WIRELESS LOGIC **WHITEPAPER**

wireless logic

Maximising uptime for IoT

How to achieve high-availability and cyber-resilience in IoT

wirelesslogic.com

Why Business Leaders should **care more about connectivity**

In an increasingly connected world, maintaining seamless network uptime for IoT devices is more crucial than ever. IoT is used for safety critical applications, for optimising business operations, delivering innovative services and creating customer loyalty. In all cases, resilient connectivity is vital and increasingly mandated by enterprises and regulators across all industry sectors.

This guide outlines the measures which must be implemented in devices, networks and operational processes to achieve high availability and resilience in IoT where complex telecom environments, cost of ownership challenges and cyber threats are on the rise.

Learn about the implementation details which are needed in devices, the cloud environment and in your Communication Service Providers network to create resilience, secure connectivity and faster, automated recovery should an outage occur.

Don't treat connectivity as a cost of doing business. A reliable, secure and resilient connectivity service will help you differentiate in the market, achieve compliance with Enterprise and Industry standards and keep you out of the crosshairs of regulators.

Contents

Reliability and Resilience:

Market drivers and Regulatory landscape

Standards bodies like ISO, ETSI, NIST combined with IEC safety and sector specific standards have served industry well as guidelines and frameworks for best practice. They and their global equivalents are now mandatory in the majority of markets.

As the world strives for greater and increased safety and security, energy efficiency, less waste and on improving lifestyles and wellbeing it is increasingly reliant on connectivity. In turn this has created targets for cyber-criminals and concerns about data security and privacy from the consumer and business communities.

As a result, governments have legislated, most notably with the EU Cyber Resilience Act, China's Cyber Security law and the Telecom Security Acts in USA and UK. Mature markets in Asia-Pacific (Japan, South Korea, Australia, Singapore, Malaysia, Indonesia) and Americas (Brazil, Canada, Mexico) have equivalents.

Standards or directives like ISO 27001, ISO22301, NIS2, NIST CSF and GDPR serve as a good proxy for the global landscape. With legislation now in force, these standards are no longer optional. **They now impose requirements designed to ensure continuous availability of devices and networks, protection and rapid recovery from disruptions and cyber-resilience and data privacy.**

In this paper we will illustrate what this means for Communications Service Providers and product/device OEMs, Service Providers and Enterprises.

Table 1 shows how the ISO, ETSI, NIST and other standards fit in an overall structure covering supply chain, risk management through to application and device security. All of these layers will apply in varying degrees to IoT solutions and all contribute to achieving the high uptime goal. There will be numerous sector or industry specific regulations in addition to those listed and the GSMA ***Global IoT Regulations*** guide provides a helpful supplementary view.

Enterprises, OEMs and Solution Providers need to consider this full spectrum (in Table 1) and design accordingly based on their business priorities and attitude to risk. In doing that , they also need to recognise that downtime can be caused by a wide range of factors including electro-mechanical failure/damage, inadequate maintenance, power or network outages and cyber-attacks like ransomware infections or denial of service attacks against related systems.

Later in the document, we examine the critical role played by communication service providers in achieving compliance with the relevant standards, delivering operational excellence and creating differentiation using ***Case Studies***.

Table 1: Example legislation, regulation, and standards structure

Supply Chain Ensuring third-party products and services comply with security standards.	ISO/IEC 27036, 28000:2022 NIST 800-161
Risk Management Managing security risks and ensuring governance.	ISO/IEC 31000 ISO/IEC 22301 NIST 800-37
Incident Response Frameworks for handling and responding to cybersecurity incidents.	ISO/IEC 27035 NIST 800-61, PCI DSS, GDPR and HIPAA
Cloud and Infrastructure Security Specific guidelines for securing cloud environments and infrastructure.	ISO/IEC 27017 Cloud Security Alliance (CSA) STAR Certification NIST SP 800-144
Data Privacy Regulations governing personal data protection and privacy rights.	GDPR, CCPA (California), VCDPA (Virginia) and CPA (Colorado). ISO/IEC 27701
Security Management Overarching cybersecurity frameworks for organisational management.	ISO/IEC 27001 NIS2 Directive (EU) NIST CSF
Network Protecting communications infrastructure and data in transit.	ISO/IEC 27033 CRA and NIS2 Directive (EU) NIST CSF
Application Security Standards and frameworks for securing software and applications.	ISO/IEC 27034 NIST 800-53
Device Security Focus on hardware, IoT, and embedded systems.	ISO/IEC 27002 EU CRA and UK PSTI ETSI EN 303645 NIST CSF US Cyber Trust mark

CSP strategies for maximising uptime

The best Service Providers in the Cloud, IT and IoT domains use a combination of strategies to ensure reliable, secure, and efficient operations which maximise uptime and resilience.

In the IoT space there are some added dynamics which don't exist to the same extent in the more controlled IT environments where the IT department has more complete control over network equipment, wired/wireless connectivity (ethernet, WiFi), policies and devices (typically a small number of approved desktop, laptop, tablet devices plus printers).

In contrast, the IoT world has a massive number of different device types and wireless technologies. Devices are almost always deployed outside of the IT domain both physically and virtually. There is less control over local wireless conditions, network congestion or availability or the regulatory and commercial landscapes especially for international deployments.

In IoT it is equally vital that OEMs, Solution Providers and Enterprises all adopt the same comprehensive set of best practices and ensure they are applied at device, network and cloud infrastructure levels. Of course, a big part of the solution will come from your Communication Services Provider but that is not absolute especially and most obviously at a device level and in your Enterprise systems.

These practices are listed here and cover a range of domains including infrastructure management, security, operational processes, and customer communication. Here are the primary best practices in summary:

The best practices

To ensure reliable, secure, and efficient operations while maximising uptime and resilience, Cloud, IT, and IoT service providers should adopt the following best practices:

1. **Infrastructure Resilience:**
   Design networks and systems with redundancy to prevent single points of failure. Use load balancing and auto-scaling to handle demand fluctuations. Implement georedundancy and automated failover to ensure continuous service, even during outages.

