

IoT Predictions

for 2023 and Beyond

By Nick Earle, CEO and Larry Socher, SVP Strategy and Alliances, Eseye

Over the last four years of predictions, we have tried to balance predicting the short-term impact of specific changes with the long-running trends that remain in motion year over year. However, in 2023 we feel we will hit an inflection point where there will be significant change in the IoT industry.



Nick Earle,
CEO, Eseye



Larry Socher,
SVP Strategy and
Alliances, Eseye

If there has been one overarching trend that has defined our predictions, it is the breaking apart of siloed, operator-driven connectivity and its replacement with a vendor-neutral approach – one where IoT devices work wherever they are, not just according to which vendor they have signed up with.

With the growth of the eSIM over the last year, which allows choice between mobile networks – the vendor lock-in model has finally broken. At the same time, we have seen the emergence of important changes that shift the IoT business

model in favour of the enterprise, starting with big plays made by hyperscalers, through the emergence of private networks, competing technologies and business models which enable new use cases, which in turn place new demands on connectivity. A growth in connectivity, user choice, and more valuable use cases, remains the long-term trajectory for IoT, and will no doubt recur year after year.

But within that long-term horizon, we see five significant trends that will change the industry and move up the agenda for IoT manufacturers and enterprise IoT managers in 2023.

The MNO proprietary lock-in finally cracks with increased choice and the hyperscaler threat

For some years we've been warning that the Mobile Network Operator (MNO) model, based around branded, proprietary SIMs, has been ready to crack. MNOs are inherently regional companies and silos – operating in limited geographies and controlling their own slice of bandwidth.



This is fine for smartphones, where people typically live in one country and have flexible roaming options for international travel and use eSIM to switch networks after moving or choosing a new domestic operator. But the model does not work for IoT projects, where millions of devices need to be shipped around the world and work out-of-the-box wherever they are placed.

The gradual replacement of branded SIMs in favour of eSIMs driven by the smartphone market makes it increasingly more difficult to lock customers in and has an even more dramatic impact on the IoT market. Perhaps the strongest indication of this was Vodafone's recent decision to spin off its IoT business – in our view a recognition that selling connectivity directly was not a growth area and by establishing a separate business that could embrace interoperability was a more viable path forward.

While increased flexibility to switch operators, driven by emerging eSIM technologies is breaking vendor lock-in, the hyperscalers are moving aggressively to capture market share at the edge and potentially pose a greater threat.

"Perhaps the strongest indication of this was Vodafone's recent decision to spin off its IoT business..."

Even as Moore's Law slows down with price performance of compute doubling every two years from 18 months, our networks struggle to keep pace with the exponential growth of data. Gartner predicts that by 2025, 75% of all data will not only be produced but processed outside of cloud data centres¹. A connected Costa Express coffee machine does its bean counting on an embedded processor, rather than in the cloud.

For this reason, the hyperscalers – Amazon, Microsoft, Google et al – have been racing to provide solutions for the edge, investing heavily in IoT and its connectivity to the cloud. Microsoft began back in 2008, with the launch of Azure Stack, followed by its Azure Stack Edge, IoT Plug and Play Bridge, and IoT Hub. AWS wasn't far behind, with its Greengrass, Outposts, Snowcone, and IoT Core solutions, while Google also made a play with its Anthos platform.

In addition to extending their cloud services and edge products, both Microsoft and Amazon are also investing

heavily in networking solutions. The former acquired Metaswitch and Affirmed Networks – which it offers through Azure for Operators – to connect up IoT portfolios to Azure through private networks. Amazon appears to be going even further by offering its own private 5G (including LTE) solutions.

All this changes the dynamics for mobile network operators. Increased competition creates choice, which puts the power in the hands of the enterprise. And unlike MNOs, the hyperscalers are global and can offer turnkey solutions, so are natural partners for many global IoT projects. The hyperscalers have the scale and power to bring the best options together and manage it behind the scenes.

IoT, of course, still requires the networks for mobile connectivity, but increasingly it's the enterprises that hold the cards, rather than the MNOs. And they should exercise that advantage when choosing connectivity options – whether directly, via a systems integrator, or through hyperscalers – demanding that connectivity is flexible and not locked into a vendor.

As a result of these shifts in control, the best option for mobile connectivity when delivering an enterprise-centric IoT platform is a next generation Mobile Virtual Network Operator (MVNO).

