KORE

IoT Technologies and Trends 2024: Ramping Up the 5G Era

KORE

Contents

Introduction

During this decade of IoT, between 2020 and 2030, technology and trends are shifting rapidly and giving rise to a new era of technology, computing, and digital applications. In this decade, 2G and 3G will become fully obsolete and replaced by 4G LTE, 5G, low power wide area (LPWA) networks and short-range technologies. New ways of compute and storage will proliferate and data will become massive and critical across thousands of use cases. In this eBook, we take a look at the current technology and trends in 2024 and how it specifically impacts the Internet of Things.

> Furthermore, 5G is anticipated to add nearly $1 trillion to the global economy by 2030.

The 5G Era

The newest generation of cellular technology is going to play a major role in IoT innovation during this decade. GSMA Intelligence[1] reports that in 2022, 12 percent of the global connections (excluding licensed cellular IoT) were 5G and that number is expected to increase to 54 percent – or 5.3 billion connections) by 2030. Furthermore, 5G is anticipated to add nearly $1 trillion[1] to the global economy by 2030.

Enhanced Mobile Broadband

Mobile broadband is very similar to broadband, which is high-quality, high-speed internet. When adding mobility to the equation, the end user is able to enjoy the same high-quality and high-speed internet anywhere through a cellular connection – in this case, 5G. It creates the ability to connect a device to a cellular network anywhere and enjoy the same quality of service.

eMBB is going to open a lot of opportunities for a variety of use cases including:

Telemedicine: This segment of connected healthcare grew during the pandemic and is likely to level off but continue to be utilized. eMBB is going to support the applications within this use case to help provide quality care that is decentralized outside of a clinic, hospital, or doctor's office.

Smart offices: Video conferencing, cloud access for software applications, remote offices, and virtual training can be supported by the high quality and speed of eMBB. Connected events: Concerts and sporting events are two examples of public events that tend to experience lag or no network connectivity due to the large scale of data communications. eMBB is positioned to handle such large scale.

Multimedia: High-definition in multimedia has the possibility to be enhanced through eMBB, such as streaming content and gaming.

Remote field serving: Primarily in industrial applications, this use case allows technicians to access equipment remotely for diagnostics and repair.

Ultra-Reliable Low Latency Communications and Critical IoT

The low latency and reliability of 5G for mission-critical applications will be realized in ultra-reliable, low latency communications (URLLC).

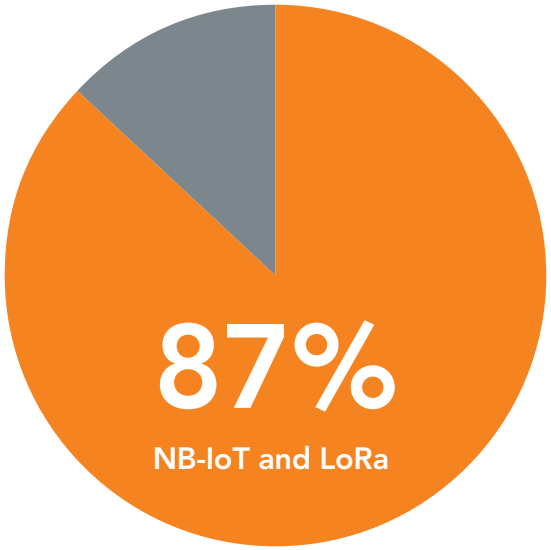
URLLC in the enterprise sector can help power the Fourth Industrial Revolution as factory processes and power systems are automated. URLLC becomes a critical component of machine learning, robotics, and autonomous operations (Automated Guided Vehicles) because a delay along the production line due to communication blips can wreak havoc. In connected health, leveraging everything from AR and AVR to robotics, URLLC can play a critical role in making sure data communications run smoothly without blind spots or lags. Smart grids can utilize data aggregation to manage power across an energy grid, especially one that uses multiple energy sources. Transportation can utilize IoT through drones for traffic control or vehicle-to-vehicle (V2V) communications for greater safety, or artificial intelligence (AI) in a move to more autonomous consumer and fleet vehicles.

Low Power Wide Area in the 5G Era

When the 3GPP standardized the fifth generation of cellular connectivity, the network technology was segmented in thirds – eMBB, URLLC, and low power wide area (LPWA). For cellular LPWA, there is Narrowband IoT (NB-IoT) and Long Term Evolution for Machine Type Communications (LTE-M).

The two major characteristics of low power wide area (LPWA) networks are spelled out in the name – low power means that this connectivity technology uses low power for a longer battery life. The wide area is a nod to its range of at least 500 meters from the gateway device to the endpoint. Additional benefits of LPWA, according to GSMA, are low device unit cost, improved outdoor and/or indoor penetration coverage compared with existing wide-area technologies, secure connectivity and authentication, optimized data transfer, simplified network deployment, and network scalability[4]. Because LPWA supports large-scale, widespread IoT deployments that support low-complexity, low-power devices, it is anticipated to create a subset of IoT called Massive IoT.

Analyst organization Omdia projects that NB-IoT and LoRa will account for 87 percent of LPWA IoT connections in 2027, which will increase from the current 85 percent of LPWA[2] connections.



LPWA IoT connections

NB-IoT and LPWA

According to GSMA, these standardized LPWA technologies were designed with the following characteristics[3], which make them attractive to IoT:

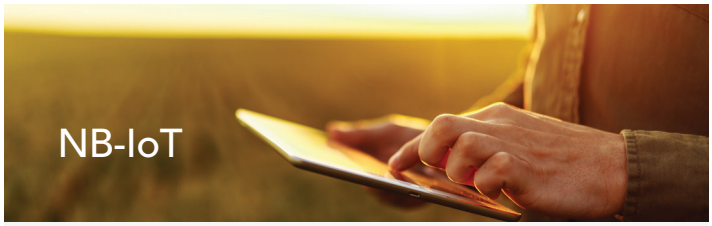
- Low power consumption that enables devices to operate for 10 years on a single charge
- Low device unit cost
- Improved outdoor and indoor penetration compared with existing wide-area technologies
- Secure connectivity and strong authentication
- Optimized data transfer (supports small,intermittent blocks of data)
- Simplified network topology and deployment
- Integrated into a unified/horizontal IoT platform
- Network scalability for capacity upgrade

While both network technologies share very similar characteristics, they do have key differences that power different use cases.

