in real-time as they move between logistics hubs, which helps prevent delays, minimize costs, better track inventory and detect safety issues. At TELUS, our solutions support thousands of vehicles and assets across Canada and the US, enabling companies to use IoT sensors for real-time visibility of their fleets. With our IoT connectivity management platform, we're helping transportation companies get "always-on" access into metrics when truckers move across long delivery routes. In Agriculture, we're supporting the weather station at the Olds College Smart Farm, an AgriTech 'lab', to provide farmers with real-time data on weather and crop health so they can drive better yields, profitability and sustainability.

If we get the devices, data management, security, partner ecosystems and connectivity right, then real-time decisions and optimized planning can be made on supply chain management, route optimization, engine diagnostics, optimal crop planting times and so on. Ultimately, IoT is going to make it simple and seamless to track and monitor everything and get secure, up-to-the-minute data on how everything is performing.

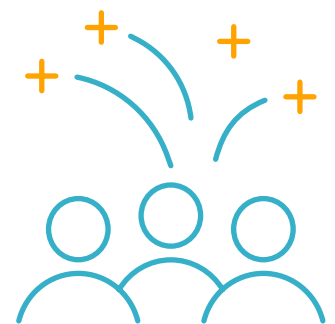
**“IoT is going to make it simple and seamless to track and monitor everything and get secure, up-to-the-minute data on how everything is performing”**



## Empowering people

One of the things that's permanently altered is not only where we're going to work, but how we're going to work. IoT connectivity will drive the kind of efficiency, productivity and speed that simply hasn't been possible before now.

Workers can be set up with a profile that allows them to securely login to workplace systems for a range of devices, so they have flexibility to work from wherever they are most effective – an approach we have as part of TELUS' Work Styles program. It might mean workers in a manufacturing facility access connected devices, such as machine tools or safety sensors, or they could work remotely by connecting new devices specifically to robotics, or connected forklift trucks that can be driven using a virtual reality headset.



A significant opportunity we're seeing for IoT is creating a more connected health care system. For example, through a 5G Living Lab at the University of Alberta, we are exploring how to leverage 5G, AR glasses and video-conferencing in ambulances to enable paramedics to evaluate stroke patients and share critical information with neurologists in real-time.

The more that is done through connected devices, the more we can get richer data-driven insights which enables you to optimize how you run your business and provide tailored experiences your customers and employees expect.



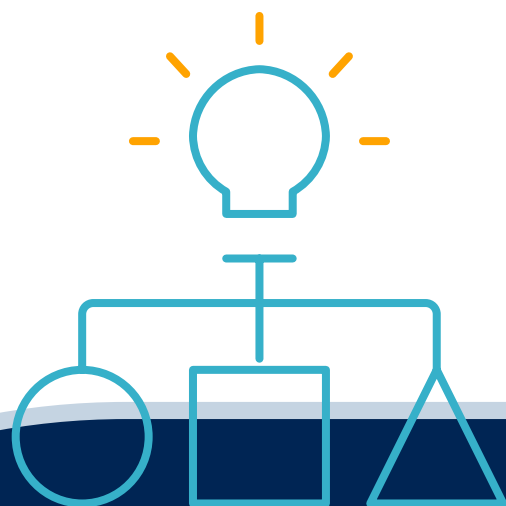
## How to make it all work

To deliver on this opportunity, companies need to think about their IoT connectivity deployment strategy holistically.

This means implementing robust cybersecurity measures, data collection and management, analytics and interoperability between devices, applications and legacy systems.

Driving interoperability in your tech stack can be incredibly complex, so you need a holistic plan and the right partners at the table providing oversight to address connectivity, security, privacy and interoperability from the start. And, of course, this all needs to be designed in a way that aligns with your business goals – whether they be optimizing machinery, operations or enabling a remote workforce.

Getting all this right unlocks huge opportunities to create a hyper-efficient, insight-driven, connected organisation. This has long been a goal of IoT, and as the world becomes more digitally oriented, and as connecting devices becomes more pervasive, the acceleration of IoT will enable you to unlock significant value for your business and workforce.



**“companies  
need to think  
about their IoT  
connectivity  
deployment  
strategy  
holistically”**



# — **Bringing together people, data, and IoT to deliver the untapped promise of Industry 4.0**

Vernon Turner, Principal and Chief Strategist,  
Causeway Connections LLC



Just a couple of years ago, many IoT projects were languishing in Proof of Concept purgatory. Good ideas were struggling to scale. But the tech industry solves problems quickly, and we're now seeing large-scale IoT programmes deliver meaningful organisational change.

But as the deployment nut is cracked, companies are discovering that IoT is much more than just a technology roll-out. It is intertwined with the very fabric of how companies operate. And this needs to be considered too.

IoT has consequences for the complex systems it operates in, and the people in those systems. The next stage of IoT needs to move from 'what can technology do?' to 'how can we combine technology and people to deliver real transformation?'

## The opportunities from IoT-human systems

This 'systems and people' thinking promises opportunities everywhere.

**Two areas stand out as being on the cusp of real transformation: Industrial Manufacturing and Smart Buildings.**

Start with manufacturing. A few years ago, we thought that the sensors and robots promised by Industry 4.0 would solve everything. But whilst they have delivered efficiency gains, the promised transformation hasn't materialised.

The reason is that industry still needs human expertise, and this was rarely considered. The real transformation will come when we recognise that these technologies must fit into and augment human systems. I am calling this 'Industry 5.0'.

An example would be augmenting human skills that cannot be done by machines. IoT sensors can monitor industrial machinery and human interactions with it. This data (alongside things like maintenance logs) can be fed into machine learning models, which learns the solutions to all the different problems any given machine will face over its lifetime. This model can then be turned into digital tools that guide the worker through the solution.

The upshot of such a system would be that, when a problem arises, the right person is assigned, they are provided with the right parts, and presented with the best solution via their phone or tablet.





In this way, employers harness technologies to get the best from their people, reduce onboarding times, create flexible workforces and fill skills gaps in unsexy areas of manufacturing that are increasingly hard to recruit for.

Smart buildings face different opportunities, but similar challenges at a top-level. Covid has changed working patterns and so builders and facilities managers need to get creative to make their offices attractive or find new uses for their space.

Air quality and temperature sensors have long tackled isolated problems. But these are incremental improvements, not a reimaging of work. The big opportunity is to bring together the whole ecosystem around the building. For example, could we integrate building management with ridesharing, offer employees an easy route in, and use the resulting data to manage capacity? Could retail outlets combine data from IoT sensors on trains to predict peaks in demand and deploy staff accordingly?

**“By using IoT to gain insights into complex human behaviour, then feeding that back into human decisions, we can truly deliver new ways of working and new value.”**



This idea of 'technology + sensor data + humans' is not entirely new. 'Human-machine teaming' has been an important aspect of military innovation programmes since the value of connected technologies became clear. For examples of success, this would be a good place to look.

## Deploying integrated transformational IoT

Two things link the different use cases above. Firstly, the user is at the centre, and the focus is on making their lives easier, so they can deliver more value. Secondly, success means creating workflows across boundaries. This means collecting reliable IoT data at scale, across different areas – some of which may be disjointed or siloed – and integrating it to create value greater than the sum of its parts.

How do you do this?

Firstly, you need quality IoT deployments throughout that collect the data you need.

The key to good data collection is good connectivity. If you are using machine learning to model the reality of complex human-machine systems, you need the sensors measuring those systems to be perfect.

