IoTNOW
HOW TO RUN AN IoT ENABLED BUSINESS

robustel

The IoT Now Mission Critical Connectivity Handbook 2025

How cellular connectivity can build trust for mission critical use cases

Introduction

Determining when a connection is critical is an open question and comes with highly subjective answers. At one extreme, most would accept that life safety use cases are mission critical and the highest levels of monitoring, robustness and security should be deployed. Below the life critical category, there are a raft of applications from alarms and security cameras to lift monitoring and water safety that can be considered as critical. These typically have similar considerations as critical national infrastructure.

Next most critical are mission critical commercial use cases. These are essential to conduct business and serve customers, though typically not life or injury-threatening situations. Transforma Insights says that typical examples here include payment terminals, where lack of service will prevent businesses from taking payments. Other examples relate to manufacturing and supply chain operations such as real-time location systems, some track and trace apps, warehouse management systems and fleet management.

Less critical but still important commercial considerations follow, such as systems for remote machinery diagnostics and maintenance applications. These can cope with short periods of unavailability but connectivity is needed most of the time to deliver value to an organisation. Finally, non-critical use cases, such as white goods, don't need to be connected to function so their connectivity isn't critical.

When communications are truly critical, failing over to a single backup operator isn't always going to assure uninterrupted connectivity. As security threats to networks intensify and coverage and quality issues continue, the traditional failover approach to a single backup operator isn't good enough for mission critical communications. Fortunately, solutions such as multiple SIMs from multiple carriers are now available and can be integrated into IoT devices, routers and gateways.

The move to robust 4G and 5G cellular connections

Life critical communications have been moving away from safety-specific networks such as land mobile or TETRA and turning to cellular alternatives as LTE and 5G have become widely available. In these use cases, 99% uptime is unacceptable so a new approach to resilience is needed that enables failover to multiple operators. Ideally, an alternative operator should be based in a different country to protect against whole-country issues that affect service provision and this should be set up in a seamless way with the connection monitored so it can switch over in the event of poor or no performance.

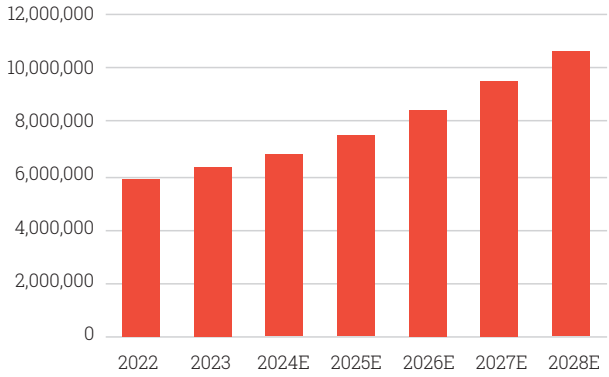
Only by combining continuous monitoring and seamless switching to unaffected operators can cellular connectivity be fully-trusted for mission critical use cases. For large scale use cases or those that utilise sensor networks, the role of a cellular router has become a critical enabler of connectivity. The router can provide the assured, secure connectivity applications need and the market has been bringing new innovations to user organisations that have transformed resilience and performance over the last ten years.

The introduction of robust, mission-critical routers that now offer dual SIM, roaming SIM and multi-carrier/multi-SIM products has been a substantial change and is seeing large volumes of robust cellular routers being deployed in support of IoT use cases across industries. The cellular router and gateway market is driven by the growing need to connect assets and workforces in remote and temporary locations as enterprises digitalise their operations.

Market growth

Annual shipments of cellular routers and gateways amounted to 6.3 million units in 2023 according to analyst firm Berg Insight, generating annual revenues of US$ 1.6 billion[1], an increase of 3% from the previous year. The Americas is the largest regional market, accounting for about US$764 million. The average selling price in the region is significantly higher compared to other markets, primarily due to a higher share of feature-rich, high-speed 4G LTE and 5G devices in the product mix. The market value of the European and Asia-Pacific regions accounted for US$424 million and US$343 million respectively. Berg Insight forecasts that the market will grow at a CAGR of 12.0% to reach US$2.8 billion in 2028.