LTE-M is an IP-based communication protocol designed for higher bandwidth or mobile and roaming applications than NB-IoT. LTE-M also supports Voice over LTE (VoLTE), so it can handle more complex IoT devices.

Use cases include:

- Fleet tracking
- Asset tracking
- Smart metering
- Point of sale devices
- People/pet tracking
- Smart watches



NB-IoT, which is currently most widely used in Europe and Asia, is built off the LTE physical layer and designed to offer extended coverage. Single-tone transmissions allow for enhanced latency in poor coverage areas. NB-IoT does not support VoLTE and is better leveraged in stationary devices.

Use cases include:

- Retail applications for point of sale
- Smart home applications
- Smart cities
- Smart buildings (utilities such as alarm systems, HVAC)
- Agriculture
- Smart metering for utilities

Unlicensed, Non-Cellular LPWA

Several proprietary LPWA network options operate in unlicensed spectrum, such as Sigfox and LoRa. When using licensed spectrum, operators must apply for and obtain a license from local regulatory agencies, such as OFCOM in the United Kingdom, to own and operate spectrum in exchange for connectivity that is 99.999 percent interference-free.

Unlicensed spectrum doesn't require any special permit or license to operate, but if multiple providers are operating in the same area, unlicensed connections have a chance of being subjected to interference.

LoRa and LoRaWAN

The LoRa Alliance has taken its private spectrum and built a public spectrum called LoRaWAN. This specification, which has been widely used in Brazil, is now deploying globally. LoRaWAN meets the requirements of Massive IoT well, addressing key objectives such as secure bi-directional communication, mobility, and localization services. LoRaWAN provides low range, low power, low-cost connectivity, and security for devices and the network.

LoRaWAN Advantages:

- Well designed for single-building applications
- Bi-directional communications are optimized
- Works well with devices that are mobile, such as tracking devices

Agriculture: With a long range that provides reliability in rural applications for devices that don't have a high data transmission rate, LoRaWAN supports measuring crop production, tracking cattle, and more in an effort to optimize operations.

Assets and logistics: Network-based location and tracking abilities at a low cost and optimized battery life make LoRaWAN suitable for the smart supply chain.

Cities: Public/municipal operations can be made more efficient with LoRaWAN capabilities, including smart infrastructure, traffic and parking management, street lighting, waste removal, and recycling.

Healthcare: LoRaWAN's low power, low cost, and reliable performance make it suitable for connected health applications, such as remote patient monitoring or mobile Personal Emergency Response Systems (mPERS).

Industrial: Industrial IoT, otherwise known as Industry 4.0, is transforming operations by digitizing legacy processes and equipment, driving profits, keeping costs lower, and maximizing efficiencies.

Utilities: LoRaWAN's ability to reach sensors that monitor utilities located underground make this a well-suited connectivity choice for smart metering.

Sigfox modules are affordable and the connectivity itself is "as-a-Service." In certain cases, companies can deploy and operate the network in-house.

Sigfox Advantages

- Lightweight protocol that manages smaller data packets efficiently
- Ultra-narrow band technology can accommodate more channels and achieve greater network capacity
- Lower total cost of ownership

Network Slicing and Private 5G

Network slicing for private 5G networks allows businesses to tailor a network for specific needs with customizable network capabilities like data speed, quality, latency, reliability, and security. Network slicing allows communication services providers (CSPs) a new value proposition for enterprises.

If network slicing is the capability, private networks are the application. Private networks, at a high level, mean a dedicated network that lies outside of public networks. Typically, the reason to use private networks falls under security and bandwidth purposes. While private networks are available via 4G LTE, the network slicing capabilities of 5G make it a much more accessible solution.

Private networks offer a host of benefits, some of which are dependent on the use case, but this solution has many key features that can support business cases in all verticals:

Security: With dependability and redundancy mechanisms that occur at every level of the protocol stack, private networks help secure mission-critical or sensitive data.

Penetration: Private cellular networks can penetrate through walls and obstructions much better than Wi-Fi can, which makes it an ideal use case in large campuses and manufacturing.

Low latency: A strong, reliable network connection means gaps or interruptions in communications. This is important in all data transmission, but critical in applications such as robotics or autonomous vehicles/machine operations.

Wide range and coverage: Large areas, like those in shipyards, airports, education or business campuses, and much more can enjoy the wide range and coverage of dedicated cellular network connectivity.

Control and customization: With full control over design, deployment, and operations, as well as the option to quickly configure the network, private networks offer greater plasticity than wired communications or public cellular. Private networks can also be highly scalable offering flexibility for integrating new applications or physical locations. A drawback of creating a private network is that it can be time-consuming and costly, so it's important to approach building private networks strategically with a clear understanding of goals for the specific business case.

A Note on Private LTE and 5G

Private networks have the ability to offer heightened security and dedicated bandwidth for many IoT use cases, but private networks can be complex and not every use case can benefit from them, and choosing the right connectivity technology and infrastructure is important.

Public, Private, or Hybrid Networks?

Public networks are those owned and operated by carriers, which is likely the most familiar association with network connectivity in enterprise use. When leveraging cellular for business operations, any connected devices and routers are going to operate on a network that the organization essentially rents from the carrier through a contract and is billed monthly.

The benefits of a public network include that it is simple to get solutions up and running quickly. The costs are typically low and there is no maintenance or upgrading required because the network is owned by a third party (the Mobile Network Operator). Coverage is wide and it can be applied across the organization, no matter where various locations might be.