For such a complex data ecosystem to work, you need to remove the complexity of connecting any device anywhere in your ecosystem. IoT needs to connect, create, and scale. The faster devices drop in, connect to your network, and start delivering data into your cloud platform, the faster the time to value.

Another challenge is bringing all your data together. There is obviously the technical challenge of combining diverse data sets into something meaningful, which needs specialist data skills. But there is also the organisational challenge of actually accessing data from different sources across – and sometimes beyond – your organisation.

**“The key to good data collection is good connectivity”**

Some suggest a marketplace for data would provide a solution. But these have tended not to work due to complexity and lack of clear leadership to drive things forward. Instead, the responsibility should fall to the 'vendor closest to the customer'. This can be literally a commercial relationship, but it can also be an employer delivering something for their employees.

Either way, they should set up a single data platform that sits at the centre of this ecosystem. This should include establishing processes, permissions, and APIs for all necessary data integrations, either directly from their own IoT devices, or from other's devices or platforms.

Finally, the end product – where the output of your data insight is presented – needs to be designed around the user. The endpoint may be an app, AR/VR glasses, a complex piece of software, a robot, or any other connected piece of technology. Whatever it is, it needs to be designed around the people it helps. It must understand how they interact with the system and be able to communicate directly to nudge or guide their decisions.



## The promised IoT transformation

Solving all this allows for transformational innovation. Once you have reliable data coming in, you can start to connect up systems to aggregate data, add layers of ML/AI to build insight, and deliver that insight to people through connected endpoint devices.

Smooth integration across this system is critical. Over the last couple of years, we have learned to do this well in a technology landscape. Now we need to learn to do it in a technology-human landscape. If you solve this integration complexity, you solve the innovation problem.





# — Context, costs, complexity, connectivity and COVID

Eric Conn, CEO & Founder, [Leverage](#)



## Asset tracking emerging as huge IoT opportunity

I'd say asset tracking is one of the big business opportunities in IoT. But it's about more than just knowing where an asset is. If the cost and friction were low enough, everyone would like to know the state of an asset and the environment around it. Context around why something is where it is can offer valuable insights.

Take the example of a hospital administrator looking for an IV pump. They learn that it's in room 316, but they already know that room is where the equipment waiting to be cleaned is kept. Imposing this context onto the pump's location allows them to assume it's a piece of equipment that can't be used until it's been cleaned.

More context is made available by the fact that most of the sensors used to detect an asset's location tend to be bundled with other, typically inexpensive environmental indicators. So not only can we know where an asset is, but we can know its state at any given time. And looking at past behaviour allows us to start predicting where and how things might be in the future, as seen in predictive maintenance.

Essentially, by telling people where their assets are, overlaying this with business logic and sensor feedback, and putting all this information on a timeline, we enable them to make informed decisions. And this is where I believe the biggest opportunity lies for IoT. There's not an industry that wouldn't want to know the state and location of all its assets.

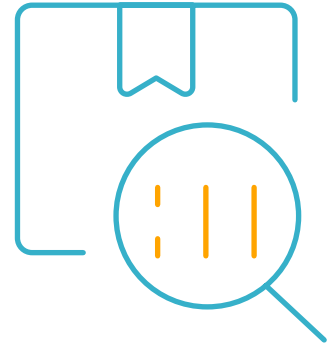


## The benefits of combining IoT data with contextual information

There are several benefits, both internally and externally.

We can use the hospital example to illustrate some of the internal benefits. Medical equipment is very expensive - a fully functional IV pump can cost \$20,000. But not knowing how many of these pumps there are, or where they're located, is not only bad for patient care, it's bad for hospital administrators trying to reduce costs. And without usage statistics, it's hard to know how long these devices last, making it difficult to decide whether to buy one or just lease it.

So, better operational efficiency, better asset usage and better decisions around buying versus leasing – these are just some of the internal benefits of IoT.



The biggest external benefit is a better customer experience. We've all become accustomed to always knowing what's happening with any service we buy. We don't like not knowing how long something's going to take – you can't plan your day around the service providers. It should be more customer-centric.

IoT can switch this around. It enables service providers to give consumers an insight into what's happening and plan their day accordingly. Uber is an example of this approach at its best. Traditionally, you wouldn't know exactly how long you'd have to wait for a cab. With Uber, you order a car, and the app tells you when it'll arrive to within minutes, with live updates. You can finish your coffee or make that call. It's a level of service taxi firms just can't provide, and it is why Uber has entirely disrupted the industry.

It represents new revenue streams, too. People are willing to pay more for better service because they're buying their time back. Taking real-time data out of previously opaque settings and using it to give insight to consumers is a huge win for any business.



## Making the math work for mass asset tracking adoption

It's being driven by what I call the ratio of IoT costs to "actual asset you want to know about" costs. It's worth putting a \$20 sensor in a \$20,000 vehicle to be able to know where that vehicle is. But it makes no sense to pay \$20 to track a \$100 item.

You have to make the math work – it has to be cheaper, better, and provide more insights and revenue than human labour. If you can't do that, no business will adopt it. You have to drive those costs down to as close to zero as possible so businesses will see the benefit and the ROI. Focus on cutting every penny out of every single cost – hardware, connectivity charges, cloud usage – the whole end-to-end lifecycle of providing a solution at the lowest possible cost.

## Reducing the cost of IoT to allow scale across more assets

Cost relates to complexity – firmware development, writing the software that runs on the devices, connectivity, just to name a few examples.

Of these, connectivity is probably the biggest challenge today. Without reliable connectivity, you're operating in a blind spot – it's hard to know the state of a device if it can't speak to you. Data, delivered by connectivity of any type, is critical to decision-making. Without it, you can't have a functional IoT.

But, whether it's a private or public network, there are many issues. Interference, licensed versus non-licensed bands, different RF environments, even weather effects – so many things can affect connectivity.

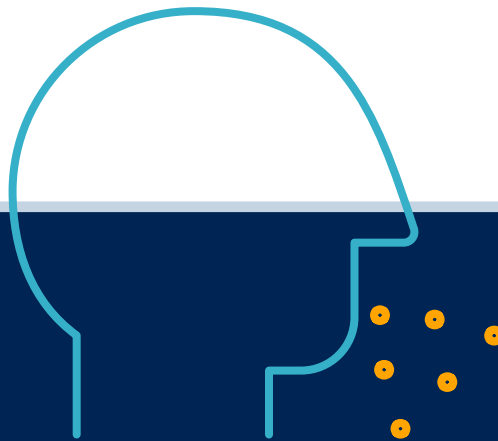
Fortunately, there are innovations like nanosatellites that will provide global connectivity. And, although they operate at low data rates, they're also driving the cost of satellite connectivity down, and unlocking new use cases. And of course, Virtual Mobile Networks are creating affordable global coverage by allowing connected assets to automatically join the best local network wherever they are in the world. It's a trend that will continue to improve. By solving the complexity, you're reducing the cost.

**“connectivity is probably the biggest challenge today”**

## The effect of COVID on the progress of IoT

COVID was a watershed moment. After everyone recovered from the shock of the first six months, when we all started working remotely, they woke up to the fact they couldn't hang out with their colleagues or walk around the factory. Rather than going to the data – the interactions with people, the business, its metrics – they had to find a way of bringing that data to them. They realised they wouldn't stay in business if they couldn't figure this out.

