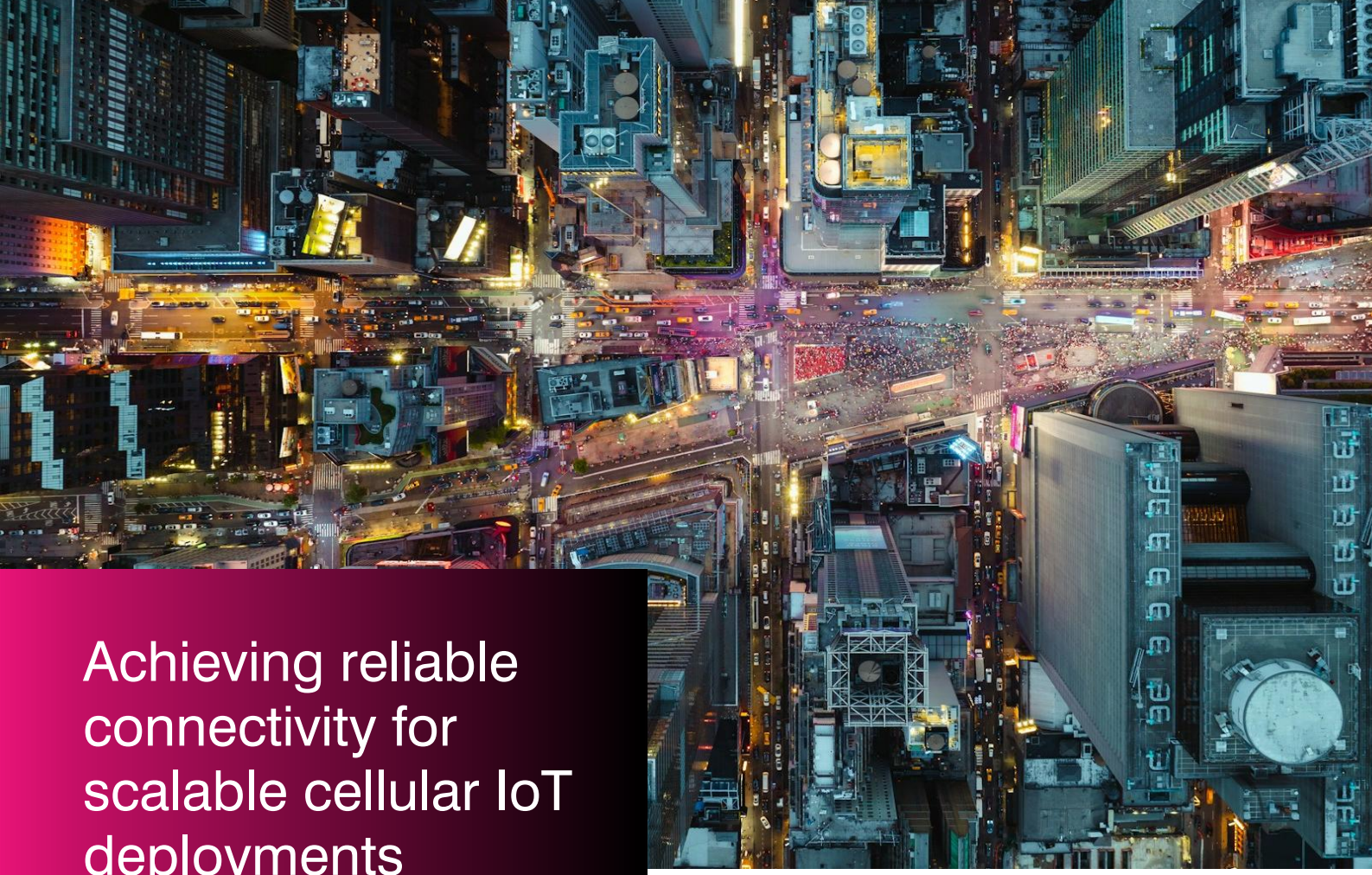


Achieving reliable connectivity for scalable cellular IoT deployments

2025

Produced by

Berg Insight™ Pelion

Table of contents

Introduction 1
The cellular IoT connectivity landscape 2
The importance of reliable connectivity 3
The financial impact of downtime 4
Key differences between MNOs and MVNOs and their implications 4
Introducing Pelion 5
Pelion's High Availability Transport Layer enables unified and secure connectivity 6
How eSIMs provide multi-network resilience and expanded coverage 7
Hardware considerations for reliable connectivity 8
Case studies 10
Conclusions and strategic recommendations 12