2. **Security:**
   Implement a Zero-Trust Architecture with robust Identity and Access Management (IAM), including multi-factor authentication (MFA) and role-based access control (RBAC). Encrypt data at rest and in transit, perform regular vulnerability scans, and use strong endpoint protection and network segmentation to mitigate risks. Automate patch management to address vulnerabilities swiftly.

3. **Disaster Recovery:**
   Establish a comprehensive disaster recovery (DR) plan with frequent backups using the 3-2-1 strategy (3 copies, 2 media, 1 offsite). Test DR procedures regularly, ensuring swift recovery after incidents. Define and meet RTO (Recovery Time Objective) and RPO (Recovery Point Objective) in line with SLAs.

4. **Monitoring and Predictive Maintenance:**
   Use real-time monitoring and observability tools for infrastructure, applications, and IoT devices. Leverage AI-driven predictive analytics to anticipate failures. Centralise log management for faster detection of issues and automate alerting and incident management.

5 **Automation and Orchestration:**
Use Infrastructure as Code (IaC) tools like Terraform and Ansible to automate provisioning, configuration, and scaling of infrastructure. Implement CI/CD pipelines to ensure rapid, reliable software updates. Enable self-healing systems to automatically detect and correct issues.

6 **Service Performance Optimisation:**
Conduct regular capacity planning and optimise performance by using Content Delivery Networks (CDNs), caching, and edge computing to reduce latency. Apply API rate limiting to prevent overloading and improve system efficiency.

7 **Change Management and Governance:**
Use formal change control procedures to reduce risks when implementing updates. Maintain version control for configurations and audit systems to ensure compliance with regulatory standards such as GDPR and ISO 27001.

8 **Customer Communication and Support:**
Provide transparent updates during incidents through status pages and regular communication. Offer self-service tools for customers to monitor their services. Proactively notify customers about potential issues using automated alerts.

9 **Sustainability:**
Optimise energy usage in data centres through virtualisation, containerisation, and power-efficient hardware. Monitor energy consumption to align with sustainability goals and reduce the overall environmental footprint.

By applying these practices, service providers can **ensure high levels of uptime, security**, and **operational efficiency**, **enhancing customer satisfaction** and **minimising service disruptions**.

CSP strategies for maximising uptime *(continued)*

The key questions you should ask your IoT Comms Service Provider

Based on decades of experience and customer engagement on formal RFI and procurement processes, we have compiled a set of questions you should ask your IoT Comms Service Provider before you embark on a new deployment with them.

These targeted questions will help you assess IoT Communications Service Provider cyber-resilience and high-availability (uptime) around key areas including infrastructure security, incident response, service availability, and regulatory compliance.

Network Infrastructure	How do you ensure the security of your communications infrastructure?
	What encryption standards do you use for data in transit and at rest?
	How is your network segmented to isolate sensitive data from less secure traffic?
	What protections do you have in place to mitigate Distributed Denial of Service (DDoS) attacks?
	Do you use firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), or network monitoring tools?
	How do you handle security patching and updates across your infrastructure?
	What access and quality controls are in place for managing and securing devices within your network?
	How often do you conduct vulnerability assessments and penetration testing of your infrastructure?
Compliance with Standards & Regulations	Are you certified under any industry standards such as ISO/IEC 27001, CRA/NIS2, TSA, NIST CSF, or others?
	What is your process for responding to audits and regulatory inquiries?
	Can you provide audit reports or third-party assessments of your security practices (e.g., SOC 2 Type II)?
	How will you ensure that our IoT devices remain compliant with GSMA and local Government/Carrier regulations over time (e.g. permanent roaming restrictions)
Data Protection & Privacy	How do you handle sensitive or personal data (e.g., encryption, data minimisation, retention policies)?
	Where is the data stored, and are your data centres geographically distributed to comply with data residency requirements?
	How do you ensure data in transit remains within regulatory borders?
	How do you handle cross-border data transfers and ensure compliance with data protection laws in different regions?
	What measures are in place to prevent unauthorised access to customer data?
	How do you enable customers to fulfil requests related to data subject rights (e.g., access, deletion, rectification)?

Incident Response & Monitoring	Do you have a documented incident response plan? Can you share the key aspects of your plan?
	How do you detect and respond to cyber threats or anomalies in the network?
	Do you offer real-time monitoring of services, and what kind of alerts do customers receive in the event of a breach or outage?
	What is your policy for reporting security incidents or breaches to customers?
	Do you have dedicated security operation centres (SOCs) for 24/7 monitoring of potential threats?
	How quickly do you respond to and mitigate security incidents?
High Availability & Disaster Recovery	What is your guaranteed uptime (SLA) for communications services?
	What redundancy and failover mechanisms do you have in place to ensure high availability?
	How do you ensure continuity of service in case of a natural disaster, power outage, network outage, or cyberattack?
	What is your disaster recovery plan, and how often is it tested?
	Do you have geographically diverse data centres to prevent downtime due to local outages?
	How do you prioritise recovery in the event of a failure or cyberattack?
Flexibility & Scalability	How do you ensure that your network infrastructure can support future scalability demands in terms of IoT device connections, data volume and latency?
Backup & Data Retention	What is your backup strategy for communications data, and how frequently are backups performed?
	How do you ensure that backed-up data is secure (e.g., encryption and access control)?
	How long do you retain customer data, and can customers configure data retention settings to meet their internal policies?
	How do you handle backup data restoration in the event of a system failure?
Third-Party Risk Management	Do you rely on any third-party providers for services, and how do you vet their security practices?
	How do you ensure that your third-party vendors comply with your cybersecurity and availability standards?
	What contractual agreements do you have with third-party vendors regarding security and service availability?