The downside to a public network is that it is a shared public network and can be more vulnerable to security such as when data privacy and security are mission critical, like with manufacturing, financial tech, healthcare, or government use cases.

Another drawback is that the organization is dependent on the operator and they do not have much control over the physical infrastructure.

With a private network, the network is owned and operated by the organization leveraging it and only authorized devices can connect. This allows the organization to dedicate the network to only its applications which can help increase security, dedicate bandwidth, potentially lower latency, and can provide higher reliability since it is not a shared network.

However, private networks can be expensive, complex, and require management and maintenance as it is the organization's responsibility and no longer the Mobile Network Operator's responsibility. Mining, manufacturing, and government are a few of the use cases where it becomes more essential to have a private network versus use cases that do not have higher risk in network connectivity.

But there are applications that can benefit from having a portion of operations running on a private network while the rest of operations are running on a public network, which is the hybrid approach. More mission-critical applications and in house applications can leverage the private network, while mobile assets and fleet can leverage the public network as these assets travel from one location to another.. However it can become complex managing multiple networks, private and public.

4G LTE or 5G for Private Networks?

With 4G LTE having many more years of 4G LTE, likely until 2030, and 5G Non-Standalone (NSA) relatively prolific and 5G Standalone (SA) still in extremely early iterations, it is equally as viable to opt for either network technology.

With the continued buildout of 5G NSA and SA networks, private networks are going to become more accessible, making a choice between the two network technologies equally viable.

5G has been built with backward compatibility to 4G LTE, so the risk of choosing 4G LTE is not similar to the radical network sunsets seen with 2G and 3G. An upgrade from LTE to 5G will be necessary, but it won't require recreating new architecture and hardware or devices. Many hardware manufacturers have created 5G-ready solutions to deploy now on LTE and upgrade to 5G later.

The majority of private networks in 2022 were LTE – 57 percent[4] in fact. But in many use cases, LTE and 5G were combined.

GSMA Goals of the 5G Era

Working closely with the mobile operators pioneering 5G, the GSMA is engaging with governments, vertical industries including automotive, financial services, healthcare providers, transport operators, utilities, and other industry sectors to develop businesses cases for 5G[5].

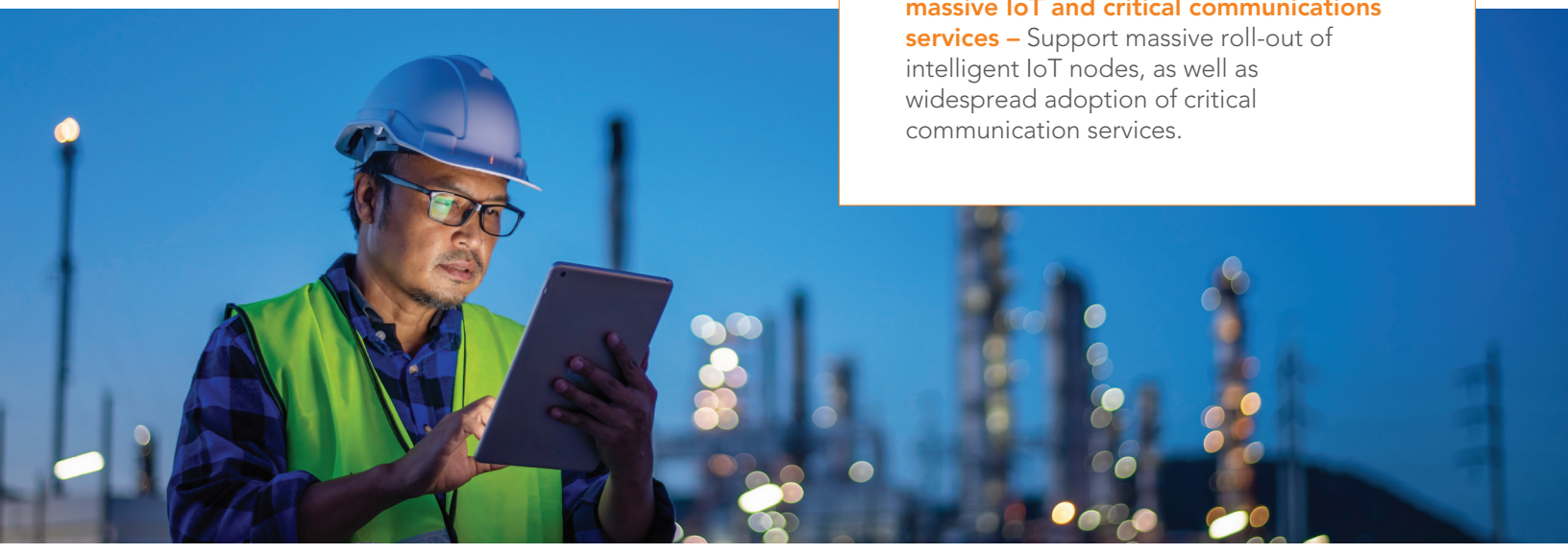
1. **Boundless connectivity for all –** Co-exist with 4G LTE networks to provide borderless, high speed, secure connectivity.

2. **Deliver future networks innovatively with optimal economics –** Cost-effectively delivers better quality networks either independently or through partnerships.

3. **Accelerate digital transformation of industry verticals –** Establish the networks and platforms required to drive digitalization and automation of industrial practices and processes.

4. **Transform the mobile broadband experience –** Enhanced mobile experience with up to 1 Gbps and <10ms, providing a platform for cloud- and artificial intelligence-based services.

5. **Drive growth in new use cases for massive IoT and critical communications services –** Support massive roll-out of intelligent IoT nodes, as well as widespread adoption of critical communication services.



The impacts of 5G are going to be numerous, but adopting this new cellular generation doesn't come without its challenges, as identified by the GSMA[6]:

1. Business case – To maximize the 5G opportunity, the mobile industry must identify new services, market segments, and suitable business models to optimize the network investment.

2. Spectrum availability – Spectrum will continue to be a scarce resource, and the availability of spectrum, at which frequency bands, and at what costs will have a significant impact on the 5G business case.