Introduction

The global cellular IoT market is growing at a rapid pace. Almost three decades after the launch of the first GSM data modules, cellular IoT has become a global $10+ billion industry connecting billions of devices that in turn power applications generating hundreds of $billions in revenue. As connectivity is becoming an increasingly central part of the strategies of many enterprises and OEMs, greater focus is placed on reliability, security, and support for international deployments.

Across industries like healthcare, manufacturing, and transport & logistics, businesses increasingly rely on reliable connectivity to ensure smooth operations and preserve efficiency. This white paper examines the impact of downtime and how multi-network connectivity, eSIMs, and thoughtful hardware selection can help businesses maintain high levels of service availability for their cellular IoT device deployments.

The cellular IoT connectivity landscape

Cellular technologies are positioned as high to mid-range technologies in the IoT market. Broadband 4G LTE and 5G meet the requirements of demanding applications in transportation and other data-intensive application areas. Cost-optimised 4G LTE technologies such as LTE Cat-1 and LTE Cat-1 bis similarly match the requirements of somewhat less demanding applications, especially if mobility is required.

LTE-M and NB-IoT push the boundaries of cellular IoT to include battery-powered devices and a wider range of low-cost devices. Berg Insight believes that the main strength of cellular technologies in the IoT market is the mature ecosystem, which has evolved over decades and currently produces hundreds of millions of new connected devices per year.

Comparison of cellular technologies for IoT use cases

Considerations	LPWA		Mid-speed	High-speed		
	NB-IoT	LTE-M	LTE Cat-1/Cat-1 bis	LTE Cat-4	5G RedCap	5G eMBB
Downlink peak rate	127 kbps	1 Mbps	10 Mbps	150 Mbps	220 Mbps	20 Gbps
Uplink peak rate	159 kbps	375 kbps	5 Mbps	50 Mbps	120 Mbps	10 Gbps
Energy efficiency	Very high	Very high	Medium	Low	Low	Low
Mobility	Medium	Very High	Very high	Very high	Very high	Very high
Latency	1.6s–10s	100–150ms	50–100ms	50–100ms	50–100	25–50
Voice support	No	Yes	Yes	Yes	Yes	Yes
Reliability	High	High	High	High	Very high	Very high
Module cost ($)	3–5	7–8	15–20/6–10	20–25	40–60	90–150
Future-proofness	Very high	Very high	High	High	Very high	Very high
Global coverage	Medium	Medium	Very high	Very high	Low	High

In 2024, the global installed base of cellular IoT connections grew to 3.8 billion. The market is going through a paradigm shift as stationary devices outnumber mobile devices used for applications like automotive telematics and fleet management. Over the past decades, adoption has spread from high-value assets to medium-value assets as the cost of connectivity has decreased.

The rise of LPWA technologies opens up new possibilities to address greenfield opportunities among low-value assets that cost less than $10. Product categories that make up a significant share of cellular IoT connections are connected vehicles, smart utility meters, alarm systems, and payment terminals, while three significant growth opportunities for cellular IoT waiting to take off are asset tracking, healthcare, and consumer products.

The importance of reliable connectivity

Connectivity plays an increasingly central role in major product categories and operational processes across industries. The trend accelerates the demand for reliable connectivity services, as downtime can have far-reaching effects that extend beyond temporary inconveniences, impacting revenue, productivity, customer outcomes, and reputation. Mobile network operators (MNOs) generally assure a specific level of operational support and uptime via Service Level Agreements (SLAs).

SLAs outline a target percentage of uptime, implicitly acknowledging that occasional outages can occur. Most SLAs offered by mobile operators guarantee around 99 percent service availability, or uptime. A service level of 99 percent uptime can however leave services down for hours at a time, all within contract limits. This perceived high service level can amount to more than 7 hours of downtime in a month and up to 3 days and 15 hours of downtime in a year.