That is exactly the job of IoT, and this has been a great tailwind for the entire industry. IoT has followed the typical route of most buzzwords – peak excitement about five years ago, followed by the trough of disillusionment. It's on its way up again now, though, and that's certainly been helped by the pandemic. It's a silver lining after a difficult time.





# — IoT is enabling a whole new business model: vertical value integration

Josef Brunner, Entrepreneur, Investor, and Advisor

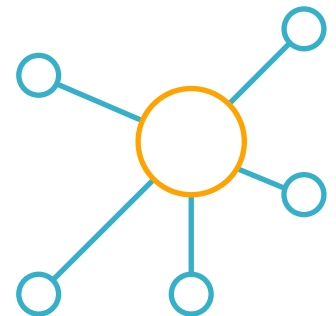


From its inception in 1877, The Bell Telephone Company, acquired companies in all parts of telecommunications – telephones, cables, exchanges, parts, and so on – giving it a competitive advantage that let it dominate the American telephone industry for 100 years.

This strategy, known as vertical integration, optimises efficiencies at every part of the supply chain, allowing tight cost control and delivering a convenient one-stop shop to customers. But it comes with risks. In 1983, Bell, then part of AT&T, was broken up by trustbusters.

Nonetheless, control of your value chain has advantages. Thanks to IoT, a new business model is emerging which deliver many of the benefits of vertical integration, without the complexity of owning lots of companies or attracting the attention of governments. We call this Vertical Value Integration.

By integrating data from IoT into clever software platforms, it is possible to combine a wide range of capabilities into a single product offer. It is not full ownership of the supply chain, but a set of arrangements – all made seamlessly possible by digital technology – that optimise efficiencies behind the scenes and allow you to deliver a one-stop shop for exactly what your customers need.



**“By integrating data from IoT into clever software platforms, it is possible to combine a wide range of capabilities into a single product offer.”**



## An example of Vertical Value Integration

To understand Vertical Value Integration, imagine you are a company that makes steel cutting machines. In the distant past (10 years ago) you would have just sold machines to manufacturers. More recently, you probably lease machines and bundle in service contracts for a monthly fee.

You can go further. You can look at your customers' supply chain and ask where the inefficiencies are. Your customers have your machine and a service contract, but they still have to buy the steel and the storage from somewhere else.

What if you went to all these other parties, agreed to deals with them, and sold it as one bundle? What if you used IoT and software to monitor usage, order supplies, and manage billing?

All this oversight lets you come up with innovative pricing models. For example, you could charge them for what comes out rather than what goes in – so they pay a fee for each steel product they make, giving them total cost control. From the customer's point of view, it's a free machine with a single contract for everything, and guaranteed capability, where they only pay for what they need.

That creates a value proposition that is hard for a customer to refuse and a business relationship that is hard to leave. Many will pay a premium for this convenience and certainty. It also allows efficiencies and price optimisation behind the scenes. If you move now, you may have a first-mover advantage, before your competitors cotton on to this business model.

In fact, this is exactly what Relayr is doing right now through a partnership with the manufacturing technology company, TRUMPF, and steel distributor Klöckner & Co. We believe it is the first business model of this kind.



## How to create Vertical Value Integration

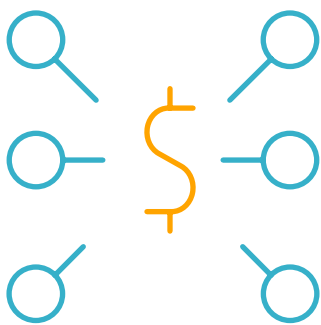
How should you approach creating such a business model?

Start by asking “how can I make my customers more successful with my products or services?” Look at how they use them now, and where the inefficiencies lie (e.g., parts and supplies, shipping, availability, idle time). Look at how industry trends (sustainability, personalisation, etc) are changing their business needs.

Then consider how you might repackaging your offer to be more complete and more convenient, where the customer only pays for what they need.

Then comes IoT, which makes this whole business model possible. Ensure your fleet of machines is equipped with the right sensors to capture the data you need about machine usage and behaviour and has reliable connectivity to continuously feed this data back.

With this data you can build a backend system that monitors usage, manages billing, schedules services, and raises orders for supplies (supported by some simple oversight app that allows orders to be checked and approved). This is all managed seamlessly in your own cloud.



## Isn't taking responsibility for everything a bit risky? Not with IoT.

If you are a responsible business owner, you might now be thinking that this all sounds a bit perilous. Taking responsibility for guaranteeing uptime and materials transfers a lot of risk to your balance sheet.

But this is where IoT changes the game again.

If your fleet of machines is equipped with the right sensors and has reliable connectivity to continuously feed this data back, we can build predictive models of how the machine and the surrounding processes work.

These give a very clear idea of how the machine will be used, what revenue it will generate, and how frequently interventions will be needed. This is essentially a function of uptime and reliability.



**IoT changes the game”**

With this data, we can project revenue and costs across the entire fleet. This can be used to set pricing to guarantee sustainable revenue.

More critically, this predictive data will let reinsurers quote to cover your risk. So, you can take all that risk off your balance sheet and create a very secure revenue model.

All of this depends on reliable IoT connectivity to transmit the data back to your cloud, where you host your models. This must work regardless of where your machines end up – whether a state-of-the-art automotive factory near a city or a rural mom-and-pop contract manufacturer. Customers not connecting their machines to a network is one of the biggest risks to this model, so designing simple setups and ‘out of the box’ connectivity, is key to success. If you don’t have reliable data at scale, there is no prediction and no value.

## More than a technology project

Realising all these benefits will mean some changes to thinking. This is not an incremental change to a leasing model. Nor is it a technology project where you stick in some IoT and see whether the data is useful. It is a new business model and needs to be approached top down.

Look at the market and your assets and ask whether new models such as vertical value integration will serve your customers better. Then ask whether they can be delivered in ways that are profitable and suitably low risk. When you have agreed on your business model, that’s the time to strategically deploy the digital technologies to enable it. This is not an IoT project, this is a business transformation project enabled by IoT.



# — If we want the benefits of interconnected IoT, the user needs to be at the centre

Ibrahim Gedeon, Chief Technology Officer, TELUS





In many ways the modern world is amazing. Thanks to a series of affordable connected technologies, I can come home, choose my lighting mood with an app, play music through my speakers through another app, set my thermostat with another.

If I were to tell this to myself twenty years ago – a time a department store salesman once tried to sell me remotely operated curtains for \$30k – it would all seem incredible. And yet, it is all still hugely inefficient.

All these devices are made by different companies and have different setups. Each needs to be registered, and each needs a different app. Right now, you might have a Google or Sonos app that finds all your devices in their ecosystem, but not in others. You might have a Wi-Fi connection that can see all the devices on that network, but not on Bluetooth or cellular. Often things that could, or should, integrate don't. You end up with a hotchpotch of IoT devices.

That isn't very pleasant now. Imagine how it will be when every bit of your home is connected – you will have a choice between endless apps or locking yourself into one vendor.

This will hold back IoT significantly. IoT is not a single point, it is an ecosystem. Whether you are setting up a smart home, or building an IoT enabled healthcare business, or rolling out industrial equipment, all your connected devices need to just work out of the box. And not just in its own right, but in ways that integrate with all the IoT devices around it.

That requires some changes.