CSP strategies for maximising uptime *(continued)*

Change Management & Service Updates	What is your process for rolling out updates or changes to your infrastructure?
	How do you notify customers of planned maintenance or changes that could impact service?
	How are updates tested before being implemented in production environments?
	How do you handle unplanned downtime or emergency updates, and what are your communication procedures?
Customer Control & Transparency	What level of control do customers have over the configuration and security settings of the services you provide?
	Do you provide visibility into your security measures and network health through dashboards or regular reports?
	Can customers conduct their own audits or assessments of your infrastructure and security measures?
	Do you offer security awareness training or resources for your customers?
Performance Metrics & Reporting	What key performance metrics (KPIs) do you track to ensure service reliability and security?
	How do you report on system performance, and what level of detail is provided to customers?
	Can customers access real-time and historical data on performance, incidents, and outages?
End-of-Life Support and Migration	How do you handle end-of-life support for outdated technology or services?
	What is your plan for migrating customers to new technologies or platforms with minimal disruption?
	How do you ensure that security is maintained during migrations or upgrades?
Cost Implications of Cyber-Resilience	What are the costs associated with ensuring high availability, security, and compliance?
	Are there additional fees for premium security services or extended SLAs?
	Do you offer scalable solutions for cybersecurity and availability based on customer size and risk?

Business Sustainability & Roadmap	Please provide detailed information regarding your company's financial health and long-term viability, including but not limited to revenue, profitability, long-term financial strategy & M&A activity.
	Please provide details on your company's investment in Research and Development (R&D), including, the percentage of annual revenue allocated to R&D over the past three years and how your company's R&D spending aligns with its long-term innovation strategy.
	Describe notable R&D initiatives or projects that directly contribute to enhancing your service offerings, including but not limited to 5GSA, eRedCap, IPv6, Packet Gateway distribution, cyber-resilience, carrier partnerships, remote SIM provisioning, eSIM and iSIM partnerships.

These questions are compiled from analyst engagements, consultant advice and customer RFI processes and provide a comprehensive assessment of Communications Service Provider ability to deliver robust cybersecurity, protect critical assets, and maintain high levels of service availability. Furthermore, they help assess whether the provider has the appropriate policies, infrastructure, and commitment to meeting industry standards and regulatory compliance requirements.

Contact us...

to discuss any of the content in this guide and receive a breakdown of how Wireless Logic addresses high-availability and cyber-resilience requirements for Enterprises using IoT.

CSP strategies for maximising uptime *(continued)*

Why cellular is the most resilient connectivity technology

When comparing different wireless technologies, it is important to consider the wider set of factors involved in technology choice. To that end, Table 2 summarises some of the key differences between popular wireless technologies alongside the resilience criteria. Bluetooth Low Energy (BTLE) has low resilience but has also proven to be a perfectly good solution for certain use-cases in the home or car.

For the majority of IoT and many Enterprise application's cellular technologies will be the most resilient and reliable option for critical applications that require consistent and secure communication, especially in dynamic or unpredictable environments.

1 **Wide Coverage and Ubiquity**
Cellular networks offer extensive coverage, often spanning vast geographic areas, including remote and hard-to-reach locations.

2 **Eco-system and Interoperability**
Cellular networks are based on well-established global standards developed by organisations such as the 3rd Generation Partnership Project (3GPP) and GSMA to ensure a high degree of interoperability across devices and networks worldwide. The Comms Service Provider ecosystem is an expansive group of MNOs (Carrier) and MVNOs providing choice and the ability to switch providers is getting easier with Remote SIM Provisioning.

Table 2: Summary of key differences in wireless technologies

	Range	Power Efficiency	Bandwidth	Best Use-Case	Latency	Networl
BTLE	Short *(~100 m)*	Very High	Low	Personal, Wearables	Very Low	Point-to
Zigbee	Short *(~10-100 m)*	Very High	Low	Home, Buildings	Very Low	Mesh
WiFi	Medium *(~100 m - 1 km)*	Moderate	High	Home, Office	Low	Star or M
LoRaWAN	Long *(up to 15 km)*	Ultra-High	Low	Remote, City, Campus	Low	Star
Cellular	Very Long *(national/global)*	Moderate to High	Moderate to High	Versatile range of stationary, mobile, real-time apps	Low to Moderate	Star
Satellite	Global, including remote areas	Low *(Improving with LEO and NTN)*	Moderate to High	Remote, Disaster Recovery, Global Maritime tracking	High *(due to satellite distance)*	Star

3 Redundant Infrastructure

Cellular networks are built with high redundancy and multiple layers of failover mechanisms. Telecom operators often use redundant base stations, backhaul connections, and infrastructure to ensure continuous operation in the event of hardware failures, natural disasters, or localised outages.

4 Strong Security Protocols

Cellular networks utilise advanced security protocols such as SIM-based authentication and strong encryption standards (e.g., 3GPP encryption, IPsec for cellular backhaul) to protect communications. This adds a layer of cyber-resilience, reducing the risk of unauthorised access and attacks that can compromise other wireless technologies.

5 Highly Reliable Power Backup Systems

Cellular towers are equipped with power backup systems (e.g., batteries or generators), enabling them to continue operating during power outages or disruptions to the electrical grid. This ensures that connectivity remains intact even during emergencies when other forms of connectivity, such as Wi-Fi or fibre, may fail.