As mentioned earlier, thanks to eSIMs, there is no need for vendor lock-in. MVNOs offer the ability to switch between networks as local or international needs require, as well as overlay and integrate other functionalities (some of which we discuss below). That, alongside hyperscalers platforms, offers the choice and flexibility that businesses need to scale IoT.

In 2023 the proprietary, vendor lock model of the MNOs selling mobile connectivity for IoT will finally crumble. They will change their business models to offer their services as part of MVNOs, which will be better aligned and more seamlessly integrate with the hyperscalers' offerings. For the enterprise, that will mean more flexibility when choosing their connectivity solutions as they build IoT portfolios that operate around the world.

...thanks to eSIMs, there is no need for vendor lock-in. MVNOs offer the ability to switch between networks as local or international needs require...

¹ What Edge Computing Means for Infrastructure and Operations Leaders, Gartner

Interoperability between public and private networks becomes a priority

Enterprises have started to invest heavily in private networks to support more reliable, higher-speed and low-latency communications. We believe that the real power of 5G is the introduction of Ultra Reliable Low-Latency Communications, or URLCC.

The combination of private networks and 5G will enable a whole new set of use cases such as autonomous trucks at a mine, factory automation, computer vision for predictive maintenance, augmented reality for remote experts, and a range of other applications to improve operations in the field. This trend is accelerating with the introduction of new “shared spectrum” models like the Citizens Broadband Radio Services (CBRS) standards in the United States. Due to limited device availability, most of these deployments have utilised LTE in 2022 and it will be a year or two before they transition to 5G.

As they grow in popularity, we are starting to see increased demand for roaming to and from these private networks onto public networks. Imagine a truck full of cargo. In transit, it shares its location and basic content monitoring data via a public cellular network, so logistics can be monitored and managed in real time. When it arrives at a warehouse, it automatically switches to the warehouse’s private wireless network, where it will have a secure, reliable high bandwidth signal, and connectivity into the company’s ecosystem.

Another example is an autonomous truck using the private network at the mine and roaming onto a public network when it transports its ore over public highways to a port.

In 2023 there will be increased focus on roaming to and from private networks as adoption grows.

From a connectivity point of view, that will mean that MVNOs who offer rules-based switching between public and private networks, while still maintaining a single management control plane, common APIs and consolidated billing, will become key players in the private network – and eventually 5G ecosystem. This will require tight integration of the private and public network roaming with a range of enterprise authentication and management tools, such as Cisco ISE, Aruba ClearPass and Active Directory.

The ascendance of ‘network agnostic’ and ‘multi-RAT’

When it really comes down to it, enterprises are agnostic to the network technologies and operators that provide their IoT connectivity. As long as they can get secure, reliable, high-performing and cost-effective connectivity from device to cloud, they do not care what network technology or operator delivers it.

Fueled by the consumer market, as modem costs continue to drop, particularly for sub-GHz solutions, we are seeing increased interest in using multiple Radio Access Types (RATs) and networks to provide more optionality, increased flexibility and resiliency and greater longevity by allowing enterprises to mix, match and optimise connectivity as their IoT deployments and the market evolves. Cellular communications will increasingly be mixed with other wireless protocols, including Wi-Fi, Bluetooth, Zigbee, Thread, and LoRaWAN. A number of modem providers such as Nordic Semiconductor, uBlox and Silicon Labs already provide multi-RAT solutions, and we are seeing additional industry consolidation such as the





Semtech (LoRaWAN) and Sierra Wireless (cellular) merger that will continue to drive this trend.

We are also starting to see incredible innovation as a new generation of low-cost Low Earth Orbiting (LEO) satellite constellations are changing the economics and viability of device to cloud satellite communications, promising ubiquitous global communications that fill gaps in the terrestrial cellular networks and can now compete on price. Adding to the momentum, we are on the cusp of 3GPP R17 non-terrestrial extensions, which will allow the use of standard cellular modem and antennae with new firmware to talk to satellites. Apple's iPhone 14 already has an eSIM with a satellite overlay, allowing emergency texts via satellite. Where Apple goes, others are sure to follow.

Taking a page out of the Uber and crypto playbooks, we are also seeing a number of disruptive crowdsourced business models such as Amazon Sidewalk and Helium test the market as an alternative to the traditional communications service provider models. Both Sidewalk and Helium use variations of the LoRaWAN protocols and could potentially accelerate adoption.