Comparison of service levels and downtime

Service level	Downtime	Daily	Weekly	Monthly	Yearly
99 %	1 %	14m 24s	1h 40m 48s	7h 12m	3d 15h 36m
99.9 %	0.01 %	1m 26s	10m 5s	43m 12s	8h 45m 36s
99.995 %	0.005 %	4s	30s	2m 10s	26m 17s

The IoT market spans a broad range of use cases, ranging from mission-critical and business-critical to non-critical applications. At the mission-critical end of the spectrum, downtime can result in severe consequences. Mission-critical applications include use cases like remote patient monitoring, emergency response systems, industrial safety controls, and critical infrastructure monitoring. Solution providers in these areas place a premium on reliability and failover mechanisms to achieve stringent availability targets – often aiming for “five nines”, or 99.999 percent, uptime.

Business-critical IoT applications such as vehicle telematics, asset tracking, smart utility metering, insurance telematics, public transport management, home alarm systems, and payments, solution providers focus on maintaining smooth day-to-day operations and preserving efficiency. While downtime may not threaten human safety, it can lead to significant financial losses, reputational harm, and missed opportunities. In both mission-critical and business-critical scenarios, organisations need to match connectivity options and service-level commitments with the demands of their applications.

The financial impact of downtime

The financial impact of downtime is perhaps the most measurable metric, as downtime in many cases directly translates to lost revenue. According to a survey conducted by the networking company Opengear in 2023, 96 percent of US businesses experience at least one outage quarterly. The survey statistics also reveal that for each minute of disruption, 24 percent of organisations lose between -$2,501 and -$5,000. As an average, this figure equates to -$4,344 for every minute of downtime incurred, pointing to the need for increased connectivity reliability. This may not sound like much on an individual scale, but when accumulated over the course of frequent outages, it becomes significant. Taking the example of a service level of 99 percent, US businesses stand to lose up to -$22.8 million in revenue over the course of a year.

Comparison of service levels and financial impact for an average business

Service level	Downtime	Daily	Weekly	Monthly	Yearly
99 %	1 %	-$62,554	-$437,875	-$1,902,672	-$22,832,064
99.9 %	0.01 %	-$6,255	-$43,788	-$190,267	-$2,283,206
99.995 %	0.005 %	-$313	-$2,189	-$9,513	-$114,160

Beyond the immediate financial losses, downtime can lead to secondary costs such as reputational damage, diminished customer loyalty, and the logistical burden of restoring operations. In certain industries like retail, banking, and healthcare, unplanned outages can be especially damaging, threatening not only revenue but also compliance requirements and public safety. Moreover, repeated or prolonged outages may prompt customers to switch vendors, further compounding financial and operational damage over the long term.

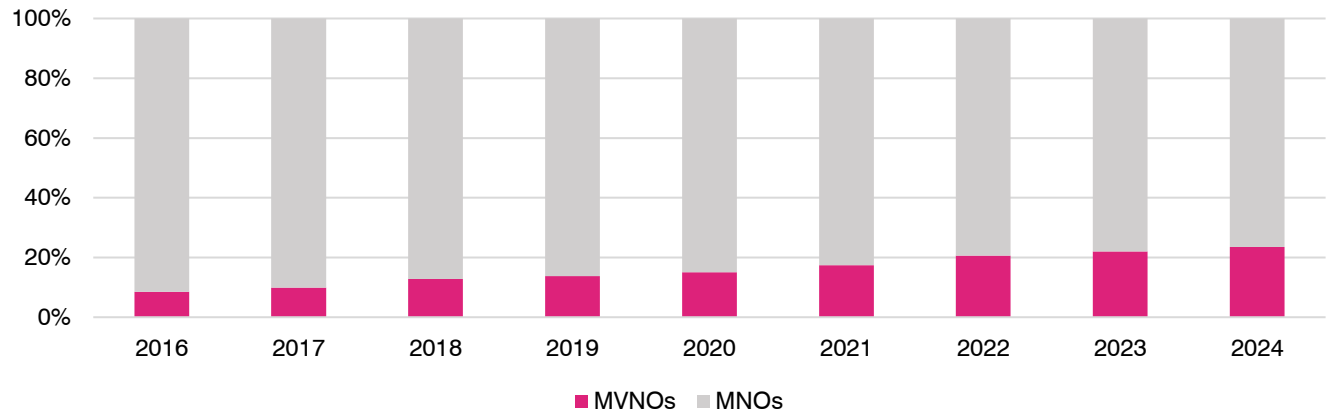
Key differences between MNOs and MVNOs and their implications