3. Technological improvements and breakthroughs – To meet the technical expectations of 5G, both the laws of physics and current network layouts will be challenged, demanding major technological advancements in device and network design.

4. Fragmentation – Lessons learned from 2G, 3G, and 4G LTE deployments prove that mobile technology is more successful when fragmentation is limited. Operators must standardize from the beginning to avoid future issues.

5. Regulation – To rationalize the significant investment that 5G deployment demands, regulatory bodies must support transparent policies that encourage investment and innovation. The innovation of 5G is significant, which estimates claiming mobile operators will be able to grow global revenues at a CAGR of 2.5 percent during the 5G era[6], it is important to note that 5G deployments must be a collaborative effort among key players in the mobile industry. The way that 5G is developed, managed, regulated, and commercialized will fundamentally establish how closely it meets expectations of innovation and economic growth.

eSIM: Single SIM – Global Connectivity

The eSIM (embedded SIM), also known as an eUICC (Embedded Universal Integrated Circuit Card) is a type of technology that provides device users with significantly increased levels of flexibility through its ability to support multiple cellular carrier profiles on a single SIM card.

Traditionally, a SIM card only contained the credentials or subscription required to access a single carrier's services – changing carriers required changing SIM cards. With eSIM, users can remotely provision their devices to switch between support carrier profiles via Over-the-Air (OTA) updates. The eSIM represents a revolutionary change in the ways cellular services are managed – eliminating the need for SIM swaps or even physical access to the device to change service providers.

The eSIM specification has been adopted by the global industry as a de facto standard for remote service provisioning (RSP) of eSIM-21 connected devices. The specification, known as GSMA Embedded SIM specification GGP .02 was developed by GSMA specifically for MRM eSIM implementations. It makes it possible to provision and manage eSIMs in remote devices by pushing a new profile to the devices OTA. Although eSIM solutions have technically been available for several years now, it has mostly been in proprietary solutions for very specific use cases, such as Apple iPads. In 2012, GSMA became involved in eSIM specifications and standardization to ensure SIM cards, provisioning systems, and equipment – regardless of manufacturer – will function together.

SGP.31/SGP.32

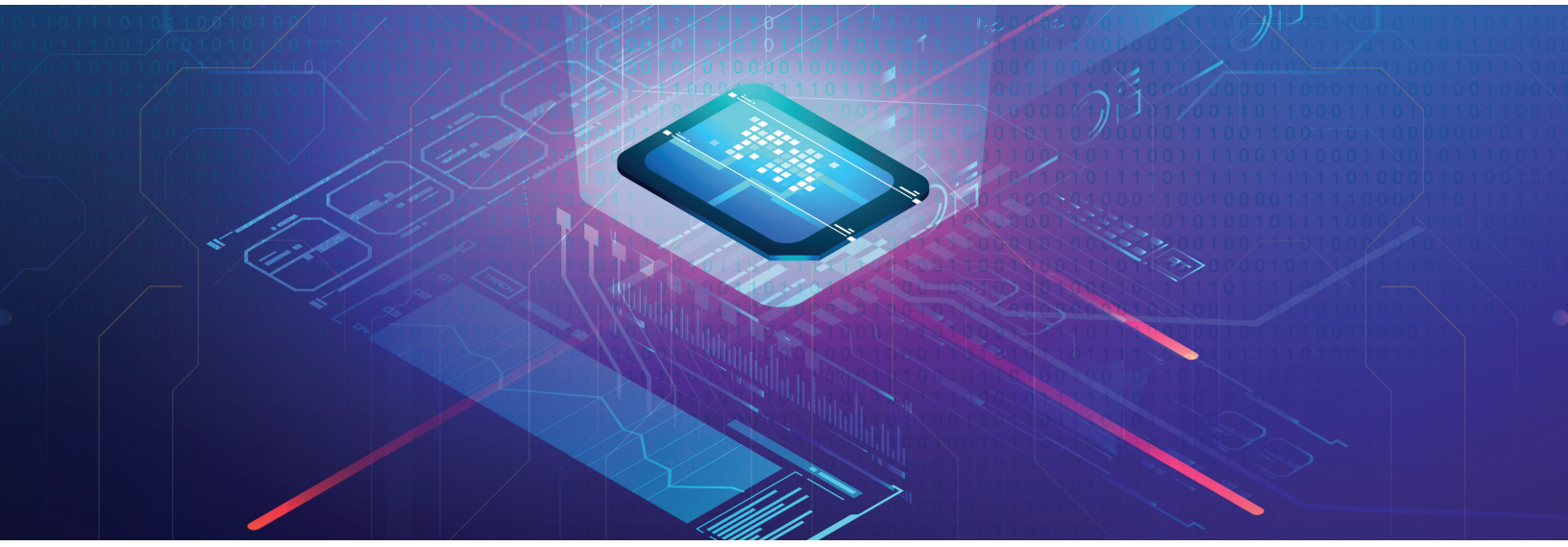
The GSMA has published new IoT architecture, requirements, and technical specifications for eSIM remote SIM provisioning (SGP.31/SGP.32). These standards enable the remote management of eSIM profiles, enhancing the flexibility and scalability of IoT deployments. By adopting these specifications, organizations can streamline the provisioning process, reduce operational costs, and improve the security of IoT systems. This development represents a significant advancement in the management of IoT connectivity.

The adoption of eSIM and remote SIM provisioning will become more widespread, driven by the need for flexible and scalable connectivity solutions. Future advancements in eSIM technology will support more dynamic and automated management of connectivity, enabling IoT devices to seamlessly switch between different networks and service providers. Additionally, the integration of eSIM with other IoT management platforms will provide a more comprehensive and streamlined approach to connectivity management.

Building Efficient Systems and Scaling with SGP.32

Adopting SGP.32 standards for eSIM remote provisioning can significantly enhance the efficiency and scalability of IoT systems. By leveraging these specifications, organizations can streamline device management, reduce operational costs, and improve security. This approach enables the seamless deployment and scaling of IoT solutions, driving innovation and operational excellence.