The use of multiple Radio Access Technologies is not an alien concept. For a long time, our smartphones have used a combination of cellular, Wi-Fi, Bluetooth, NFC and other protocols to support everything from Internet data, peripheral communications, financial transactions, location services and provisioning.

With continued drops in prices for modems driven by the consumer market, we anticipate the cost of putting multiple modems into an IoT device to become much more economical over the next few years. This will make multi-RAT an attractive way of both increasing flexibility and performance, while driving lower cost communications.

As a result of these forces, we expect to see more IoT devices with multiple modes of connectivity in 2023. This is a natural corollary to, and extension of, the previous predictions – as types of network increase, so devices will need more functionality to work wherever they find themselves.

...we expect to see more IoT devices with multiple modes of connectivity in 2023.

Most providers focus on one or two of these technologies, which may not be enough. The next generation MVNO

needs to extend its solutions to not only solve the problems of global cellular connectivity but must embrace multi-RAT and seamlessly support and optimise network solutions across cellular, Wi-Fi, LoRaWAN and satellite, while providing seamless integration for site protocols such as Wi-Fi, Bluetooth, Zigbee and Thread.

Consumer and enterprise IoT use cases converge to create new connectivity challenges

While we have often seen success in the consumer market drive enterprise adoption, as evident by enterprises having to support Wi-Fi in the office, the two worlds have typically remained relatively separate. The networks that power the digital home remain managed by the family, while VPN and other overlay technologies bridge them to their offices.

But we are starting to see a number of IoT use cases that challenge the separation of home networks and the enterprise world, particularly in healthcare and home energy management. In 2023, we can expect to see these, and similar use cases start to break the separation between consumer and enterprise requiring networks that can seamlessly be managed by both worlds.

Take healthcare. COVID-19 drove healthcare services to finally embrace connectivity and collaboration solutions to provide in-home medical services including remote patient monitoring (RPM). The 'hospital ward' is taken into patients' homes through wearable and other devices that capture and process complex metrics.

To date, this has consisted largely of consumer health devices that share data over Bluetooth to a mobile device. But as remote patient monitoring starts to provide more critical services – including cardiac monitoring – healthcare providers need enterprise-grade IoT solutions and connectivity.

They can no longer rely on a consumer managed home network and broadband Internet access to be up and running when a patient's life may be at risk. To provide these services, they will need solutions that integrate the home network communications using Wi-Fi, Bluetooth, and Thread to wearables and other RPM devices, and ensure multiple upstream network options by adding 5G fixed wireless access to existing wired broadband solutions to increase resiliency. We predict that medical-grade clinical devices will move into the home setting during 2023, requiring integrated connectivity

solutions that bridge the home network to broadband Internet with increased adoption of multiple broadband providers to increase reliability.

Similarly, the way that we manage energy distribution in the home will change dramatically over the next few years. This is fuelled by the rising cost of energy, growth in electric vehicles (EV) and demand for home EV chargers, economic incentives encouraging the installation of solar panels to generate your own energy, and increased adoption of home generators and batteries to provide power during the increased electrical outages driven by climate change, hurricanes, fires, and other natural disasters. For example, we may not want to run our washer or dryer while we are charging our car. We may also want to cut off energy to a number of our appliances to ensure the refrigerator has priority during a power failure where we are using our home batteries and generator.

Not only will we want to better manage how we distribute and use power in the home, but the increased adoption of solar and other renewables fundamentally changes the structure of the grid. The home shifts from a consumer of power to both a consumer and producer. Over time this shift should result in bi-directional flow of energy to and from our electrical grids, requiring integration between home energy management and our utility companies.

Much like the healthcare RPM example, this will drive the need to integrate home energy management solutions like SPAN electrical panel with Itron electrical meters that govern the interface between the home and the grid to orchestrate bi-directional power consumption.

...the way that we manage energy distribution in the home will change dramatically...

The rise of next-generation MVNOs will help enable this integration in 2023. Those who support in-home networking protocols such as Wi-Fi, Bluetooth, and Thread along with cellular and other connectivity can work with both enterprise solution providers and the digital home ecosystem to connect the dots and deliver integrated solutions. MVNOs will provide connectivity solutions that bridge the two worlds.