Mobile network operators (MNOs) and mobile virtual network operators (MVNOs) both play important roles as providers of cellular IoT connectivity services. MNOs own spectrum licenses and operate the radio access networks that are essential to deliver wireless services. Due to the nature of their business, MNOs typically operate on a national or regional basis. MNOs can often provide IoT connectivity services at competitive rates, leveraging their network footprints and ability to negotiate favourable roaming agreements. Services are however typically delivered through single networks inside the MNOs' footprints, which can limit service resiliency and coverage.

Unlike MNOs, MVNOs do not own spectrum or radio access networks but purchase network capacity at wholesale rates from MNOs. A key differentiator for MVNOs is the ability to aggregate multiple radio access networks and thus provide superior area coverage and multi-domestic footprints on a single platform. Established MVNOs typically also have more

advanced localisation capabilities through IMSI and eSIM profile donor agreements. As these players do not own and operate national radio access networks, they are becoming increasingly international, supporting customers in many parts of the world.

Share of IoT connections by MNOs and MVNOs (World ex. China 2016–2024)



In the IoT space, the main advantage of MVNOs is the ability to deliver multi-network connectivity, as connectivity solutions relying on a single network can result in inconsistent service. As shown in previous examples, a 99 percent SLA may still result in periods of costly downtime. This underscores the importance of multi-network connectivity, which ensures broader coverage and greater resilience by allowing IoT devices to seamlessly switch between networks when needed. Between 2016 and 2024, the share of IoT connections contracted to MVNOs has increased from 8 percent to 24 percent.

Introducing Pelion

Pelion, a global MVNO, is playing a pivotal role in delivering reliable IoT connectivity by providing scalable and flexible network solutions tailored to the needs of the growing IoT ecosystem. Pelion leverages existing infrastructure from major MNOs across the globe to offer businesses and organisations effortless connectivity for their IoT deployments. By utilising multiple networks, Pelion ensures that its customer's IoT devices remain connected, offering unmatched reliability, even in remote areas or under varying network conditions, which is crucial for industries like manufacturing, energy, transport, logistics, and healthcare.

What sets Pelion apart in the IoT space is its ability to bring together best-in-class solutions across connectivity, security, support, and reliability. Delivering connectivity services across various communication technologies, such as 3G, 4G LTE, 5G, NB-IoT, LTE-M, all optimised for diverse IoT use cases. So, businesses can future proof connectivity and reliably connect to 600+ networks across the world, using a single eUICC enabled IoT SIM.

Pelion's platform also allows for simplified subscriber management, seamless roaming, and real-time data analytics, which are essential for ensuring the smooth operation and cost control of IoT deployments. This versatility ensures that businesses can scale their IoT deployments with confidence, knowing that they have access to reliable, high-quality connectivity wherever their devices are located.

For industries that depend on real-time data, such as fleet management or remote monitoring, Pelion's solution guarantees minimal downtime and continuous performance. By providing a robust, multi-network IoT platform, Pelion ensures that businesses can unlock the full potential of their IoT solutions while enjoying cost efficiency, high reliability, and global reach. This focus on reliability and availability makes Pelion a trusted partner for any organisation looking to deploy IoT at scale.

Pelion's High Availability Transport Layer enables unified and secure connectivity

As IoT deployments scale globally, enterprises face challenges in ensuring seamless, secure, and low-latency connectivity across diverse networks and geographies. Pelion's High Availability Transport Layer addresses these challenges by delivering a private, resilient, and high-performance connectivity layer that abstracts complexity and enhances control over routing IoT data.