**“IoT is not a single point, it is an ecosystem”**



## The user, not the device, as the authenticator

The idea we propose is to create a platform that is owned by 'the user', to which any IoT device can be linked.

It's a bit like a computer operating system. It provides the ubiquitous platform for apps to be installed upon and has all your basic data so new apps can be installed without having to go through lengthy setups every time. It also allows data sharing between them, so for example a shopping app can talk to a payment app, or a virtual assistant can talk to the calendar app. It doesn't matter that these apps are all from different providers.

Such a platform would contain protected data that IoT devices need to operate and certify, which would all be helpful in the cloud and provide secure protocols IoT devices to talk to each other. All of this is done in the background, away from the device, keeping data safe. The user would still be free to use whichever smart home app they prefer, but their devices – lightbulbs, speakers, thermostats - would be able to easily talk to each other via the platform. And all data could be easily switched if you wish to change to a different app – so you avoid vendor lock-in.



## How to create user authentication

Creating this platform depends on connectivity solutions that enable it.

The user must first be authenticated, which could be done through a network provider like TELUS. This lets us create a portal based around a user profile, not a device or the brand. Then we can partner with IoT device OEMs. We are not the only player who can do this and if everything is open, the user has a choice. Business will be won on who has the best experience and partner ecosystem, spurring companies to focus on customer experience.

Then IoT devices need a way of authenticating against the user so they can join their profile. The eSIM offers a solution. As Nick Earle discusses in his article, the eSIM can be embedded in any device and makes managing connectivity simple

regardless of where it is in the world. It offers an option to manage device connectivity and a tool to authenticate the user onto a network.

eSIM will revolutionize the IoT connectivity value chain. With eSIM and, more specifically, an eSIM management platform, local network connectivity for a device can be maintained independently of region or country. IoT customers can now engage with a single service provider like TELUS that supports local connectivity and cost certainty in any market, enabling globally connectivity for those devices.

Next, devices need to be able to talk to each other. All IoT devices should be built on open platforms and standards and publish APIs so that devices can sync up. And you need partnerships between them. If this is sorted all devices can communicate via the platform.

**“The eSIM can be embedded in any device and makes managing connectivity simple regardless of where it is in the world”**

## A foundation on which to build a connected world

If we deploy this, any IoT device you buy can be set up so the eSIM (or another method of connectivity) quickly authenticates to your personal platform – e.g., via your phone which just requires your PIN or face scan. This can happen regardless of the network whether it's using Wi-Fi, or wireless connectivity like 5G that will allow for unprecedented and greater quality of service and even more secure and efficient connectivity - it can then talk to any other device on that platform, regardless of how each is connected or what app they are controlled by. This simplifies onboarding and opens new opportunities for apps to work together. You can then build a family of technology on top of it.

This is not just for homes and individuals – in fact, the real value is in business and government. Cities can set up a platform where the user – e.g., the city council – is the authenticator. Then all their connected parking meters, EV chargers, environmental sensors – even connected bins – can all just use their eSIM to authenticate onto the city's profile and all share data and interact. This would feed into a front-end interface that allows users to monitor trends and connect systems to improve city experiences.

This is good for the user, but also good for innovation since anyone can design a new IoT device, which can just drop into a standard portal which then manages secure authentication and connectivity. We avoid the situation we are in with, say, Facebook where they are so entrenched that many companies are obliged to work with them. We also open IoT to a wider audience who may not be able to afford the big brands and want lower-cost lower-frills options that can be developed once the system opens up. This is the democratisation of IoT.

An analogy can be made to cloud computing. In the old days, a business would need to have servers and computers and devices and be clocked into one operating system. The cloud let them build whatever they wanted on someone else's infrastructure with near-zero CAPEX. That removed barriers to entry for many businesses. An open IoT portal would do the same.

The current system is built around complexity and protectionism, and it shouldn't be. We have seen where this leads. Companies can hold on to their protective models for so long and then something comes along – like the cloud did – which makes everything blow the old models out of the water. This will happen with IoT sooner or later. Given the benefits to business and the user, sooner would be better.





## — We need to talk more about IoT

Leonard Lee, Managing Director  
and Founding Member, [neXt Curve](#)



## The industries doing IoT really well

Oil and gas have always been on the leading edge of IoT. Sensors on drills allow oil rig operators to detect changes in rock structure and pressure, helping them to predict potential problems, for example. The healthcare industry is on top of it, too. Connected wearable devices have been used for some time now to remotely monitor the health and safety of vulnerable patients.

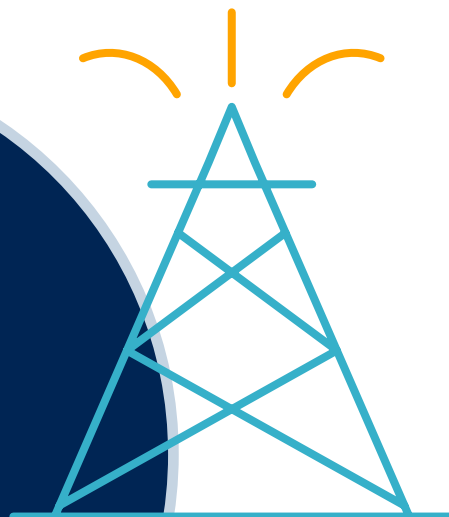
It's not simply a question of whether they're good at it – they've actually been doing it. And as the technology gets cheaper for them, and the endpoints more robust, they're able to do even more.



**Oil and gas continue to push the envelope of what can be done in IoT.”**

That's why these two industries in particular make interesting studies for any other industry that's looking at how IoT can not only improve operations, but also drive new products and services, and enable new business models. These aren't hypotheses – they've gone through those back-end transformations themselves. You can observe what they have actually done with IoT and the outcomes.

When you look at the state of IoT adoption today outside of these industries, we're not seeing the massive numbers everyone might assume we would – even post-pandemic. There are certainly enough drivers, but maybe there aren't enough people that understand what we can really do with IoT. For too many people, it's still a buzzword.



## Lack of understanding holding things back

I think the biggest thing holding back IoT right now is the way we talk about IoT. As long as it's weird and confusing, no one will buy it.

A lot of companies looking to sell IoT are struggling to figure out how to help people understand what it is. Interestingly, a lot of "IoT companies" themselves have a fragmented understanding of what IoT is. People often conflate IoT and AI, for example. Some IoT data does indeed go into the cloud and enables cutting-edge AI, but IoT itself does not automatically deliver AI, so it needs to be clear what part of that picture it is serving, what it isn't, and what else is needed on top of IoT to deliver value. But also, this isn't the only use of IoT, sometimes it's just about knowing where things are or being able to do important firmware updates over the air, and there's no need for anything more sophisticated than a connection to the device.

So IoT companies have to figure out how to become part of the solution conversation – and that will be different for different customers – rather than just the technical enablement solution. They have to work out how to speak to business people who are actually going to fund any significant project outside of what a CIO or CTO might buy into.

## A question of education

It is a question of education on all sides.

It's about educating vendors on how to wrap their technology in a business value proposition, how to target it based on opportunities, and how to develop the experience and competency to do that in a very bespoke way.

IoT vendors need to make all the technical jargon easy to understand, and handle all the technical aspects customers want, like integration.

The end-users – businesses in digitally transforming industries like health or energy – on the other hand, aren't obliged to learn anything. The only thing they need to know is how to translate this IoT stuff their consultant keeps talking about into business value. They want to know about the simple things that IoT does that matter most to them, such as improving the visibility of their assets or enabling predictive maintenance.