SGP.32 will be integrated with AI-driven management platforms, enabling more intelligent and automated provisioning and management of IoT devices. The adoption of blockchain technology for secure and transparent provisioning processes will further enhance the security and reliability of IoT deployments. As a result, organizations will be able to scale their IoT solutions more efficiently and securely, driving greater innovation and value.



According to the GSMA[7], there are several key impacts to the accelerated adoption of eSIM

- Adoption of global standards and/or specifications versus proprietary solutions
- 5G pushing greater adoption of cellular connectivity for solutions, which tangentially would increase eSIM use
- iSIM as another comparable connectivity technology choice
- eSIM addressing top challenges in IoT deployment such as integration with existing technologies, the cost of implementation and security
- IoT companies offering a powerful eSIM strategy in addition to their main core proposition

Finding the True eSIM

The adoption of eSIM is accelerating as IoT is becoming a more prolific technology and the economy is becoming more and more global. With a market becoming more saturated with options, it's important to distinguish a true eUICC solution from similar competitors.

Dual SIM: Some mobile devices support the use of two SIM cards, described as dual SIM operations. When a second SIM card is installed, it allows users to switch between two separate mobile network services manually, has hardware support for keeping both connections in a "stand-by" state for automatic switching, or has individual transceivers for maintaining both network connections at once.

Soft SIM: This is a software-based SIM card with no actual SIM hardware. An eSIM is either embedded or removable and can be ruggedized for IoT use.

Multi-IMSI: A standalone Multi-IMSI SIM solution is comprised of a single SIM that has several IMSIs, which are the unique numbers that let Mobile Network Operators (MNOs) authenticate their subscribers so they can access the network. Multi-IMSI simply means a device has the ability to connect to several different networks. So, while Multi-IMIS on its own can be pre-programmed with the ability to connect to more than one network, it's the eUICC eSIM that is the ideal global, future-proofed technology because it can switch to networks remotely and it allows greater ease and flexibility for global deployments and long-term IoT solutions – ideally for a device's entire lifecycle. KORE has been involved in a mission-critical use case of drone logistics, where eSIM was leveraged to switch between satellite and cellular connectivity. Swoop Aero, an Australia-based drone logistics company, utilizes its drones to deliver medical supplies and treatments to remote locations across the globe, most notably COVID-19 supplies.

When looking for a true, eUICC eSIM to support future-proofed, out-of-the-box, global connectivity, look for the following capabilities:

- A single SKU eSIM that is globally connected
- A carrier-agnostic platform that minimizes roaming costs
- Connecting that has the resilience to overcome network sunsets
- Standards-compliant RSP technology that allows remote, automatic connectivity to the optimal network
- Device monitoring to ensure the solution is always connected and operating properly
- Connectivity management tools that teams can use to manage connectivity profiles, as well as provision data and devices
- Security that is based on industry standards
- An architecture that can scale along with the business

Simplify IoT complexity with a trusted advisor and global, independent leader in eSIM capabilities:

- Achieve global coverage via a single eSIM and the KORE eSIM profile, with support for additional carrier profiles as needed
- Enhance scalability and growth by introducing new business models and value propositions enabled via natively connected devices
- Eliminate SIM switching costs and improve operational efficiencies with remote eSIM provisioning
- Minimize total cost of ownership and maximize returns on IoT investments through a consolidated operational model
- Future-proof connected devices with a single eSIM that can support multiple carriers and network technologies

> *"We at Orange are thrilled to partner with KORE, taking an important step to unlock the full potential of eSIM for customers with IoT use cases that require high performance and global coverage,"* commented Bénédicte Javelot, CEO Orange Wholesale France. *"More than ever, our customers are expecting us to go beyond traditional connectivity to provide global, innovative and resilient IoT solutions."*

Security and Regulatory Requirements

A more connected ecosystem poses a threat to cyber safety and the way we navigate personal and business information online. The discussion surround IoT security has hit a critical mass in the industry, but in a positive way. Instead of considering security to be a value-add or something to be shored up after a security incident, we're going to see a bigger push towards security by design.

Building 'Security by Design'

Incorporating security measures from the outset of the IoT development process is crucial. This involves designing hardware and software that inherently protect against potential threats. Key strategies include implementing secure boot processes, encrypted communication channels, and regular firmware updates. Additionally, leveraging technologies such as Trusted Platform Modules (TPM) and Hardware Security Modules (HSM) can enhance the security of IoT devices. By prioritizing security from the design phase, organizations can mitigate risks and protect sensitive data throughout the device lifecycle.

Security by design will become a standard practice, driven by increasing regulatory requirements and the growing sophistication of cyber threats. Future IoT devices will incorporate advanced security features, such as AI-driven threat detection and response systems, making them more resilient against attacks. Moreover, the development of industry-wide security frameworks and standards will help ensure consistent security practices across different IoT applications.

SASE Offering Heightened Security Measures

Secure access service edge (SASE) is a global cloud-based network and security service that initially was leveraged for mainly an enterprise IT infrastructure beginning around 2019 on the heels of software-defined wide area network (SD-WAN) deployments. Now it is evolving into an emerging trend in IoT to securely manage IoT devices. According to research by Palo Alto Networks, IoT devices are subject to a host of security threats – the top three categories being exploits, malware, and user practice issues such as phishing or weak passwords[8]. The research states that more than half of IoT devices are subject to medium- to high-severity attacks – 57 percent. SASE security combines cloud-access security brokers, cloud secure web gateways, zero-trust network access, firewall-as-a-service, and DNS – alongside its networking services leveraging wide-area networking – to provide a secure, scalable infrastructure for flexible widespread deployment of Internet-connected endpoints. SASE has an edge component, delivered through Point of Presence (PoPs) or data centers that bring the capabilities closer to the device level, which is a growing trend in IoT that helps minimize entry points for attacks along data communications.