Integrated into multiple MNO's core networks, Pelion's private APN connects with multiple packet gateways in geographically distributed locations for each integrated carrier. This approach ensures redundancy, security, and consistent network behaviour, independent of the underlying infrastructure. Pelion's infrastructure ensures IoT device traffic remains isolated from other IoT devices, as well as consumer devices, offering end-to-end security while maintaining strict compliance with enterprise security policies. Key benefits include:

- **Private APN:** Ensures dedicated and secure IoT device communication, avoiding exposure to public Internet threats.
- **Consistent security policies:** Enforces centralised security configurations across all devices, regardless of the connected MNO.
- **End-to-end encryption:** Encrypts IoT data transmission to protect against unauthorised access and cyber threats.
- **Traffic isolation:** Prevents cross-network interference and reduces risks of congestion from consumer traffic.

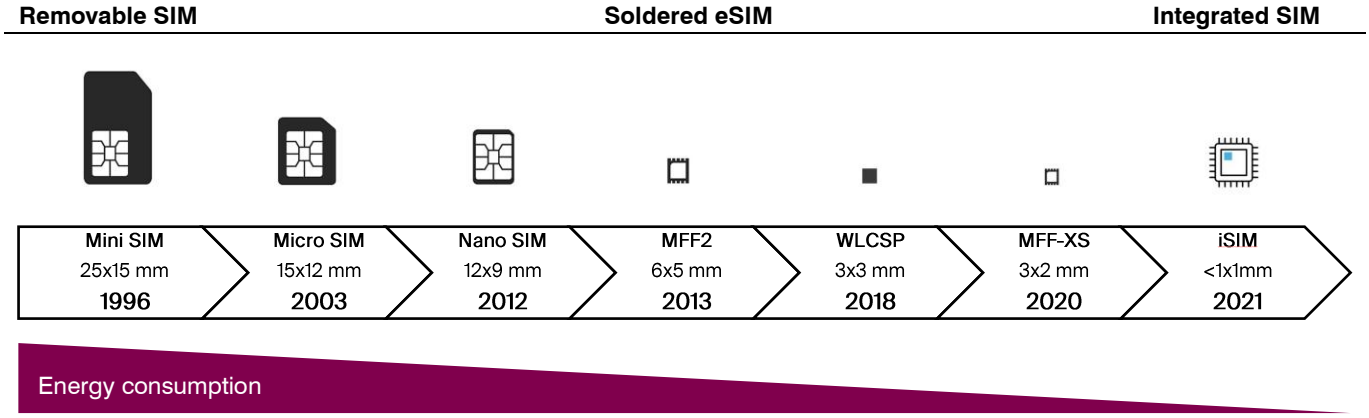
How eSIMs provide multi-network resilience and expanded coverage

Subscriber identity modules (SIMs) have played a major role in the success of cellular communications by providing a secure way to authenticate the subscriber to the network, linking the user subscription, device and network together. The IoT market has special requirements for SIM solutions which is one of the main drivers behind the development of new technologies and standards in this field. Traditional SIM cards are non-programmable, presenting a multitude of supply chain complexities, and are sensitive to a wide range of conditions common for industrial environments including high temperature, shocks, vibration and humidity. Two solutions address these problems: embedded SIM (eSIM) form factors and remote SIM provisioning (RSP).

SIM form factors and eUICCs

SIMs come in a range of standardised form factors, ranging from traditional, removable SIM cards to embedded SIMs. Standard SIM cards are typically associated with a single mobile operator profile. eUICC is a software component that provides the capability to store one or multiple mobile operator profiles on a single SIM and can be implemented in any form factor. The term eUICC, however, is commonly used interchangeably with eSIM. There are two main types of embedded form factors. An eSIM is integrated into the module or mounted on the PCB, while an integrated SIM (iSIM) is integrated into the design of a SoC or MCU.

Comparison of SIM form factors



Remote SIM provisioning

Remote SIM provisioning (RSP) is the process of remotely managing SIM profiles on a deployed SIM without physically changing the SIM itself. GSMA has played a key role in the standardisation of RSP technologies and published its first eSIM specifications for M2M and consumer use cases in 2013 and 2016 respectively. The technical specification for M2M devices is called SGP.02, while the technical specification for consumer devices is called SGP.22.

A challenge associated with the M2M Specification is the requirement for complex bilateral integration processes between mobile operators, as secure links must be established between two components called the SM-SR and the SM-DP, making it difficult to switch profiles between mobile operators. While the model is highly resilient and widely adopted by automotive OEMs, it is unsuitable for many other IoT use cases.