Ultimately, it all boils down to someone communicating the really simple principles that can often be obfuscated by technical detail.



**“IoT vendors need to make all the technical jargon easy to understand”**

## Appreciating the role of connectivity in enabling IoT

I think the importance of connectivity is often underestimated.

When you look at the broader context of an IoT solution a company is delivering or piloting within their enterprise, or across a product line, the role of connectivity can often end up being overlooked. This is really a short-term view, though.

When you look at the longer-term cost of actually building the solution out, connectivity is there as a recurring cost of operating the solution's critical infrastructure, and this needs to be factored in if you want a good IoT offer. At the end of the day, businesses need to perform a cost-benefit analysis to ensure they have the level of connectivity they need for an effective long-term solution.

Again, it comes down to education. People like building cool devices. But the underlying connectivity service has to be there, or it won't work for the user. And that costs money, because connectivity infrastructure is not cheap, especially if it's private. But without connectivity, none of it works.

To deliver the kinds of use cases I talked about in healthcare and oil and gas, businesses need to focus on what it is they're trying to solve, what they're to improve, and how IoT – and connectivity – will play into that. If there's a message to vendors that are trying to sell IoT to enterprises, it's to help them understand exactly that – in plain English. That's where the value lies.







## — IoT is key to the super resilient organisation

Ade McCormack, Digital Transformation Advisor  
and Associate, The Møller Institute



The post-COVID world is chaotic. People are more distributed and diverse, geopolitics is changing, consumer and business trends are in constant flux.

Against this backdrop, the old model of business is no longer good enough. Companies operating in the physical world cannot rely on industrial-era models of long cycles of creating products, building a factory to make them, and selling it through distributors. They need to be faster and smarter.

This rapid innovation approach has long been the paradigm for businesses such as Google and Amazon, who constantly monitor customers' online behaviour and respond to the slightest change in near real-time. This ability to sense and adapt has made them super resilient organisations.

Now IoT is enabling companies operating in the physical world to do the same. By connecting their products and assets, old school manufacturers can have real-time relationships with customers, users, and employees. They can use IoT data to sense concerns that may alienate customers or opportunities that may bring new ones in. The leading organisations of tomorrow will become like living organisms, constantly sensing and responding to their environment.



## What does the super resilient organisation look like?

Innovation can be small product tweaks or major new launches. Some sensing will simply be spotting problems and reacting quickly. If you notice your devices have low use in certain areas, perhaps there is a connectivity problem you need to quickly address. If you see unusual behaviours, it's your chance to dig into those and tweak products.

But the super resilient organisation also does new innovations rapidly. This means using IoT to spot new opportunities.

For example, a connected fridge may provide data that—with the right analysis—reveals valuable insight into how people shop and cook. This may reveal a need for other connected kitchen products and provide a direct channel to sell them to people who need them. This may also present new collaboration opportunities with food and drink companies, or whole new business lines.

IoT also supports the innovation process itself. When launching a connected device, you can quickly beta test a prototype in the real world, instead of the artificial environment of focus groups. You launch a small run and monitor how it is used by real customers, allowing you to tweak it before the full launch – much as companies like Facebook do before fully committing to new online offers.

Some companies already do this well. Google Nest learns about the user and adapts accordingly and uses data it collects on user behaviour at home to develop new smart home products. Rolls Royce uses IoT data feeds from jet engines to monitor its products for issues so it can respond rapidly, whilst also feeding that data into R&D to create improved engine designs.

But sadly, outside of the tech giants, few big companies are getting this right. Too many are trying to recreate the safe world of 2019 with long term stable strategies when instead they should be becoming fast-moving and adaptive.

It would be premature to declare strategy dead. But certainly, strategic plans need to be reconsidered, or at least augmented, with real-time situational awareness. Company strategies should become more like military strategies – an overarching plan which has self-preservation at its heart. A plan which sends scouts to assess a constantly changing hostile environment and is ready to change the moment something new is discovered. As the military adage goes, 'no plan survives first contact with the enemy', or as Mike Tyson said, 'everyone has a plan until they get punched in the mouth.'

## IoT – the sensors of the constantly sensing organisation

IoT is the front end of this change towards a situationally aware organisation. It's like the military scout, or a gazelle on the savanna constantly ready to respond to a threat. When embedded into your products and infrastructure, IoT gives you a constant feedback loop on its environment and its user's behaviour.

This opportunity is often not well understood. Too often, companies see IoT as functional, as a way to spot machine problems or stock getting low. This is fine and necessary. But few go a step further and set up processes for feeding this IoT 'sensing' data into high-value decision making. As a result, they miss opportunities to deliver new value to their customers – opportunities their competitors will eventually see.

## How to set up a super resilient organisation

Making all this work will need new organisational setups. One way to do this would be for the IT department to evolve into a listening office – like a signals agency, an internal GCHQ. They would have data management and analytics tools to capture data from their global network of connected products and assets and measure changes in the environment, customer behaviour, and sentiment.

This data must then be turned from information into knowledge and eventually wisdom, by deploying data, business, and subject matter experts to look at what the data is saying and use it to spot opportunities.

The key to this is implementing tools and processes to share information with the right

**“IoT is like the military scout, or a gazelle on the savanna constantly ready to respond to a threat”**

people throughout the organisation. So, a signal that a product develops a fault after a year needs to be conveyed directly to the person who can update the design to fix that fault. A new market opportunity needs to be directed straight to a small, agile innovation team, not channelled through layers of corporate decision making.

## Leadership in a 'sensing' world

In this newly chaotic world, leadership needs to understand the pace of change. Innovation often does not sit neatly in old school organisations, which are sometimes more interested in doing the same thing more efficiently, than taking risks and trying new things.

Organisations need to get better at collecting data, understanding it, and acting upon it to deliver innovation. And innovation itself needs to move from a siloed department to the engine of the organisation.

Not everyone will succeed. As we emerge from the pandemic, many big companies are reaching for old security blankets of corporate strategy. But those that embrace this connected, data-driven world, who use IoT to sense and respond to opportunities, have a chance to leap ahead of the competition. Now is the perfect time for smart leaders to steal a march on their cautious competitors.





## — Unlocking the potential of cellular IoT

Mikael Persson, Chief Technology Officer,  
[Sigma Connectivity](#)





2021 is the first year in which the volume of cellular IoT usage has been on a par with mobile. And its growth is likely to continue – particularly in narrowband IoT (NB-IoT) and Cat-M1, a low-power wide-area (LPWAN) cellular technology that is built specifically for IoT projects. Interestingly, this usage was expected to slow during COVID but, in fact, the opposite was true. Working from home, many people invested in the same type of equipment they used in the office, which led to an additional push of at least 10 percent.

Nonetheless, implementing an IoT deployment isn't as straightforward as many think, especially as we move closer toward 5G. It's important for a company to know whether, when they deploy their devices, they'll work well in certain countries, and not at all in others. But it can be very hard, for smaller companies, in particular, to find specific information on networks in different countries.

Dealing with different operators around the world can be challenging – a company with 1,000 devices won't receive the same attention as Apple, Sony, or Samsung. It's tough from a business perspective, too. Developing, deploying, and owning a cellular IoT network can be expensive, and that's without factoring in licensing fees.

And most companies are unable to test everything everywhere. While it's easy for companies to carry out field testing in their own country, it becomes complicated when they want to sell into 30 different countries.