Figure 1: Cellular router and gateway shipments (World 2022-2028)



Source: Berg Insight

Only by combining continuous monitoring and seamless switching to unaffected operators can cellular connectivity be fully-trusted for mission critical use cases

[1] https://media.berginsight.com/2024/11/01152926/bi-terminal8-ps.pdf

Private networks for critical connections

4G and 5G connectivity has become the standard for critical communications and Industrial IoT (IIoT) customers with mission-critical operations that are looking for a private network solution will choose private 4G or 5G over non-cellular alternatives, reports ABI Research, which estimates these users will drive revenue to US$112.6 million by 2029[2].

The firm says many mission-critical, private cellular IoT needs are found in industrial segments such as utilities. Use cases also include health and safety monitoring in mines, where customers can use private 5G networks to automate mining equipment, such as drill rigs or haulage vehicles. Automating such heavy equipment can improve the safety of raw material transfers, while also producing important data for predictive maintenance.

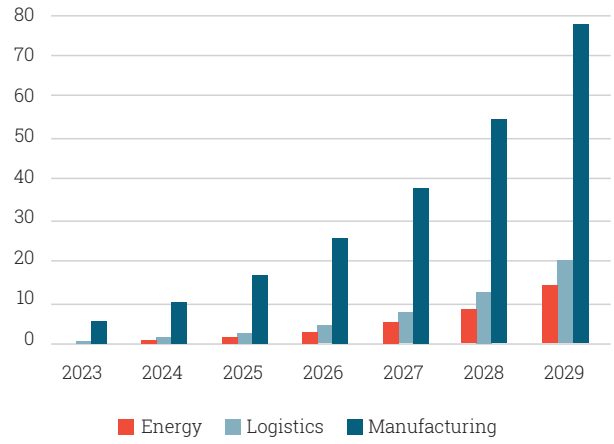
Video surveillance is one of the popular mission-critical IoT applications for private 5G, with live remote video streaming being a critical operational tool for lone workers who must oversee industrial sites like utility plants or ports. Lone workers using a private 4G- or 5G-enabled camera can provide real-time feedback on their work and safety, rather than relying on voice-only communication. These critical, IIoT use cases can help justify the purchase of a relatively expensive private cellular network and will partly drive total private network IoT connections in the future.

Routes to success in critical communications

The critical communication router market is characterised by high-end providers which create highly-customised routers to address customers' specific needs. These highly robust solutions offer multiple carriers, smart roaming functionality and are built specifically for the harsh realities of critical use cases. That might involve extremes of heat or cold, prevention of moisture ingress or ruggedised casings to protect the router from damage.

Ultimately, the limitation here is cost. A deploying organisation can select every critical functionality they need and fine tune the solution for the exact needs of their deployment scenarios. However, with mass scale IoT deployments now the norm, very expensive routers, even for high value mission critical use cases become unsustainable.

Figure 2: Private 4G and 5G IoT Connections by Market Segment



Source: ABI Research

The firm says many mission-critical, private cellular IoT needs are found in industrial segments such as utilities

[2] https://go.abiresearch.com/hubfs/Marketing/Whitepapers/66%20Must-Know%20Tech%20Stats%20For%202025/ABI_Research%2066%20Must%20Know%20Tech%20Stats%20For%202025.pdf

Cost vs. quality

At the other end of the scale, highly cost-effective routers and gateways can be bought at scale. These will contain standard features such as dual SIM capability and some of the robustness of high-end solutions. However, costs will have been saved on all aspects of the device so resilience may drop off during the life of the deployment and certain deployment characteristics may not be fully addressed by these solutions. In addition, lower cost solutions often lack the usability, support and cloud-based management capabilities that higher quality options offer.

There is a middle ground between cheap yet flawed robust routers and gateways and highly-specified yet expensive high-end mission-critical routers. A segment of vendors has emerged that combine the usability, flexibility and quality of high-end providers with a more appealing cost base. Providers here deliver quality designs that have been fully tested and certified and combine these with cloud platforms for simple management of large installed bases of mission critical routers.

How Robustel helps

Robustel, which has been providing industrial quality solutions for IoT including wireless modems, routers, gateways, edge compute devices and cloud software for over 15 years, has several million devices deployed globally in a wide range of environments from the extreme to the everyday. The company combines high-quality engineering with competitive pricing, helping organisations in sectors such as security, oil and gas, healthcare, manufacturing, agriculture, transport, utilities, smart cities and smart retail overcome their toughest connectivity challenges. Robustel's portfolio spans 3G, 4G and 5G technologies, as well as Wi-Fi and low-power wide-area networks (LPWAN) specifically LoRaWAN — enabling resilient, future-ready connectivity for mission-critical applications

An increasingly important part of delivering mission critical communication is plug and play failover to SD-WAN in order to provide a 5G backup route. The ability to locate a router externally increases the likelihood of receiving a strong 5G signal so a robust router that allows businesses to utilise SD-WAN can provide the back-up a use case needs.