SGP.32 – the second coming of eSIM for IoT devices?

Addressing challenges related to the M2M specification, GSMA published the IoT eSIM specification, SGP.32, in 2023. The specification builds upon proven elements of both the consumer and M2M specifications to simplify the integration process for device makers and cellular IoT connectivity providers. A key design principle for the development of the eSIM IoT specification was to leverage existing SM-DP+ systems in order to simplify and accelerate deployments. More than 300 mobile operators had deployed SM-DP+ systems to support consumer eSIM services at the end of 2024, which will be technically able to support IoT eSIM services.

Other key features of the eSIM IoT specification include emergency call, roll-back, and fall-back features, as well as support for lightweight communications protocols. The emergency call feature enables emergency calls even if the primary profile is unavailable, while the roll-back functionality reverts to a known working profile if a new update fails. The fall-back mechanism enables the eSIM to switch to alternative or bootstrap profiles when coverage is insufficient.

Combined, these features greatly improve the reliability of cellular IoT connectivity services and keep devices operational in critical scenarios. Support for the CoAP and MQTT communications protocols is essential for constrained devices that cannot support SMS and HTTPS. The main barrier to full commercialisation of SGP.32-based solutions is the certification requirement of IoT eSIMs. The first GSMA-certified IoT eSIMs are expected to become available in the first half of 2025.

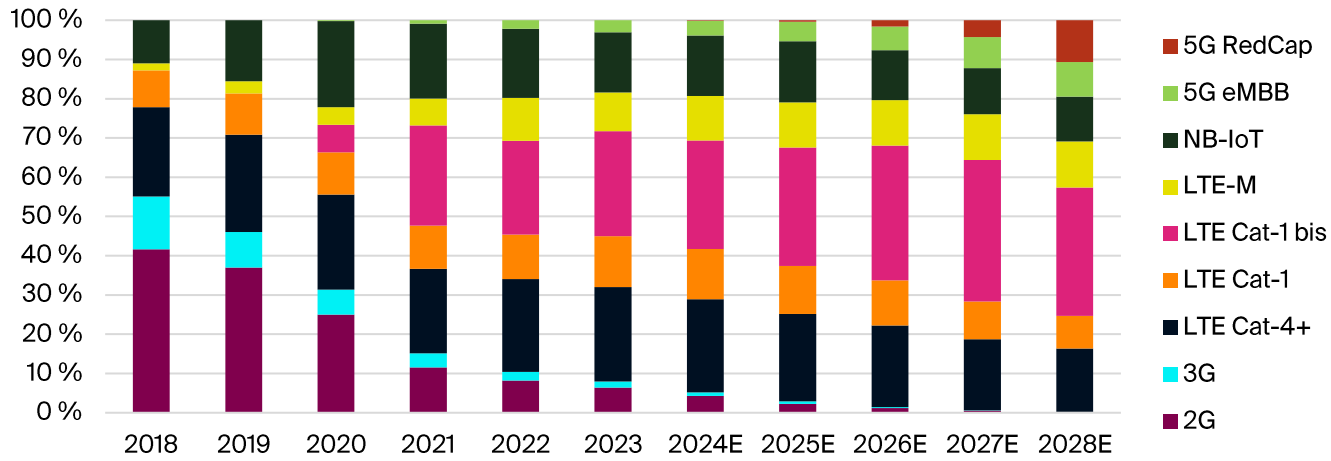
Hardware considerations for reliable connectivity

Beyond connectivity and SIM solutions, reliable connectivity is also the outcome of careful hardware design choices. And as the saying goes – hardware is hard. At a high level, the hardware stack for cellular IoT devices comprises two main components: cellular modules and antennas. The selection and implementation of these components are essential to achieve optimal performance in cellular IoT applications.

Cellular modules have been designed to meet demands from diverse IoT applications. In the early phase of an IoT project, the device maker needs to match a module with the best-suited cellular technology to a particular device, balancing factors such as speed, power

consumption, size, certifications, regional coverage, and cost. The most popular cellular technologies for new designs are today LTE Cat-1/LTE Cat-1 bis, LTE Cat-4, LTE-M and NB-IoT, though 5G eMBB and 5G RedCap are expected to become more attractive options in the coming years. Additionally, vendor support and firmware update capabilities also play a crucial role in managing long-term security and functionality.