Virtual network operators can help overcome a lot of these problems. But even they aren't always able to ensure all the features needed to operate a particular device effectively in a particular region. Connect the same device to three or four different networks in Sweden, for example, and you'll get three or four different levels of performance.

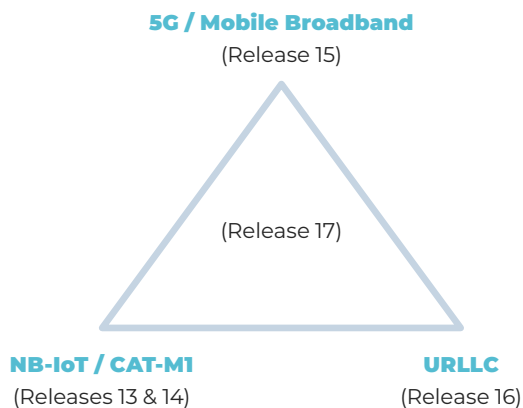
Roaming can be an issue, as well. Of course, if a company knew exactly which countries its devices should work in, it would be possible to check the rules. But when some countries issue a financial penalty for non-compliance with roaming regulations, while others have banned it altogether, not knowing is clearly problematic.

The area of cellular IoT is currently very fragmented. However, it's hoped that Release 17 of the 3GPP mobile broadband standard – the third release of 5G specifications with a key focus on enabling cellular IoT for 5G – will, in time, help to ease many of these issues.

**“Implementing an IoT deployment isn't as straightforward as many think, especially as we move closer toward 5G”**

## Best of all worlds

This diagram is a simplistic view of how things will connect in the future:



Communication IoT devices with a lot of throughput and data, consisting mostly of automotive and mobile deployments, will be located toward the top; devices that consume very little data, such as utility meters and sensors, will be in the bottom left corner; and devices that require greater stability, such as intelligent transport or critical infrastructure, sit in the bottom right corner. But 99 percent of all IoT projects want to be in middle, enjoying the best of all worlds. This is where Release 17 will be located – promising flexibility in terms of reduced requirements on the device side “RedCA = Reduced capability”.

With each release comes additional features. In addition to URLLC (Ultra-Reliable Low-Latency Communication), for example, Release 16 introduces V2X – vehicle-to-everything communication – which is hoped will prevent a large number of automotive accidents, while



the introduction of satellite-based positioning, offering at least the same performance as GPS, should save power by not actually requiring GPS.

But experience shows that even when Release 17 becomes available – in around two years' time – it will take another four years before it's fully operable. Every release – from 2G on – can take several years to sufficiently mature. NB-IoT and CAT-M1 were released around four years ago, and only now are they starting to become stable. When it is up and running, though, it's hoped that Release 17 will truly unlock the potential of cellular IoT.

## Connecting everything that can be connected

Cellular IoT is growing, but that growth doesn't come easy. New developments in connectivity, and new 3GPP releases will further enable this, though, and Release 17 in particular which is expected in 2023.

Now, of course, we're on 5G, and in around seven to 10 years' time, there'll be 6G, which will bring added bands and functionality. By this time, 5G will be the mainstream network, and everything that benefits from being connected will be connected. But with 6G expected to improve throughput by about 100 times compared to 5G and cut latency by a factor of 10 – that's 100,000 nanoseconds, compared to one millisecond today – the efficiency it represents is almost unimaginable.

It's a huge and exciting plan for the future, and it's the basis for the growth in IoT we're expecting to see, and for an easing of the current challenges in deploying cellular IoT.





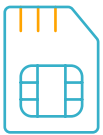
# —Overcoming the challenges of global IoT deployments with eSIM and localisation

Steffen Sorrell, Chief of Research, Kaleido Intelligence



Since the beginning of the pandemic, IoT adoption has shifted up a gear. Companies who previously hadn't considered it, and perhaps didn't understand the concept, have begun looking into what it could mean for their business.

Cellular IoT, in particular, although accounting for a relatively small proportion of overall IoT connections, offers reliable connectivity and certain guarantees in terms of a mostly licensed spectrum. In fact, no other wireless technology offers the same deployment scale for IoT projects, because cellular allows connections via mobile networks that exist globally, rather than relying on people's Wi-Fi connections or pairing to a phone – options that are widely but by no means universally available, or desired. Advantages like these have led to increased interest in cellular IoT versus other connectivity technologies.



But, as the demand for connectivity and connected devices continues to grow, it's important to understand that unlike with mobile, where you can pick up a phone and add a SIM, there are complexities to manage when connecting an IoT device.

For one thing, there are hurdles to overcome in terms of whether the device is able to roam, which may be subject to different local regulations, and risks might arise further down the line. Phones – and many IoT devices – use a roaming SIM and rely on a local operator's roaming agreement in the hope that it provides what is required.

But even the largest operators have constraints around that footprint. They also have constraints in terms of the quality of service (QoS) they provide their customers. An IoT application such as a real-time health monitoring device may have specific QoS requirements regarding low latency, for instance, or the country in which the device is operating may have regulations concerning cross-border data flows or permanent roaming. Either way, the traditional roaming SIM model doesn't really work as a catch-all for IoT devices.





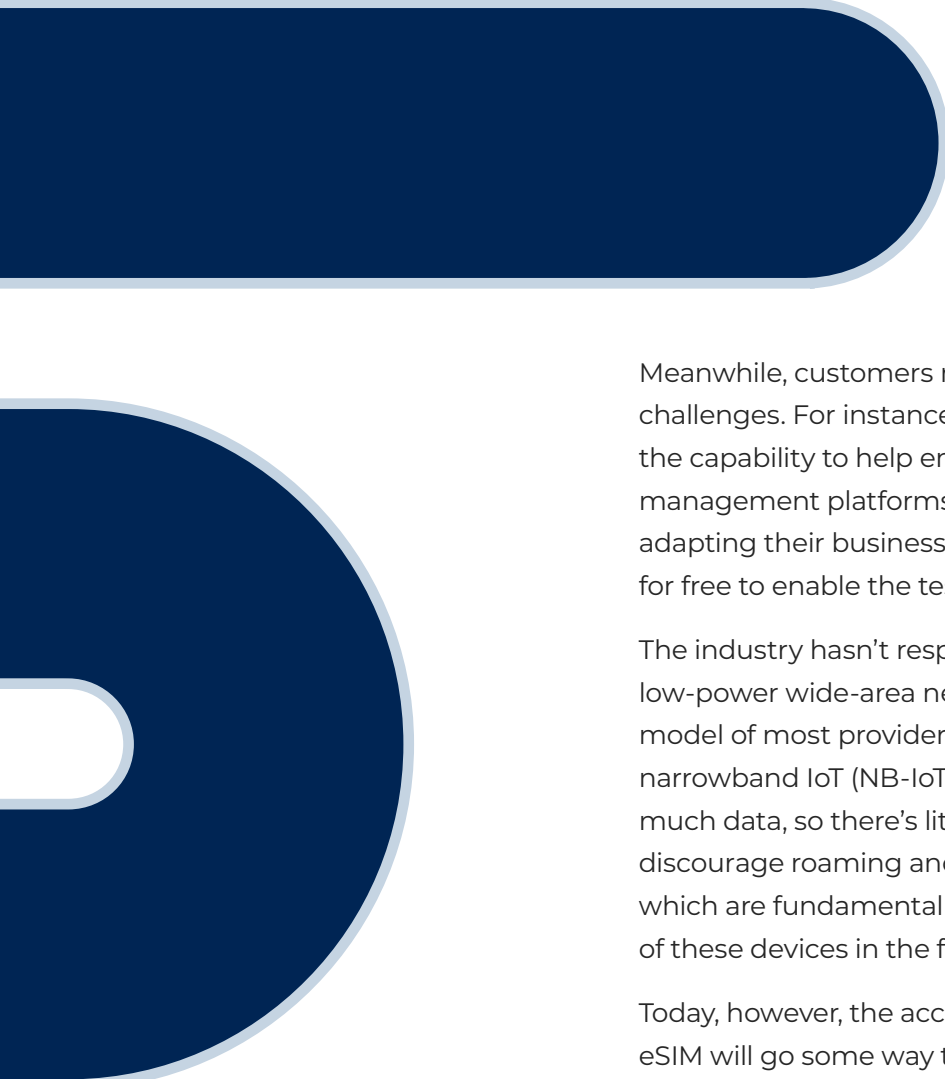
## The many technical challenges of global IoT deployments