Regulatory Requirements for IoT Management - Ensuring Compliance with Industry Standards

Compliance with regulatory requirements is crucial for the successful deployment and management of IoT systems. This involves adhering to industry standards, such as GDPR for data protection and ISO/IEC 27001 for information security management. Engaging with regulatory bodies and staying informed about evolving regulations

can help organizations navigate compliance challenges. Additionally, implementing robust security measures and best practices can mitigate risks and ensure compliance with regulatory requirements.

Regulatory requirements for IoT will become more stringent, with a focus on security, data privacy, and environmental sustainability. Automated compliance monitoring tools will emerge, enabling organizations to continuously assess their adherence to regulations and standards. The development of global regulatory frameworks will harmonize requirements across different regions, simplifying compliance efforts for multinational organizations. Furthermore, the adoption of privacy-enhancing technologies, such as differential privacy and homomorphic encryption, will support compliance with data protection regulations while enabling valuable data analysis.

Device Compliance and Certification

Ensuring compliance with industry standards and obtaining necessary certifications is crucial for the market success of IoT devices. Regulatory requirements vary by region and application, encompassing aspects such as electromagnetic compatibility (EMC), radio frequency (RF) exposure, and safety standards. Engaging with certification bodies early in the development process can streamline compliance efforts and prevent costly delays. Additionally, adhering to best practices for design and testing can facilitate successful certification and market entry.

The regulatory landscape for IoT will continue to evolve, with increasing emphasis on security, data privacy, and environmental impact. Automated compliance tools will emerge, simplifying the process of obtaining certifications and ensuring ongoing adherence to standards. Furthermore, the development of global harmonized standards for IoT will reduce the complexity and cost of achieving compliance across different markets.

The GSMA, in an attempt to create a universal standard for authentication and authorization of IoT devices, has created IoT SAFE (IoT SIM Applet For Secure End-to-End Communication). This initiative enables IoT device manufacturers and IoT service providers to use the SIM as a robust, scalable, and standardized Root of Trust to protect IoT data communications. A root of trust can be a hardware, firmware, or software component that performs security functions. In the case of IoT SAFE, the SIM is the hardware root of trust. IoT SAFE delivers a common procedure to secure data communications with a reliable SIM, rather than using proprietary and possibly less secure hardware elements in the device.

Benefits of IoT SAFE include:

- Improvement in the security of solution offered or reduction in device complexity
- Secure, seamless cloud onboarding with enterprise connectivity
- Extended certificate lifecycle management
- Value-add to SIM/eSIM platform
- Portability, ease of deployment
- Connectivity and protocol agnostic

Intelligent Network Monitoring

Security is a critical element of any IoT deployment. Many connectivity management platforms cannot detect fluctuations in usage at the device level. Those fluctuations are important to flag, however, as they could potentially indicate security breaches or device malfunctions. Intelligent network monitoring platforms have become a holistic approach to network and device monitoring to help manage the complex network and usage details of IoT deployments.

The most powerful platforms include:

- Real-time traffic monitoring
- Monitoring of multiple conditions, including IP address or IMEI changes, anomalous communication patterns, loss of connection, and more
- Insight via complex rules with actions, including condition alerts, notifications of SIM status changes, advanced threat actions, and more
- Endpoint management

Trending in IoT

Certainly some of the largest trends in IoT center on 5G, as this new network technology creates a lot of new opportunities for use cases as well as the need for service providers to differentiate and diversify offerings to meet the needs of the 5G era.

IoT Hyperscalers

The world of the internet and digital solutions has traditionally been pretty fragmented and required a lot of laborious custom building. To create an employee tracking system at an enterprise, it required buying or building compute and storage and then configuring applications. Now, with data storage and compute, it's as simple as going online and purchasing what you want from one of the cloud hyperscalers, such as Google Cloud, Microsoft Azure, or AWS. It's simple, easy, and a very common way of buying and operating digital solutions.

The same holds true for IoT – early iterations of IoT were complex, even for simpler solutions. IoT solutions are even more complex now. Endpoints must communicate at all times. Connectivity must travel with solutions or support massive or critical applications. Data needs to be cleansed and communicated securely to the cloud for analytics that delivers powerful results, like artificial intelligence and machine learning.

IoT is headed toward that democratization where leveraging solutions is as simple as going online and clicking a button. What this is going to require is strong partnerships across the ecosystem and the rise of IoT hyperscalers, including cloud hyperscalers.

Hyperscaler has traditionally been rooted in the major players of cloud services, but IoT hyperscaler is a term dedicated to a similar level of scale as those major cloud service providers, but dedicated solely to IoT.

IoT is well beyond a connectivity proposition, but the true value lies in combining resilient connectivity with the ability to easily ramp and manage in an effective, low-cost approach, or democratization. IoT is moving toward a massive scale, and this needs to be accomplished from build to deployment and management in a global, flexible manner. An IoT hyperscaler can manage each touchpoint through simplistic, secure offerings under a single roof, which addresses a significant gap in the market. IoT hyperscalers can offer to users the plug-and-play approach to IoT that lessens CapEx, enhances ROI, and is built to scale.

Transforma Insights identifies a successful IoT hyperscaler as being able to provide a massive scale, low-cost management, and combined device and/or connectivity offerings[9]. Connectivity in IoT is becoming simply table stakes, as well as the broad management of connectivity through a connectivity management platform.

End-to-end solutions are of high value[10] in the IoT industry and an IoT hyperscaler offers the comprehensive, robust set of solutions needed to deploy, manage, and scale IoT.

Analytics for Artificial Intelligence and Machine Learning

The enhancement of analytics is going to be a massive tidal wave as more and more data is collected through both LPWA- and 5G-connected devices. The push toward artificial intelligence (AI) and machine learning (ML) is creating a push for a significantly lessened lag between data collection and processing/analysis. This in particular is a large area that can be addressed by an IoT hyperscaler with key partnerships in the IoT ecosystem – especially with cloud hyperscalers, such as Microsoft Azure, AWS, and Google Cloud.