Share of cellular module shipments by technology (World 2018–2028)



While cellular modules enable devices to connect to cellular networks, the antenna largely dictates how well a device performs wirelessly. Even though an antenna is a conceptually basic passive component, there are many challenges associated with their implementation. The complexity of RF design requires a deep understanding of electromagnetic principles, signal integrity and the intricacies of printed circuit board (PCB) design.

Major smartphone OEMs have teams of hundreds of engineers that design custom antennas for their devices. In contrast, cellular IoT device makers typically do not have the resources or scale to design antennas in-house and instead rely on specialised antenna vendors that provide off-the-shelf antennas, as well as custom antenna design services.

There are a range of types to choose from when deciding on what kind of antenna to use. The most important factors to consider are size, cost and performance. The ideal antenna has an infinitely small form factor, zero cost and excellent performance. This is however not possible in the real world and trade-offs must be made, meaning that there is generally no one-size-fits-all antenna solution. A key to successful antenna implementation is to address the challenge early in the design process, as ensuring antenna efficiency and performance often requires multiple design and test iterations.

Case studies

Case studies from Pelion's partners Gardner Denver and Oysta provide examples of use cases from two different industries – industrial and healthcare – with the need for reliable connectivity. These real-world deployments illustrate how robust IoT solutions can deliver continuous data flow, minimise downtime and support mission-critical operations across diverse sectors.

Gardner Denver leverages Pelion's connectivity to drive digital transformation in industrial equipment

Gardner Denver, a leader in air and gas compressors, sought to transform its business by embracing Industry 4.0 and delivering real-time data solutions to optimise plant performance. To make this digital shift possible, they partnered with Pelion for its flexible, global connectivity. Pelion provided the robust IoT connectivity and global network coverage necessary to power Gardner Denver's iConn platform, enabling remote diagnostics, predictive maintenance, and energy optimisation. With Pelion's seamless, scalable solution, Gardner Denver was able to focus on innovation while ensuring reliable connectivity for their global customers.

One of the key challenges faced by Gardner Denver was how to extract value from data collected by thousands of devices in remote locations, while retrofitting existing equipment for IoT enablement. With Pelion's robust connectivity solution, the company was able to focus on developing the iConn platform and enhancing user experience, instead of managing complex connectivity and network contracts.

At the heart of iConn's capabilities are IoT-enabled sensors integrated into compressors, collecting vital data such as vibration and temperature readings. This data is transmitted via eSIM and a 4G LTE network to a browser-based tool, enabling remote monitoring, analytics, and predictive insights. These insights not only highlight machine parameters but also predict trends that could signal potential failures, enabling predictive preventative maintenance (PPM) and reducing costly downtime.

The agility of Pelion as a partner also enables Gardner Denver to scale quickly, adding resources as needed while maintaining a single eSIM for all territories, simplifying deployment and reducing operational complexity. The partnership with Pelion has not only transformed Gardner Denver into a service provider but also helped the company expedite its growth from delivering basic analytics to offering cognitive data analysis processed at the edge.

Oysta's smart remote monitoring device, powered by Pelion IoT, ensures reliable, secure connectivity for independent living

Caring for vulnerable individuals, such as the elderly or those with other vulnerabilities, often means constant surveillance and worry. Oysta, a leader in remote telecare services, recognises this and has developed a comprehensive solution. Their customers, whom they call VIPs (Vulnerable Independent People), are individuals who desire to live independently but need reliable monitoring to ensure their safety and wellbeing. The challenge lies in ensuring these individuals remain connected without intruding on their independence, all while providing peace of mind to their families and caregivers. To achieve this, Oysta needed a connectivity solution that was not only dependable but also adaptable to the unique needs of their diverse user base.

The Oysta Pearl device is more than just a wearable or portable unit. It's an IoT-powered tool equipped with SOS buttons, fall sensors, reminder alarms, and safe zone monitoring. The device continuously transmits real-time data to Oysta's IntelliCare platform, which connects directly to 24/7 remote monitoring facilities. This integration helps ensure that emergency alerts and other critical information are received instantly, without delay, which is essential for the vulnerable population Oysta serves.