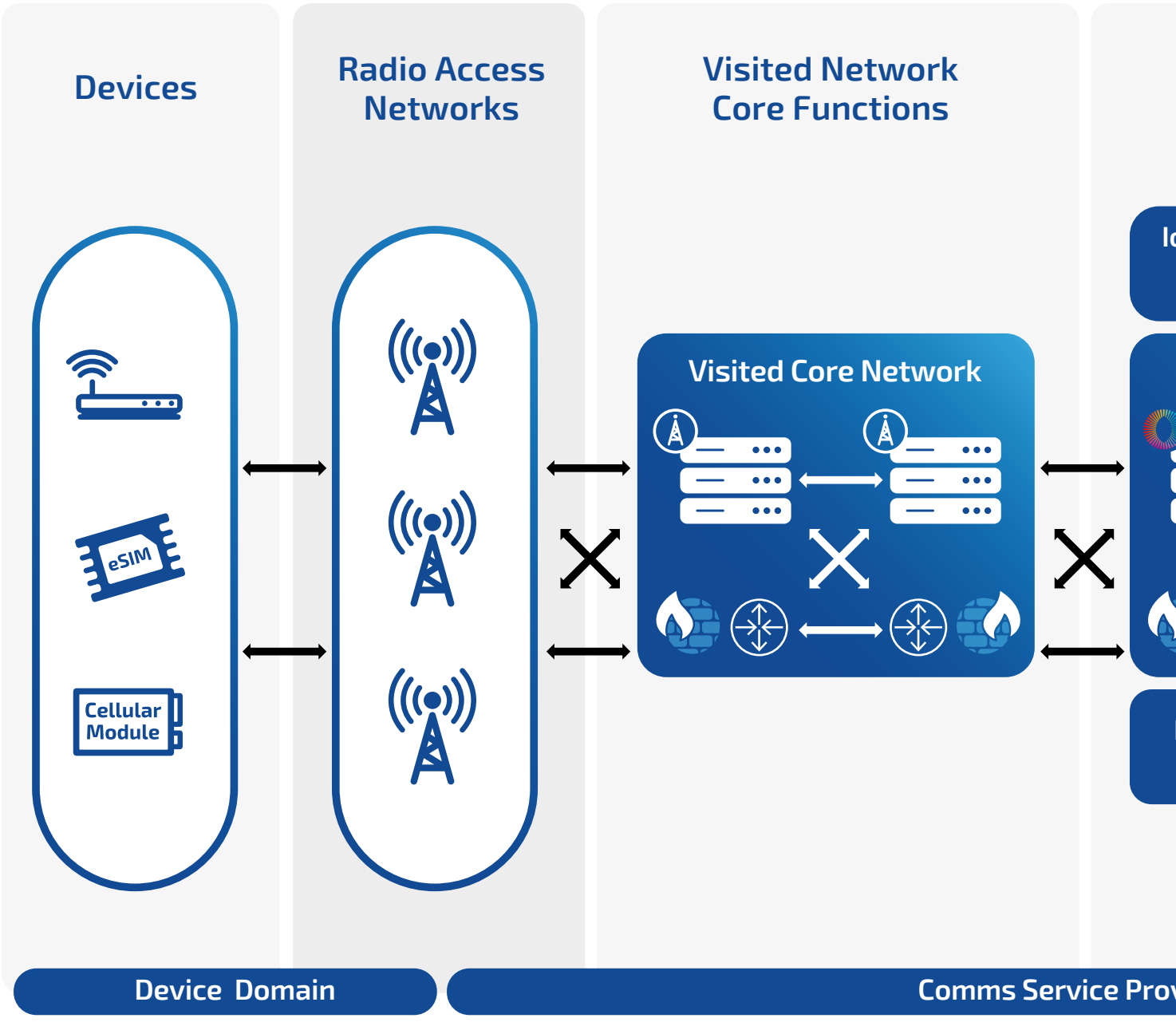
6 Mobility and Roaming Capabilities

Cellular networks provide seamless mobility and roaming capabilities, allowing devices to remain connected while moving across regions or networks. This is especially important for IoT devices, vehicles, or assets in motion, as it ensures uninterrupted connectivity across borders or cellular coverage zones without manual reconfiguration.

k Topology	Security	Resilience	
-point	AES-128	Limited	*Limited resilience due to short range and susceptibility to interference in crowded environments.*
	AES-128	Moderate *(mesh network adds redundancy)*	*The mesh network topology improves resilience because data can be rerouted if one node fails, though overall resilience depends on the density of nodes.*
Mesh	WPA2/WPA3	Moderate	*Moderate, dependent on network configuration. Vulnerable to interference, router failures, and network congestion.*
	AES-128	High	*High resilience due to its ability to operate in low-power, long-range networks. LoRaWAN devices can continue operating for extended periods in remote locations without relying on power-hungry infrastructure.*
	SIM-based authentication, carrier-grade encryption	Very High	*High resilience, with robust infrastructure, multiple failover systems, and strong network management practices.*
	Strong encryption	Very High	*Satellite networks are extremely resilient, especially in disaster scenarios, remote locations, or areas where terrestrial infrastructure is damaged or unavailable.*

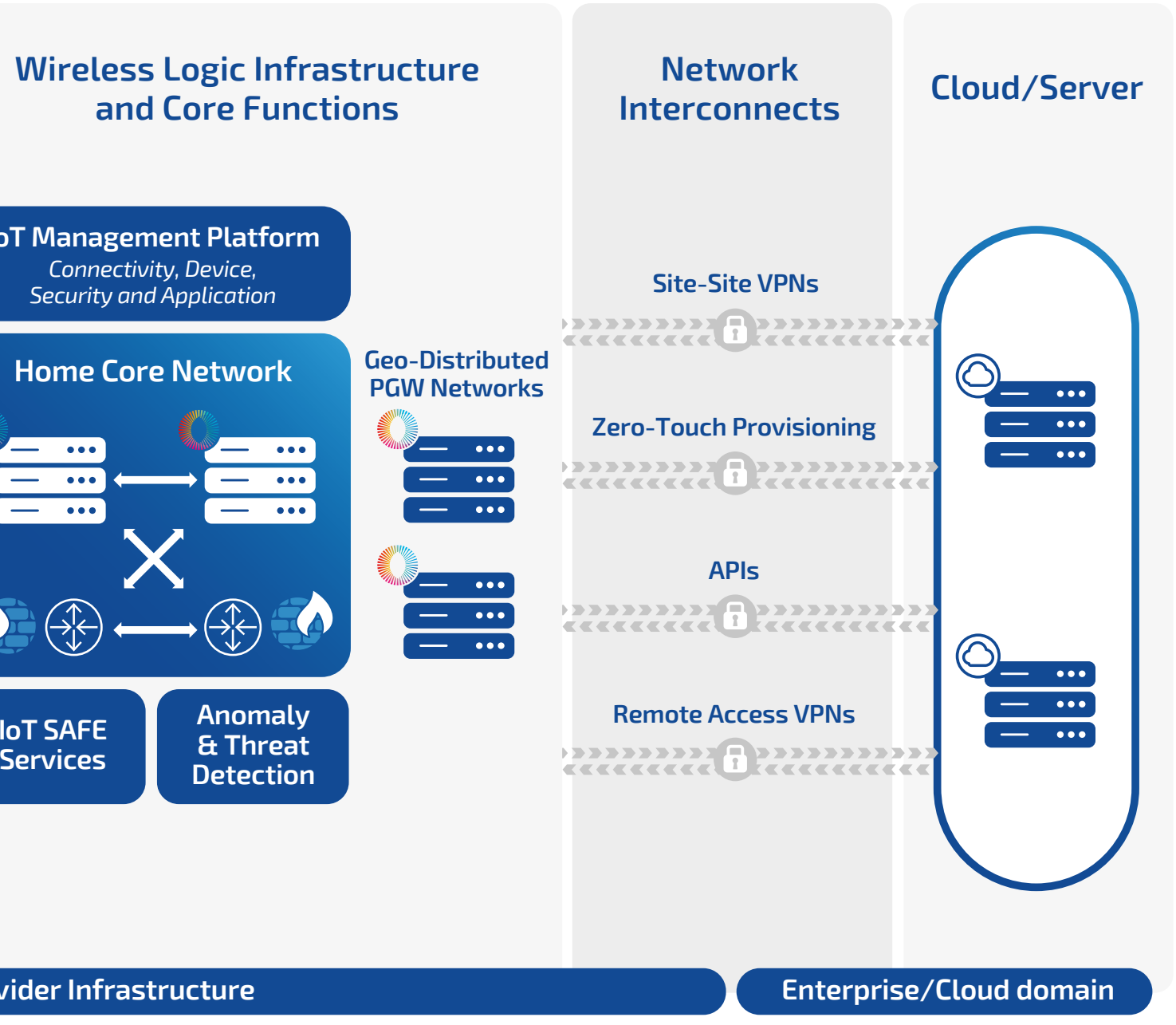
At a glance:

Creating end-end reliability, resilience and s



Advanced Network

ecurity for IoT



and SIM Capabilities

Breakdown:
Creating end-end reliability, resilience and se

In the IoT space there are additional dynamics and variables which don't exist to the same extent in the more controlled IT environments where the IT department has more complete control. With IoT, there are a vast number of device types and wireless network environments outside of the CISO, CIO, IT perimeter.

Vulnerabilities in the Device and Radio Access Network domain

Cellular has a long track record of resilience and reliability but as with all wireless technologies, it can be impacted by environmental and technical factors which are almost always temporary, and the implications can vary depending on the application. The potential sources of connectivity loss at a Radio Access Network are described below.

Systems that depend on real-time communication, safety or business critical, such as critical infrastructure, health monitoring, autonomous vehicles or industrial automation will need should be designed accordingly at a device and system level. Other IoT systems involved in more passive monitoring situations may not even be affected.

1 **Network Coverage and Signal Strength**
Design systems with redundancy to prevent single points of failure. Use load balancing and auto-scaling to handle demand fluctuations. Implement georedundancy and automated failover to ensure continuous service, even during outages.

2 **Interference**
Electromagnetic interference (EMI) from industrial machinery, power lines, or electronic devices, and radio frequency interference (RFI) from nearby communication systems, can degrade cellular signals. This is particularly problematic in industrial environments or densely populated urban areas, where multiple devices transmit signals simultaneously. The presence of nearby cellular towers operating on similar frequencies can also cause signal degradation, resulting in connectivity issues for IoT devices.

3 **Network Congestion**
Network congestion occurs when many devices attempt to connect to the same cellular tower, particularly during peak usage times or in high-density areas. This congestion can overwhelm the network, leading to slower data transmission, higher latency, or dropped connections. IoT devices, especially those that require real-time data, may experience significant delays or loss of connectivity when networks are congested.

4 **Extreme Weather and Natural Disasters**
Severe weather conditions such as heavy rain, snowstorms, lightning, or high winds can lead to signal attenuation, especially in higher frequency bands like 5G. Natural disasters like hurricanes, floods, and earthquakes can damage critical cellular infrastructure, including towers and underground cables, causing widespread outages. During such events, even resilient IoT devices can lose connectivity as the supporting network infrastructure is disrupted.

5 **Construction and Power Outages**
Construction activities pose another risk, as workers may unintentionally damage cellular infrastructure, such as underground fibre-optic cables. Additionally, temporary construction barriers can obstruct wireless signals, degrading connection quality. Power outages, caused by storms or accidents, can take down cellular towers and other network equipment, leading to significant connectivity issues for IoT devices relying on continuous communication.

Return to Contents

curity for IoT

Mitigating these risks involves proactive planning, robust SIM, device, system and application design, resilient network infrastructure, and incorporating backup systems to ensure **consistent, reliable connectivity for IoT devices across various environments**.

Breakdown: **Creating end-end reliability, resilience and security for IoT** *(continued)*

Mandatory IoT device capabilities for high-availability and cyber-resilience

Whether you are an OEM, Solution Provider or Enterprise users, high-availability and cyber-resilience in IoT devices can only be achieved by implementing a range of security, reliability, and redundancy measures outlined below. It is not enough to rely only on your Communications or Cloud Service Providers capabilities, the device capabilities and how devices behave on the network are equally important.

IoT devices are often highly distributed and operate in diverse environments, making them particularly vulnerable to cyber threats and potential downtime. They are also often cost or resource-constrained which means compromises on best practice implementations will inevitably be needed. Make those compromises in a carefully considered way.

Use our guide to create requirement specifications and as a framework for those design decisions.

Secure Boot & Firmware Integrity	**Secure Boot:** Implement secure boot mechanisms to ensure that only trusted, signed, and authenticated firmware can run on the device. This prevents malicious code from being injected into the boot process.
	Firmware Integrity Checks: Regularly verify the integrity of the device's firmware and software using cryptographic hashing (e.g., SHA-256) to detect tampering.
	Over-the-Air (OTA) Updates: Provide secure mechanisms for OTA updates with proper encryption, authentication, and verification to keep devices patched against known vulnerabilities.
Device Authentication & Identity Management	**Unique Device Identity:** Ensure each IoT device has a unique, immutable identity to prevent impersonation or spoofing.
	Mutual Authentication: Implement mutual authentication protocols (e.g., X.509 certificates or Public Key Infrastructure, PKI) for establishing trust between devices and servers.
	Hardware Root of Trust (RoT): Utilise hardware-based security, such as Trusted Platform Module (TPM) or Secure Element (SE), to provide a hardware root of trust for cryptographic operations and device identity.