In addition, innovations such as 5G RedCap are opening new opportunities for mission critical connectivity. Robustel is actively exploring solutions in this space, working closely with mobile network operators across the world to ensure the business case and market requirements are right before bringing devices to market.

Robustel's focus on mission critical use cases means it has huge experience of supporting customers and has done the groundwork to ensure compliance with regulations in customer markets and that security requirements are addressed. The company takes a holistic approach to security and maintaining ISO security standards, conducting annual penetration testing across its device firmware, operating systems and cloud platforms. Potential vulnerabilities are proactively identified and addressed before they can be exploited, and cloud services are hosted on Microsoft Azure to ensure enterprise-grade resilience.

Cloud management

The cloud functionality is essential for managing large volumes of routers and gateways across the globe with the different carrier and regulatory requirements that involves. That global capability is vital for many mission critical IoT deployments and provides strength and depth that national or regional device providers can't match.

Robustel can also streamline development of solutions thanks to its flexibility. The company has its own factory and its own software engineering resources so, if a small adaptation to the firmware is required, it can be easily expedited.

Having been in this market for 15 years during which its core team in China has remained in place, as well as its specialists in the UK, Germany and Australia, Robustel has been able to build long term relationships with customers. This is important to build trust and for organisations with long lifecycle devices, it's essential to know that their vendor will be with them for the duration of that deployment. At its core Robustel sees its value in understanding the needs of customers and then working to find the right fit from within its portfolio.

Use case example – Smart water management

From the drought-sensitive central Anatolian plains to the snow-laden highlands of Kars, managing water effectively is a national imperative in Turkey. Since 2014, GSL, an IoT integrator in Turkey, has partnered with Robustel to deliver innovative connectivity solutions across energy, utilities and critical infrastructure. The companies' latest collaboration focuses on deploying Smart Water Management Systems in coordination with Turkey's top water authorities: the General Directorate of Meteorology (MGM), the Ankara Water and Sewerage Administration (ASKI) and the State Hydraulic Works (DSI).

These agencies are moving beyond reactive models, introducing sensor-based systems that collect real-time data across basins, reservoirs and remote mountain sites. Backed by SCADA platforms and cellular telemetry, this infrastructure helps ensure environmental sustainability, public health and national compliance with global water governance standards.

The environment can be brutal for environmental infrastructure. In Ankara, water basins sprawl across semi-arid lowlands, requiring sensors to be deployed across vast, hard-to-reach distances. In contrast, the Kars region in the northeast experiences extreme winter conditions, with snow and ice covering high-altitude reservoirs for months at a time. These vastly different conditions created logistical and environmental barriers for deploying water quality monitoring systems.

Autonomous devices

Sensor nodes were installed on buoys floating in remote reservoirs, some of which were only accessible by boat, while others were placed at altitude on rugged terrain. In both scenarios, technicians had limited access for setup, calibration or maintenance. Traditional cabling for power or data was out of the question. The systems needed to be 100% autonomous, climate-resilient and capable of operating for long periods without physical intervention.

This diversity in deployment sites meant that a one-size-fits-all approach was impossible. The solution needed to adapt to both mobility on water and harsh topography on land, without sacrificing performance. For Turkey's public water agencies, ensuring nationwide consistency in water quality monitoring demanded a solution that was flexible, rugged and technically fit for both extremes.

To compound the challenges, across Kars and other remote Turkish provinces, GSM signal quality ranged from weak to non-existent. Even in Ankara, known for its infrastructure investment, many basins and reservoirs fell into coverage dead zones or zones with unstable bandwidth.

Conventional routers lacked the network resilience to adapt. With limited support for multi-network SIMs and intelligent failover, these devices either stalled when a signal dropped or required manual intervention to reset. This was unacceptable for a system expected to run 24/7, often unattended.

The systems needed to be 100% autonomous, climate-resilient and capable of operating for long periods without physical intervention.