To make this solution work seamlessly, connectivity is paramount. Oysta sought a partner that could offer reliable, flexible, and secure connectivity to ensure that their devices would always stay online, no matter where they are. This is where Pelion stepped in, providing an IoT connectivity solution that guarantees reliable uptime across multiple network technologies, including GSM, satellite, Wi-Fi, 3G/4G, and NB-IoT. This flexibility allows Oysta's devices to adapt to the best available network, ensuring the reliability their customers need.

Mario Zuccaro, Oysta's Founder and CEO, explained, "We partnered with Pelion because nobody else could provide the solution we needed: a SIM that was able to roam across networks and provide seamless connectivity." Pelion's partnership with Oysta goes beyond connectivity – it's about collaboration and long-term success. Pelion's scalability has been key to Oysta's rapid growth. For instance, during the COVID-19 crisis, Pelion helped deploy 2,500 devices in just two weeks, supporting efforts to free up hospital beds and allow patients to recover at home.

Looking ahead, Oysta is expanding with the Oysta Pearl II, featuring new sensors for monitoring temperature, blood pressure, and environmental factors like air quality. Powered by Pelion's IoT connectivity, these devices provide a unified view of both the individual and their environment, enhancing predictive healthcare.

Conclusions and strategic recommendations

Reliable connectivity is not just a technical concern, it's essential for sustainable business growth. From industrial automation to healthcare monitoring and beyond, organisations depend on consistent and secure connectivity to support everything from routine tasks to mission-critical processes. Below, we explore key trends that emphasise the importance of reliable connectivity and illustrate how the right IoT connectivity partner can help drive operational excellence.

- Minimising downtime is crucial. Even a service level of 99 percent can leave services down for hours at a time, all within contract limits. As shown in a survey conducted by Opengear, US businesses stand to lose up to -$22.8 million in revenue over the course of a year with a service level of 99 percent. Downtime can also lead to secondary costs such as reputational damage, diminished customer loyalty, and the logistical burden of restoring operations. By prioritising high-availability solutions and clear redundancy strategies, businesses can mitigate these risks and sustain long-term growth.

- IoT connectivity solutions that leverage multiple networks markedly improve resilience. Devices can automatically switch to the strongest available connection, reducing the risk of coverage gaps and single points of failure. This multi-network approach is particularly beneficial for businesses managing large fleets of devices or operating across diverse geographies. A secure high availability transport layer further strengthens the reliability and security of IoT solutions.

- Selecting robust hardware, such as modules and antennas carefully matched with the specific application, ensures consistent performance under varying conditions. Using eSIM and multi-network connectivity solutions allows for hassle-free network updates and eliminates the need for onsite SIM swaps. Together, these measures help future-proof deployments against evolving technological and operational demands.

- Collaborating with a specialised IoT MVNO can simplify scaling and global expansion as these providers typically offer flexible service-level agreements, unified SIM management and access to multiple MNO networks. By entrusting connectivity challenges to an expert partner, businesses can focus on innovating and delivering value in their core areas.

Berg Insight is an independent industry analyst and consulting firm, providing research, analysis and consulting services to clients in the areas of IoT and digital technologies. Our analysts possess deep expertise in major IoT verticals such as fleet management, automotive telematics, smart metering, smart homes, mHealth and connected industry. Founded in 2004, we operate on a global basis from our head office in Sweden.

Our clients include many of the world's largest mobile operators, vehicle OEMs, fleet management solution providers, wireless device vendors, content providers, investment firms and venture capitalists, IT companies, technology start-ups and specialist consultants. We have provided analytical services to 1,500 clients in 72 countries to date.

If you have any questions about our market report subscriptions and advisory services or simply want to understand how Berg Insight can help you, don't hesitate to contact us at info@berginsight.com.

© 2025 Berg Insight AB. All rights reserved. Berg Insight is an independent producer of market analysis. This Berg Insight product is the result of research by Berg Insight staff. The opinions of Berg Insight and its analysts on any subject are continuously revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. Berg Insight disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.