An IoT hyperscaler works diligently the endpoint of devices and device management, the connectivity, and the IoT platform that helps deliver the data (which also needs to be cleansed and normalized) for the greatest analytics results. An IoT platform also helps customers manage and monitor devices, whether a deployment has a fleet of devices in the thousands or is dispersed globally. A comprehensive and streamlined IoT core provides organizations with the ability to select their preferred communication protocol, allowing them to receive telemetry data from devices. It also provides the means for management of devices and device policies from the cloud while also issuing OTA commands and configuration update back to devices.

Additionally, IoT core also provides a secure method for data communication, as it only allows authenticated devices to access your system in the cloud, and protects the transported telemetry data with end-to-end encryption.

Some early use cases in IoT of leveraging artificial intelligence is highly focused on AI-enabled video analytics – video management systems, computer vision systems, and object recognition are a few subsets that can enhance security and safety in many applications such as construction, smart cities, manufacturing, fleet management, and healthcare, to name a few.

High Bandwidth and Fixed Wireless Access

Fixed wireless access (FWA) leverages 4G LTE or 5G connectivity to create fixed broadband access that uses cellular radio frequencies instead of wired cables. Essentially, it is much like high-power WiFi, but it does not have the same risk as wired connections and it also supports greater bandwidth. Enterprises and organizations that have typically relied on wired solutions are looking more toward FWA as digitization grows and connectivity becomes a mission-critical component.

FWA is also beneficial for those interested in reduced latency for tasks such as streaming video for training purposes in local retail establishments or data localization for improved Quality of Experience (QoE).

Smart cities, homes, buildings, and universities are top use cases for FWA, in addition to retail. But FWA can also help mitigate traditional challenges like digital deserts, where access to wireless broadband has been lacking, and thus providing high-speed internet.

Installation is a major boon of FWA as there is no need for digging trenches to allow for wires. In this sense, FWA is "Day 0 connectivity" for new locations that need to get up and running quickly without waiting for the highly physical implementation of traditional wireless connectivity.

FWA can be leveraged as a primary of a secondary connection for failover. In many applications, it is pertinent to consider the value of using hardware that is 5G ready. While 5G standalone (5G SA) is still in development, the backward compatibility of 4G LTE can be leveraged in 5G-ready routers. Once 5G SA is available, there would be no need to replace hardware.

Fixed wireless access will give enterprises and retailers a powerful approach to high bandwidth IoT use cases. A great example is retail, particularly in the restaurant industry. Leveraging connected devices for ordering and point of sale is likely to increase, partially due to the convenience but also as a means of mitigating workforce challenges. Online ordering and integration into third-party delivery applications, offering on-site wireless connectivity, and connected appliances are other elements in such use case that would demand greater bandwidth, and more reliable, than what traditional wireless broadband can offer.

Smart Living

With the rise of city-based living, IoT solutions can help consumers and businesses navigate in a way that goes beyond voice-enabled assistants and smart locks to address sustainability. For the EU, specifically, there has been discussion regarding EV charging stations and ways to make cleaner fuels more widely available. There has also been a distinct movement from basic telematics to connected video technology to boost fleet safety and efficiency. In-vehicle video solutions can provide near real-time alerts for driver distractions, unsafe road conditions, and vehicle status – allowing fleet operators to act quickly in a move toward an ultimate reduction of risk. With each of these smart living advancements, the need for high-speed, IoT-specific network connections grows. Especially as solutions scale and deploy in more locations, there's an increased need for carrier flexibility and improved coverage. These applications of IoT where LPWA technologies will be highly useful.

The Resurgence of MVNE Mobile Virtual Network Enabler (MVNE)

Service offerings are nothing new, but as mobile cellular connections continue to rise worldwide, Mobile Virtual Network Operators (MVNOs) have started to challenge traditional MNOs. They are doing this by providing SIM-only mobile subscriptions to consumers seeking alternative mobile plans. As well as looking to address specific niche markets (with unique content offerings), they are thereby distinguishing themselves from MNOs. Launching a mobile virtual network should not be complicated and customers are now looking toward those fully managed offerings, where they can build their own propositions and offer tailormade connectivity services by creating their own rate plans and roaming footprint. The overall goal is to launch mobile brands to the marketplace with minimum upfront investment so they can focus on running their business.

Leveraging iSIM

While traditional and eSIM modules will remain a popular choice, iSIM will rise an attractive option due to its small size.

Integrated SIM (iSIM) incorporates the SIM operating system into the cellular chipset, also known as system-on-chip (SoC) design. This technology will be well utilized in low-power use cases, and it also creates a space saver in hardware since there is no need for a physical chip or tray for a SIM within the device. Power savings will occur, as well, since the device will not have to power a separate SIM card. The iSIM technology carries very similar benefits to eSIM and builds on eUICC functionality. It can be provisioned automatically and over-the-air, which makes it a global, future-proofed cellular connectivity option.

Edge Computing

Multi-access edge compute (MEC) is the standard architecture for edge computing and it isn't synonymous with edge computing. Edge computing is more of a broad concept, while MEC is the infrastructure. According to ETSI, a European Standards Organization that has worked to define global MEC standards, its MEC standardization initiative has been developed to, essentially, create a common thread between telcos, cloud service providers, and the IT world. MEC, ETSI states, allows application developers and content providers an approach to cloud computing and IT services at the network edge. Through MEC, MNOs can open their Radio Access Network (RAN) on the edge, allowing developers to create edge applications and services.

The Edge Stack

The edge is comprised of many different components that are necessary for creating overall value. It's important to understand the overall infrastructure of the edge stack in order to make the best decisions in creating deployments.

Generally speaking, the edge is created of: Services and applications: The topmost layer of the stack is the end user application that delivers the benefits of edge computing. Application development: This layer involves the network functions, APIs, and application software that power the end user applications. IoT/enablement platform: The IoT enablement and computing platform is the center where applications are hosted and run, which includes the virtualization layer. This very crucial component of the technology stack is what drives the significant value of edge computing solutions and needs to be nimble and flexible to allow for greater management and scalability.