There are complexities, too, in terms of deployment.

An IoT development lifecycle, such as the manufacture and roll-out of a million connected vending machines around the world, is a significant time-sink.

It requires months of development and testing. It's important to know, for example, that a device's software and hardware are correctly configured, and that it's capable of recovering quickly in the event of a network outage.

But the expertise required isn't always available for enterprises. It's rarely their core competence, so they'll tend to look toward the wider industry to provide it.



Meanwhile, customers may encounter some additional challenges. For instance, some connectivity providers don't have the capability to help enterprises in that lifecycle. Connectivity management platforms, for example, may not be capable of adapting their business model to offer a small amount of data for free to enable the testing and facilitation of a deployment.

The industry hasn't responded well to the emergence of low-power wide-area networks (LPWAN) either. The business model of most providers is based on data consumption, and narrowband IoT (NB-IoT) or LTE-M use cases don't consume much data, so there's little in it for operators. Essentially, they'll discourage roaming and functions such as power-saving modes which are fundamental to the longevity and cost-effectiveness of these devices in the field.

Today, however, the acceleration of concepts like eUICC and eSIM will go some way to solving these issues, using over-the-air (OTA) mechanisms to localise a SIM wherever possible or, if not, to provide a solution that can address any risks to the deployment that may arise in the future.

## Overcoming barriers to permanent roaming

[It's expected that, by 2025, 1.7 billion IoT devices will carry an eSIM onboard – 457% as many as today.](#)

Permanent roaming, when IoT devices roam onto a foreign network for more than 90 consecutive days, is a significant driver in this.

But there's a question of regulation. Countries including Turkey, Brazil, Singapore, China, and the UAE have all prohibited permanent roaming in one way or another. Elsewhere, some operators – most notably in Australia and the US – are very much against IoT devices permanent roaming in their country. A regulator, looking at the impact of this, could then decide that permanent roaming was no longer allowed.

These two factors mean there's a less than accommodating global view of permanent roaming. But eSIM and localisation offer a solution to permanent roaming bans and prohibitions. eSIM decouples the SIM from the operator so that network providers can be switched remotely OTA. This flexible framework enables companies to adapt to the local market deployed in and avoid the roaming model by downloading and activating a local operator's connectivity profile – otherwise known as localisation.

Indeed, there has been an emergence of eSIM vendors who work with operators around the

world to use their networks to provide a global connectivity service. Of course, eSIMs do come at a little extra cost. The hardware is more expensive than a typical SIM, and the supply chain is tightly controlled and certified, pushing up the OpEx. But it's worth weighing up these costs against the potential risks of not using an eSIM. If a company has two million SIM cards in a particular country, and they're suddenly shut off, with only a limited time available to rectify the situation, it can cost millions to ensure those devices don't become paperweights.

**We're witnessing a significant uptick in cellular IoT deployments, but they're not simple – there's a lot of complexity that needs to be overcome, especially when operating across different geographies.** eSIMs, therefore, have an important part to play in this. A better understanding is required, too, of the technical challenges involved, challenges that can be addressed either by internal expertise or by external partners.

2020 was supposed to have been the year things really took off, but due to the pandemic it never really happened. But, because of the need to reduce business risks, adapt processes, and achieve greater transparency, we're now seeing an increased demand for connectivity. Today, with the right technology and the right expert resources, companies can begin to enjoy the benefits of a truly global IoT deployment.

**“eSIM and localisation offer a solution to permanent roaming bans and prohibitions”**



# — eSIM: creating the perfect storm to accelerate digital transformation

Nick Earle, CEO, Eseye



Every now and then a technology shift completely upends the way companies do business. It often happens silently at first, with its true significance only becoming apparent when people start building real-world-world applications on top of it. The touchscreen technology that enabled the iPhone is an example, and later 4G made smartphone connectivity fast enough to create a mobility revolution.

The eSIM is such an innovation, and its time has come. It is a technology that allows connectivity to be done differently, and as such, will enable IoT to reach its full potential.

eUICC (*embedded universal integrated circuit card*) is the software component of eSIM which helps to make it all happen. It provides the capability to store multiple network profiles that can then be provisioned and managed over-the-air. eSIM is nothing short of revolutionary. It means that customers can integrate a single SIM into their device design and it's good to go, anywhere in the world.

This is important to any global company with connected products or assets, including many that may not be obviously IoT companies.

For example, PUDO (pick up drop off) lockers, such as Amazon's, need to be opened by different people every day. When the parcel is dropped off, the locker sends a code to the recipient, which they use to open it. If it can't connect, the business case falls apart. Likewise, EV chargers need to communicate with their charging network to log people on, manage the charge, and process the payment. Both need reliable connectivity, or they will have disappointed customers. The coming of the eSIM is key to these large corporate global deployments of distributed connected technology.

## What does the eSIM actually change?

You may be thinking, 'well surely it was already possible to connect to different networks?' Well, yes but it was a more cumbersome affair.

We could do it using multi-IMSI SIM technology - an approach where Eseye led the world. This technology enables a single device to store several network profiles on a single SIM and switch between them. It was a decent fix, and for the user, the result looked similar. But the back-end management was much more technically challenging – incurring costs for network providers who had to handle the switching. It also was limited by the number of profiles stored on the SIM.

The eSIM works differently. It allows any device to connect to another mobile network virtually – a layer of software that manages connections to the physical networks. **All switching is handled by the software, not the SIM, which is much easier and more cost-effective.** As this becomes standard there will be no need for SIMs to be separate exchangeable technologies, they will be integrated into the device, and eventually part of the circuitry.

“The eSIM  
works  
differently”





## Why are eSIMs so important now?

eSIMs have been around for a few years but they have really started to become mainstream in the last year or so.

Part of the reason is that the economics of Mobile Network Operators (MNOs) has changed. They used to charge each other for roaming and make a profit. As costs of data came down, this revenue shrinks, whilst the network switching kit to manage roaming agreements stays the same. Roaming has gone from a money maker to a drain.

This has made networks open to collaborative agreements that allow Virtual MNOs (VMNOs) to manage the network switching. This does away with complex reciprocal agreements and instead lets the networks get paid by anyone, or any device, using their network. Eseye's AnyNet Federation (similar to the airline's STAR Alliance) make VMNOs possible, and therefore allow eSIMs to fulfil their potential. With the most localization options of any provider, our model ensures a flexible global connectivity approach without the need or risk that comes with permanent roaming. As a sign that the industry has recognised the opportunity, module manufacturers such as Thales and Kigen have recently announced eSIM strategies.