Antenna Design & Positioning	**Antenna design and positioning are critical for maintaining high-availability connectivity in IoT devices.** Proper design ensures optimal signal strength and coverage, while strategic positioning minimises interference and signal obstructions. Effective antenna placement enhances reliability, reduces connectivity loss, and improves overall performance, especially in challenging environments or remote locations
Data Encryption	**Data Encryption at Rest:** Use strong encryption algorithms (e.g. AES-256) to encrypt sensitive data stored on the device, preventing unauthorised access if the device is compromised. **Encryption for Data in Transit:** Secure communication channels using transport-layer encryption protocols such as TLS/SSL to protect data transmitted between devices and networks. **End-to-End Encryption:** Ensure that data remains encrypted from the point of collection to the final destination, reducing exposure to man-in-the-middle (MITM) attacks.
Resilient Network Communication	**Redundant Communication Channels:** multi-network, multi-IMSI SIMs and/or eSIM, iSIM solutions to maximise the control and ability to switch between network provider infrastructure. **Fallback and Failover Mechanisms:** Use network failover systems to ensure continuous service availability in case of network outages. This might include **Network Segmentation:** Ensure that IoT devices operate on segmented networks, isolating critical devices and limiting exposure to other vulnerable systems in the network.
Real-Time Monitoring & Threat Detection	**Intrusion Detection and Prevention Systems (IDPS):** Integrate built-in IDPS capabilities that can detect anomalies in real-time and prevent malicious actions such as unauthorised access or denial-of-service (DoS) attacks. **Log Monitoring:** Enable detailed logging on IoT devices to monitor and record system events, security incidents, and performance data, which can be analysed for proactive threat detection. **Health Monitoring:** Include features for real-time monitoring of device health, such as CPU usage, memory consumption, network latency, temperature and other critical performance metrics to ensure that devices are functioning optimally.

Breakdown: **Creating end-end reliability, resilience and security for IoT** *(continued)*

Fail-Safe & Redundancy Mechanisms	**Redundant Hardware Components:** Where feasible, design devices with redundant hardware components (e.g., dual power supplies or redundant communication paths interfaces) to avoid single points of failure.
	Graceful Degradation: Ensure that IoT devices can continue to operate in a degraded mode if some components fail, allowing essential functions to continue.
	Backup Power: Include backup power sources, such as battery power or energy-harvesting technologies, to ensure uninterrupted operation during power outages.
Patch Management & Vulnerability Updates	**Regular Firmware Updates:** Establish a robust process for delivering secure and timely firmware patches to address security vulnerabilities.
	Automated Updates: Where possible, implement automated patching mechanisms that don't rely on user intervention to reduce the risk of vulnerabilities remaining unpatched.
	Update Rollback Mechanism: Provide the capability to roll back firmware updates if an issue arises during or after the patch, ensuring minimal disruption to service availability.
Device Access Control	**Role-Based Access Control (RBAC):** Implement role-based or privilege-based access control to limit which users or systems can interact with the device, minimising the attack surface.
	Multi-Factor Authentication (MFA): Incorporate multi-factor authentication for accessing the device's management interfaces to prevent unauthorised access.
	Least Privilege Principle: Design the device's software and firmware to adhere to the least privilege principle, ensuring each service or component has only the minimum level of access necessary to function.

Resilience to Physical Attacks	**Tamper Detection:** Embed tamper detection mechanisms that trigger alarms or wipe sensitive data if the device is physically tampered with.
	Secure Hardware Enclosure: Use secure, tamper-resistant enclosures to protect internal components from unauthorised access or hardware attacks (e.g., JTAG or debug ports). Ideally select embedded SIMs and eliminate removable SIM card slots.
Device & Data Lifecycle Management	**Secure Decommissioning**: Provide secure decommissioning procedures to ensure that sensitive data is securely erased when the device reaches end-of-life.
	Data Retention Policies: Implement configurable data retention policies that allow organisations to control how long data is stored on the device before being deleted.
	Device Recovery: Enable devices to self-recover from failure states (e.g., watchdog timers) and return to a secure operational mode, minimising downtime.
Compliance with Industry Standards & Regulations	**Follow GSMA TS.34** – IoT Device Connection Efficiency Guidelines to ensure devices behave well on the network and don't generate unnecessary network signalling or waste their own energy resources.
	Ensure that devices comply with appropriate ISO, NIST, ETSI standards for data and cyber-security.
Testing & Quality Assurance (e.g. TUV, UL)	**Penetration Testing:** Conduct regular penetration testing on devices to identify potential vulnerabilities that hackers could exploit.
	Stress Testing: Perform stress testing to evaluate the device's ability to maintain functionality under high-load conditions or during network outages.
	Certification: Seek certification from trusted third-party security authorities to validate the security and availability of IoT devices.

Breakdown:
Creating end-end reliability, resilience and security for IoT *(continued)*

High-Availability through Edge Computing & Decentralisation	**Edge Computing:** Offload critical processing to the edge (local gateways) to minimise latency and ensure functionality even when the cloud service is unreachable.
	Decentralised Data Storage: Implement decentralised data storage architectures (e.g., blockchain or distributed ledger technologies) to ensure data integrity and availability even if a central server is compromised.
Security by Design & Privacy by Design	**Security by Design:** Integrate security into the design and development process of IoT devices, considering cybersecurity risks at every stage.
	Privacy by Design: Ensure that privacy considerations (e.g., data minimisation, anonymisation) are incorporated during the development of the IoT device to comply with privacy regulations such as GDPR.
Third-Party Component Security	**Third-Party Component Vetting:** Ensure that any third-party components (hardware or software) included in the device are thoroughly vetted for security vulnerabilities and regularly updated.
	Supply Chain Security: Implement stringent security checks throughout the supply chain to prevent tampered or malicious components from being integrated into the final product.