With an understanding of what is needed to manage the convergence of the different technologies and security

protocols needed by such sensitive applications, MVNOs can provide the integration framework needed to address converging enterprise and consumer use cases such as these.

IoT starts and ends with the device

In 2011, Marc Andreessen coined the phrase “software is eating the world.” The logical conclusion of this trend of software companies dominating the world is that hardware ceases to matter. This may seem intuitive, but when it comes to IoT, it is wrong.

While it may be the software, applications and data that ultimately deliver business value for the Internet of Things, unless the device or ‘thing’ can communicate effectively from device to cloud, the application breaks. In many cases devices and applications are operating in remote, often hostile, noisy environments such as a mine, oil rig, pipeline or refinery, manufacturing floor or warehouse. Designing, deploying and optimising an IoT solution to provide flexible, reliable, and resilient communications can be incredibly complex, particularly for devices that will be in production for years in a constantly changing market.

There are many factors that have held back IoT adoption but the biggest one is the importance of the device ecosystem and device skills. The ecosystem is hugely fragmented and challenging to navigate. There are lots of options across microcontrollers, modem providers, software stacks, and other components.

As a result of this, customers and solution providers are struggling to design their devices correctly the first time, which is exacerbated by supply chain problems driven by COVID and an increasingly more hazardous geopolitical environment. Recent Kaleido Intelligence research² confirms that the largest contributing factor to holding back their IoT deployments was device design, with 84% of enterprise respondents citing as their number one challenge. That challenge could be the biggest sticking point to unlocking all the choice that is being created by the innovation in RAT, networks and business cases discussed in this report.

Given that most enterprises have no device expertise, or in many cases do not want to have any on staff, then Gartner's observation that 80% of all IoT projects fail before they are even launched is not much of a surprise³. Companies cannot

² New IoT Connectivity Survey Highlights Issues Slowing Down IoT Adoption, Eseye, June 2022

³ 8 out of 10 IoT projects fail even before they are launched, Economic Times, May 2016



take advantage of the growing choice discussed in this report unless they build their devices to connect when and where needed.

While the device and hardware clearly matter, once again it may be software that provides a solution. To reverse the trend of failed IoT projects, the device needs to be flexibly designed with the right hardware components and have software intelligence embedded into it so that it can operate in different environments, detecting available connectivity, and selecting and optimising the right networks and protocols to support the use case requirements. And there are complexities and trade-offs of this optimisation – there is a balance to be struck between power requirements, the interoperability of various RATs, bandwidth, latency – and of course ensuring cost is kept within the right range for its use case.

We predict with confidence that more attention will be needed on the device to unlock the true potential of IoT.

So, one thing is clear, in 2023 more than ever before, hardware WILL be important. Taking the time to get the device design right is the key to unlocking IoT success. Devices now more than ever need to have connectivity flexibility built-in by design, with intelligent software that can help select, manage, and optimise communications so that they can adapt as the market evolves.

2023 – the year control shifts from the network operator to the enterprise and the device

2023 will be the year everything changes in the world of connectivity. A perfect storm of market conditions – the growing threat from the hyperscalers, greater investment in edge technology, the incremental growth of private networks and 5G – all change the dynamics of connectivity. We are looking down the barrel at a world in which IoT is set free to be designed around sophisticated global use cases, not by the limitations of regional connectivity providers.

As power shifts from the regional MNO to the enterprise, hyperscaler and embedded intelligence on the device, a new breed of MVNO will be needed to help stitch together these capabilities, mix, and match different technologies and operators, and finally provide true global device to cloud connectivity keeping control in the hands of the enterprise. This next-generation MVNO must go well beyond aggregating and reselling cellular roaming.

They need to provide on device intelligence software that can take advantage of not just localised access to cellular networks around the globe, but also other network technologies and operators including support for LoRaWAN, satellite and other emerging networks, integration with private networks, Wi-Fi, Bluetooth, and Thread for downstream communications.

With all the above managed by sophisticated connectivity management platform that uses a rules engine and machine learning to orchestrate and optimise connectivity.

Perhaps most importantly, from 2023, after more than 40 years of being locked into the MNOs' ways of working, the power and choice will finally be in the hands of the enterprise and the device with a new breed of MVNO emerging to unlock this potential.



For more information, visit www.eseye.com