Hardware: This infrastructure includes servers, routers, end devices, and other physical infrastructure that resides in a data center.

Physical location: This is where the edge computing physical infrastructure is placed, whether it's the telco site, the telco tower center, or the network premise.

Use cases for MEC, as identified by ETSI, include:

- V2X
- Video analytics
- Location services
- Optimized local content distribution
- IoT
- Augmented reality

2024 Top of Mind Questions

Why is the adoption of NB-IoT slower than other LPWA technologies?

NB-IoT adoption was sluggish since its launch in 2017 alongside LTE-M and then with other competing technologies in LoRaWAN and Sigfox. The issue lies in network operators not wanting to deploy vast networks without high demand, yet device manufacturers not wanting to roll out massive quantities of NB-IoT enabled devices without the proper network support. The benefits of the technology were not diluted, it was just a matter of investment in terms of MNOs and OEMs.

However, NB-IoT is catching up, with IoT Analytics reporting a 2022 growth of 61 percent year-over-year[11] for the LPWA technology.

How important is the integration of the IoT in the cloud to manage data?

The integration of IoT devices with cloud platforms is essential for efficient data management. Cloud platforms offer scalable storage, advanced analytics capabilities, and real-time processing of IoT data. By leveraging cloud services, organizations can gain actionable insights, enhance decision-making processes, and optimize operations. Key considerations include selecting the appropriate cloud provider, ensuring data security and privacy, and implementing robust data governance policies.

Edge computing will complement cloud integration by processing data closer to the source, reducing latency and bandwidth usage. This hybrid approach will enable more efficient and responsive IoT systems. Moreover, advancements in AI and machine learning will enhance cloud-based analytics, providing deeper insights and predictive capabilities. Cloud-native IoT platforms that offer seamless integration with various IoT devices and protocols will become the norm, simplifying deployment and management.

What does cloud native mean and how does it relate to IoT?

The Cloud Native Computing Foundation defines cloud native as tools and applications that empower organizations to build and run scalable applications in public, private, and hybrid clouds[12]. Essentially, software development can be accomplished faster and at greater scale when the applications are cloud native. A few other key benefits include cost efficiency, a great vendor-agnostic approach to cloud services, as well as automation and flexibility such as agile workflow and DevOps culture.

What is the Internet of Everything?

The nomenclature for IoT has progressively changed over the years, with the earliest name being Machine-to-Machine, or M2M. The Internet of Things was coined by Proctor & Gamble computer scientist Kevin Ashton when proposing the use of RFID for asset tracking in the supply chain. The Internet of Everything is likely a new iteration as the technology proliferates and more and more devices are connected in life and business.

Will iSIM overtake eSIM?

In short, no. Both SIM options are incredibly similar and boast the same benefits of out-of-the-box, global, and future-proofed connectivity. The key difference in iSIM, according to Kigen, is iSIM supports system-on-a-chip (SoC) architecture, which allows for less real estate occupied by the SIM card[13]. A great use case for this would be wearable devices – the less room there is on the physical device, the less space there is for a SIM card.

How important are local downloadable profiles to eSIM?

Local downloadable profiles, in addition to zero-touch provisioning, is a major differentiator in a true eUICC eSIM and a Multi-IMSI solution. Multi-IMSI can hold multiple carrier profiles and it is more of a failover solution if the connection in an area is poor. An eUICC eSIM allows you to connect to the local profile and download it, rather than just be stored. This is an extremely key feature that makes it possible to achieve global connectivity.

What is zero-touch provisioning for eSIM?

One of the key benefits of eSIM is its flexibility, and that comes in several forms when considering eSIM for enterprises. The first major capability of eSIM for enterprises in relation to flexibility is zero-touch provisioning. Zero-touch provisioning allows for eSIM to be activated with the touch of a single button. For thousands of devices deployed across a widespread geography, this can streamline the process significantly.

The same over-the-air (OTA) provisioning allows for carrier changes to take place remotely. If a thousand devices in Germany need to switch network operators, then an engineer in the United States can manage that remotely in a matter of minutes.

The key in these situations, as well, is the ability to auto-provision in bulk. When it comes time to scale operations with more devices, or more locations, or both, bringing those new devices online is simple when done in bulk.

The ability to have a single SKU that can be provisioned to specific carriers also helps provide significant flexibility in logistics management both in ordering, shipping, and receiving.

What is ZigBee protocol for IoT?

ZigBee is a low power consuming IEEE 802.15.4 (2003) standard-based specification, and the brainchild of 16 automation companies. What makes it novel is the use of mesh networking, which makes utilization of communication resources much more efficient. ZigBee-based IoT nodes can connect to the central controller making use of in-between nodes for propagating the data. It makes both the transmission and handling of data robust.

Sources:

[1] https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf
[2] https://www.rcrwireless.com/20230426/internet-of-things-4/nb-iot-and-lorawan-leave-rivals-for-dust-as-lpwa-iot-jumps-23-per-year
[3] https://www.gsma.com/iot/mobile-iot/
[4] https://www.rcrwireless.com/20220928/5g/almost-900-organizations-deploy-lte-5g-private-networks-gsa
[5] https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf
[6] https://www.gsma.com/iot/mobile-iot-commercial-launches/
[7] https://www.gsma.com/iot/wp-content/uploads/2022/03/MWC22-eSIM-Summit-Master.pdf
[8] https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[9] Transforma Insights, Who's Winning the Race to Become a Hyperscale IoT Connectivity Provider
[10] https://www.rcrwireless.com/20211006/5g/top-3-hyperscalers-and-how-they-are-impacting-5g
[11] https://iot-analytics.com/number-connected-iot-devices/
[12] https://www.cncf.io/
[13] https://kigen.com/resources/blog/sim-esim-isim-whats-the-difference/