By implementing these measures, OEMs can ensure that their **IoT devices are both highly available and cyber-resilient**, helping organisations mitigate risks, ensure continuous operation, and comply with industry regulations. These principles also help **improve customer confidence and trust** in the reliability and security of IoT products.

Advanced Device, Network and SIM capabilities for high-availability and cyber-resilience

On page 8 we documented an expansive list of targeted questions designed to help you assess IoT Communications Service Provider cyber-resilience and high-availability.

If you want to see a Wireless Logic response to each of the questions listed you can request that via *Contact Us*.

In the following sections we will summarise some of the key device guidelines and solutions which Wireless Logic deploy in our own networks and with our customers to optimise high-availability and cyber-resilience.

What devices should do if outages do occur to protect themselves and ensure a graceful recovery.

Advanced Network and SIM capabilities which will help you achieve compliance and differentiation.

Contact us...

to discuss any of the content in this guide and receive a breakdown of how Wireless Logic addresses high-availability and cyber-resilience requirements for Enterprises using IoT.

Breakdown: **Creating end-end reliability, resilience and security for IoT** *(continued)*

What devices should do if outages do occur to protect themselves and ensure a graceful recovery.

The GSMA document ***TS.34 - IoT Device Connection Efficiency Guidelines*** provides an extensive set of best practice guidelines for IoT devices and should be followed by IoT device developers.

In IoT scenarios, the IoT device firmware and software play a significant role in the overall performance and behaviour of the IoT system as a whole, including the impact on the cellular network. With no human intervention to fall back on, the mechanisms that manage start-up and how devices behave when transitioning in and out of coverage or during recovery from an outage need to be designed into IoT devices.

The 8 steps below focus on those recovery steps which help ensure data integrity, minimise power consumption, and restore connection efficiently and without overloading the recovering network.

Use our guide to create requirement specifications and as a framework for those design decisions.

Detect the Network Loss

Make a distinction between an outage event or a temporary loss of connection caused by change in location and coverage loss.

Regular Monitoring: The device must continuously monitor its connection status by checking for network signals, loss of heartbeat messages, or failure to receive acknowledgments from the server.

Timeouts and Retries: Implement a timeout mechanism to define how long the device waits before considering a communication failure. Upon timeout, initiate a predefined number of retry attempts to reconnect.

Graceful Shutdown of Non-Critical Functions

Data Buffering: Before shutting down or switching to low-power mode, the device should buffer any unsent data locally (in non-volatile memory if possible). This ensures that no critical data is lost during the outage.

Prioritise Tasks: Suspend non-essential functions such as sending periodic status updates or less critical telemetry, while critical functions like monitoring sensors should continue operating and storing data.

Switch to Low-Power Mode

Power Conservation: To extend battery life during a network outage, the device should switch to a low-power mode (e.g. deep sleep or idle mode). This reduces power consumption while maintaining readiness for the network to come back online.

Scheduled Wakeup: The device should periodically wake up at defined intervals to attempt reconnection, ensuring it doesn't remain in low power mode indefinitely.

Retry Connection Attempts	**Exponential Backoff:** Implement an exponential backoff algorithm to manage reconnection attempts. After each failed attempt, the device should increase the time between attempts (e.g., 2 seconds, 4 seconds, 8 seconds, etc.), preventing excessive battery drain and reducing network load.	**Monitor Signal Strength:** Before retrying a connection, the device should check for network signal strength to ensure conditions are favourable. Attempting reconnection in poor signal conditions can lead to excessive power consumption.
Fallback to Alternative Networks *(If Available)*	**Send Alerts:** If possible before the complete loss of communication, the device should notify the server or cloud platform about the impending network loss to allow the system to take appropriate measures, such as marking the device as offline or changing data processing logic.	**Switching Strategy:** Define a strategy for how the device switches between primary and secondary networks, including conditions to return to the primary network once it's restored.
Alert the Device Management and / or Cloud/Application *(When Possible)*	**Send Alerts:** If possible before the complete loss of communication, the device should notify the server or cloud platform about the impending network loss to allow the system to take appropriate measures, such as marking the device as offline or changing data processing logic.	**Offline Mode Activation:** The cloud can mark the device as 'offline' or 'disconnected' until it successfully reconnects, ensuring data consistency and preventing errors in communication.
Automatic Recovery & Re-Synchronisation	**Restore Connection:** Once the network is restored, the device should automatically re-establish the connection with the server or cloud platform.	**Re-synchronise Data:** The device should upload any buffered data collected during the outage and synchronise its clock and status with the server to ensure all data timestamps and system states are aligned.
Fallback Error Handling	**Set Time Limits for Outages:** If the outage persists beyond a predefined limit, the device should escalate the issue, either by switching to a backup communication method (if available) or by generating alerts for user intervention.	**Local Actions:** In the event of a prolonged outage, the device should have predefined local actions to handle its critical functions independently, such as logging sensor data, issuing local alerts, or maintaining environmental controls.

Focus on Advanced Network and SIM capabilities which will help you achieve compliance and differentiation

- **eSIM, iSIM and Remote SIM Provisioning**
- **Device Authentication & Identity Management**
- **Secure Private Networking**
- **High Availability Network Core**
- **IoT Management Platform**
- **Anomaly & Threat Detection**
- **24/7 Global Operations**

At a glance: System Architecture

eSIM, iSIM and Remote SIM Provisioning (RSP)

Wireless Logic has been deploying eSIM solutions for more than 10 years and has extensive experience and strong carrier (MNO) partnerships.

The physical security and reliability benefits of embedded eSIMs and integrated iSIMs provide a significant advantage over removable SIM cards. For maximum advantage, OEMs, Solution Providers and Enterprises must also leverage Remote SIM Provisioning (RSP) to manage the full SIM lifecycle from factory to field.

Standard Solution

Our standard SIM solution is a multi-IMSI SIM profile deployed in an eSIM which provides the maximum flexibility. The default profile is always designed to provide maximum coverage and resilience which can mean 3 or 4 networks per country in the key markets Multi-IMSI and eSIM mean that updates and localisations can be made via Over-the-Air (OTA) updates.