The Robustel R1511

After a thorough evaluation of environmental, technical and operational constraints, Turkish technology integrator GSL selected Robustel's R1511 router as the backbone of the communication infrastructure. Compact, robust and purpose-built for industrial deployments, the R1511 delivered on every requirement for Turkey's water monitoring modernisation project.

As Robustel's local integration partner, GSL provided on-the-ground support for equipment specification, procurement and installation. Drawing on its deep understanding of both Turkish regulatory frameworks and field engineering, GSL ensured that every device was installed in compliance with environmental and operational requirements. Their coordination with public agencies also ensured that timelines were met and system testing was conducted smoothly.

As a Robustel partner since 2014, GSL played a pivotal role not only in solution selection but also in ensuring rapid procurement, configuration and deployment across complex terrain. Drawing on deep knowledge of local infrastructure and regulatory frameworks, GSL's technical team integrated RS485-based sensor data into central SCADA systems via Robustel's R1511 routers, facilitating real-time communication with minimal power requirements. GSL continues to provide ongoing technical support, ensuring uptime and system stability across seasonal cycles.

RCMS for future scale

Robustel's cloud-based device management platform, RCMS, can be enabled as a future enhancement. Once fully adopted, RCMS will allow key stakeholders to remotely monitor router status, push firmware updates and ensure device uptime from a central dashboard, further increasing operational efficiency. The deployment of Robustel's R1511 industrial router has delivered measurable impact across Ankara and Kars, advancing the national agenda for Smart Water Management Systems in Turkey.

Mission critical connectivity checklist

Mission-critical IoT requires more than connectivity; it demands resilience, security and long-term trust. Executives should consider evaluating potential vendors/partners against the following five non-negotiables:

Resilience

Why it matters: Enterprises cannot tolerate downtime. Multi-carrier connectivity with seamless fail-over is the baseline for maintaining business continuity in mission-critical IoT. Robustel enhances this with smart roaming which ensures unsteered roaming and multi-SIM deployments automatically choose the strongest network — going beyond basic SIM failover.

Security

Why it matters: Evolving threats mean IoT devices must be protected at the same standard as enterprise IT systems. Compliance, penetration testing and data protection are essential. Robustel applies ISO-certified processes, annual penetration testing and hosts Robustel Cloud Manager Service (RCMS) on Microsoft Azure for enterprise-grade security and resilience.

Lifecycle Assurance

Why it matters: Mission-critical deployments run for years. Vendor stability, long-term support and proven field experience are critical to protecting investments.With more than 15 years in the market, millions of devices deployed and long-tenured global engineering teams, Robustel provides continuity throughout the lifecycle of customer deployments.

Cloud Management

Why it matters: Managing large fleets requires more than a dashboard - it demands tools for provisioning, monitoring, updates and integration into enterprise workflows. RCMS is a toolbox with zero-touch provisioning, real-time monitoring, OTA updates, robust VPN access and open APIs to integrate seamlessly with ERP, CRM and orchestration systems.

Adaptability

Why it matters: Harsh conditions and regulatory demands mean off-the-shelf solutions rarely fit. Flexibility is essential for scaling reliably across environments.Robustel's in-house factory and software teams deliver tailored hardware and firmware adaptations quickly - without sacrificing certification or scalability.

Conclusion

The demands and variables that are inherent to all mission critical IoT deployments mean that organisations can't simply take a router off-the-shelf and expect it to meet all their deployment's needs. Climate extremes, harsh external conditions, patchy cellular coverage, lack of access to power supply, inaccessible locations and cost constraints all play their roles in determining what products can be selected. The near-ubiquitous availability of cellular networks coupled with the dual and multi-carrier SIM era has transformed resilience, enabling multiple means for a device to failover to an alternative operator, ideally seamlessly.

This, combined with the ability to flexibly and securely manage, a new breed of cost-optimised, thoroughly engineered, range of routers and gateways specifically designed for mission critical IoT, is creating the trusted environment that enterprises and organisations need to expand their critical IoT operations. The margins are appealing but the stakes are high so it's essential that large fleets of devices can be managed by solutions from trusted partners who understand the varied landscapes of the mission critical world. Building on that trust is fundamental to future success.

When resilience and trust matter most, Robustel is more than a vendor. We're a long-term partner with 15 years of global experience helping enterprises, OEMs, and MNOs secure, scale, and simplify mission-critical IoT.

Learn more or connect with an IoT expert at **robustel.com**