At the same time, the pandemic has shifted old ways of thinking and working, changing mindsets towards distributed devices and workforces that leave the organisational perimeter. This change in thinking has opened people up to innovative distributed approaches to their business structure – which is the right mindset for IoT. These two trends – one of technology, one of thinking – create the perfect storm for an acceleration in global IoT deployments.





## Distributed devices bring security worries

However, nothing is simple. Companies rightly think 'If I could make any device smart and put it anywhere, I could transform my business'. But they also know that if devices are connected, they can be hacked. Money, personal data, or even property (in the case of lockers) could be stolen. [Recent Eseye research](#) found **39% of IoT decision-makers said security was their biggest hurdle – the highest single result.**

Security pros like devices to be inside their organisation's perimeter where they are easy to keep an eye on. IoT devices by their nature exist outside of the perimeter, expanding the edge of the organisation, where they are connected to someone else's network (usually the MNOs). The potential downside of an eSIM is that you cannot work directly with an MNO, from whom you can make security a condition of the contract because you often don't know which MNO is providing the connectivity.

To solve this problem, you need not only a VMNO approach but also for them to operate a single multiprotocol label switching (MPLS) network, across which all data can easily travel. This 'single eye of the needle' approach to IoT data is the most effective way to have oversight of all data transmitted from the device, all managed through a single layer of software, regardless of which MNO is currently servicing the connectivity.

With this single private network approach, the VMNO can implement a set of deep packet inspection capabilities on the network traffic to monitor the devices, identify unusual behaviour at the source, quarantine the devices, remediate the issue, and then allow them back onto the network. This is how Eseye's architecture works. By linking our network to our customers' network, we are treating every device as if it was directly connected to an ethernet port behind the enterprise firewall. **Only in this way can IoT device security be as strong as any enterprise IT network.**

**“Eseye offers advanced, agentless security to the edge of the network”**

## Where next for IoT?

In summary, a transformative IoT technology is now here in the eSIM. Over the next few years, we anticipate a large number of start-ups and established companies to launch IoT devices worldwide. As this happens, we expect security concerns around the edge of the network to become a major buying requirement. This may slow progress temporarily as people adjust to new mindsets and approaches, but in time solutions will be proven safe and people will trust them. Then IoT will accelerate exponentially.

The smartphone was a revolution. But it was 4G that brought fast mobile data and opened a world of mobility for the consumer, allowing a new world of mobile services to be built on top of the phone. The phone connectivity model never quite worked for IoT which couldn't abide connectivity black spots. But with the eSIM, we are about to see a similar shift in what is possible, and a whole new world of connected business applications as a result.

That will unleash a wave of innovation just as mobile connectivity did.

**We'll witness a transfer of power from the MNO, with their proprietary SIM approach, to the enterprise with an agnostic eSIM model.** This in turn will enable truly global deployment of devices without the administrative burden of multi-SIM management. And when this happens IoT will finally cross the chasm from early adopters to main street mass deployment.





# – **Visibility and understanding** – **securing the IoT**

Peter Doggart, Chief Strategy Officer, Armis



Many of the real-time connected devices, sensors, and widgets that make up the IoT – such as a remote telehealth monitoring solution or a connected streetlight – are extremely powerful pieces of hardware. Very fast, with their own memory and processor capacity, they're essentially small computers. But, as they come into our lives at an exponential rate, each of these devices represents a potential vulnerability.

Securing them isn't straightforward, however. Each of these devices contains embedded software – to control its actions, transmit data, or perform analysis at the edge. But their security is often overlooked and, as they're typically closed systems, it isn't possible to upgrade or add to the existing software. Even if you could, the sheer number of permutations means you'd have to write millions of varieties of software. It simply wouldn't make sense. How, then, do you go about securing the IoT?

“  
**IoT security  
is often  
overlooked**”

## Education is key

Most people, when designing an IoT system, don't think about security from the outset. Unless they're working for Apple or Microsoft, they'll typically rely on third parties in their software stack. Rather than reinvent something, it's easier to use a few lines of open-source code – even if they don't really understand it and have no idea whether it's right for their application.

It's little surprise, then, that we at Armis continue to find masses of zero-day vulnerabilities in critical systems. About two years ago, we [announced](#) 11 fairly major vulnerabilities in a real-time operating system used in billions of critical industrial, medical and enterprise devices, the nature of which meant they couldn't be recalled and weren't easily patched.

Given the risk these vulnerabilities represent, it's vital that we educate the developers of such devices about the need to build in security from the ground up, to build in the ability to patch, and to think from the perspective of DevOps all the way through to production operations. By helping them understand this, we stand a good chance of preventing the opening of potential floodgates for security hacks.





## Moderating the response

But, as important as education is, we still don't have enough understanding to fully address the issue. The problem will always be asymmetric by nature. Bad actors only have to find one crack in a network's defences, and they're in. What we must do, therefore, is weigh up the benefits of an IoT network against the risks. We need to understand the potential impact on our systems if an attack does get through, and what we should do to mitigate that impact.

Dedicated network monitoring tools, designed to track IoT systems that extend well beyond the organisational perimeter, can alert a company to thousands of potential threats to its IoT network in a single day. But it isn't possible to investigate all of them. The company has to prioritise, and that's done by understanding the risk impact to its business.

The first step is to understand that a vulnerability isn't necessarily the end of the world – it's actually probably something mundane. It's then a case of classifying or characterising what that vulnerability could do. What's the power of that particular exploit? And if exploited, what impact could it have on a company's other systems?

It's a case of moderating the response depending on the level of threat. There are now sensors in bathrooms in airports across the world, for instance. If those IoT systems are hacked, then the toilets may not be as clean as they should be for a few days. That's worth dealing with but it's not an emergency.

If the systems pose a threat, you can quarantine the system away from other systems, and still operate. If it's really serious, with the potential to do a large amount of harm, you could take your system offline although, given the knock-on effects this would have, this is only the best response in very high-risk situations. In most cases, by understanding the risk, it's possible to put appropriate controls in place.

## A different perspective

Although relatively new, the technology exists to help establish whether or not there's an issue. Effectively using a big inference engine, it gathers data and passively listens to what's being said between the connected devices within an IoT system. With over 700 MNOs around the world, this is no easy task, of course. But, by using a broker to manage all that global connectivity from a single platform, you'll have a much clearer picture of data flows, enabling you to infer a great deal about what's going on. You can then overlay a lot of contextual information on to your network. **You can know, for example, what a particular device is, what it's connected to, where it's located, who's able to access it, and what good and bad behaviour look like.**

With this level of visibility, you'll quickly know whether you need to worry about a particular device. With a proper risk analysis and mitigation plan in place, you'll be able to use this insight to respond accordingly. It's a different way of looking at things from a security perspective, taking incredible inference from data to provide clarity on what's going on.

Ultimately, though, we need a greater understanding of how, when we add in more connected devices, to live with the risk. Visibility, skills, and education are paramount. There's a lot of learning still to be done when it comes to securing the IoT.





**No Limits.**



 @eseyem2m  
 Eseye  
 eseyeM2M  
 [www.eseye.com](http://www.eseye.com)