The key benefits to you

RSP helps Enterprises maintain a high-level of coverage and resilience over time and use network level or SIM-level changes over-the-air to resolve performance, commercial and quality issues should they arise. The rise or government or carrier restrictions on permanent roaming means RSP is essential for Enterprises who deploy internationally.

Customisation Options and Advanced Functionality

The ability to download and switch IMSI's and SIM profiles OTA provides flexibility and customisation options which can be designed around your business and deployment needs. Wireless Logic has the most expansive carrier eco-system and portfolio of IMSI and eSIM profile partners.

Ease and Cost of adoption

Wireless Logic supports multi-IMSI and all three RSP standards (SGP.02, SGP.22 and SGP.32). We will work with you to identify and automate a solution which suits your business processes and deployment needs. Navigating the RSP eco-system on your own can be complex and expensive so it's important to select and work with a specialist partner like Wireless Logic.

Learn more about Remote SIM Provisioning and why you should partner with Wireless Logic.

Device Authentication and Identity Management

A unique and immutable device identify is essential for preventing impersonation or spoofing. In other words, to ensure that only authorised devices are communicating with your servers.

We solve this while also enabling you to reach devices from your servers using a series of measures described below.

Standard Solution

We advocate the use of private IP addresses in addition to SIM based authentication. These measures combine with Private APN and VPN to separate and secure your device traffic from regular internet traffic and the threats which can exist there. If a public IP address is really required by your industry or your customer's, then we have solutions which improve the security of those public IP endpoints.

Customisation Options and Advanced Functionality

Use the SIM to store and distribute certificates and automate PKI creation and maintenance using our standards-based, secure IoT SAFE infrastructure. IoT SAFE is a GSMA standard which enables the certificate-based security used in contactless payments, mobile and IT industries to be implemented on IoT devices.

The key benefits to you

Robust authentication and identity management defends your network against spoofing, ransomware attacks and unauthorised network access which can lead to service loss or device/network downtime.

Ease and Cost of adoption

We provide private IP and APN solutions as standard. Enterprise adoption of IoT SAFE requires some planning and collaboration with OEM/ODM and Cloud/Server teams but it is otherwise but is very cost-effective and can produce savings on bill-of-materials and cost of ownership on identity (certificate) management.

Learn more about IoT Security and why you should partner with Wireless Logic.

Secure Private Networking

More than 95% of IoT connections managed by Wireless Logic use NetPro, our Private APN and VPN services infrastructure.

NetPro services form a critical part of your defence against security threats and combine with carrier encryptions and IP-based encryption protocols such as TLS to provide end-end encryption of data in transit.

Standard Solution

We advocate Private APNs as standard. An APN is a gateway which enables IoT devices to use mobile network infrastructure to connect to enterprise networks, without having to access the public internet. Our NetPro infrastructure includes high-capacity fibre links to carrier networks and is implemented in geo-resilient data centres to maximise reliability.

Customisation Options and Advanced Functionality

IPSec VPNs are typical for site-site VPNs (connecting Wireless Logic to Enterprise infrastructure) and SSL VPNs for ad-hoc remote access. Unless you are already using end-end TLS encryption on your device-server traffic, IPSec VPNs are essential.

The key benefits to you

Use secure private networking solutions to prevent data theft, ransomware, malware and man in the middle attacks and protect your brand and reputation

Ease and Cost of adoption

Private APNs and carrier encryption comes as standard, VPNs require some planning between NetOps teams on each side but should be used in all but a few cases where the simplest binary (on/off) or sensor data is being transmitted. See ***Device Authentication and Identity Management*** for details on cost-effective TLS implementation in IoT.

Learn more about Secure Private Networking and why you should partner with Wireless Logic.

High-Availability Core Functions and Interconnects

Wireless Logic operates a dedicated IoT core network designed and built for IoT.

This is in addition to carrier partner core and radio network infrastructure. In all cases, the core functions run on geographically dispersed data centre infrastructure with separate power supplies to ensure reliability and resilience.

Standard Solution

Our Core infrastructure operates in an active-active, mode ensuring that there is a continuous view of the health of our systems and a failover available for all traffic in the event of service degradation. Time to restoration of service if device needs to establish a new connection is automatically handled by directing traffic to the active node with no manual intervention required.

Customisation Options and Advanced Functionality

We also operate a network of distributed Packet Gateways to provide localised and low latency data connections to Enterprise network or internet services.

We advocate dual-IP addresses for devices and map those to redundant packet gateways to automate failover and outage recovery processes should an outage occur.

The key benefits to you

Our mission-critical applications are structured as microservices and run on Kubernetes clusters, strategically positioned across multiple data centres. The active-active setup ensures high availability and reliability while minimising the risk of downtime.

Ease and Cost of adoption

Mapping of traffic between core and regional packet gateways requires advance planning but adoption of Conexa is otherwise seamless. If dual-IP addresses are used then servers must resolve using DNS before contacting remote devices.

Learn more about Conexa and why you should partner with Wireless Logic.

IoT Management Platform

Monitoring and Management of IoT devices at a connection, device, security and application level is essential for detection and resolution of operational and security incidents.

This includes detection of unauthorised data consumption, location, device health and system or application level anomalies. Real-time detection and pro-active reactions will be critical for preventing wide-spread loss of service and outages.

Standard Solution

SIMPro is our fifth generation Connectivity Management Platform which has evolved to include Device (DevicePro), Security (NetPro) and Application-level Management (Kheiron). The first line of defence is SIMPro which monitors location, frequency and volume of consumption and can alert, throttle, block or quarantine connections which violate your defined parameters..

Customisation Options and Advanced Functionality

DevicePro lets you monitor device health (signal strength, battery levels, temperature) and perform OTA configuration or firmware updates. Kheiron is our Application Enablement platform which include Digital Twin and application data contextualisation and visualisation with, mobile push notifications, SMS and email alerting.

See also ***Anomaly & Threat Detection***

The key benefits to you

A 2022 IBM data security report identified that the average time to detect and report a security breach was around 9 months. Real-time multi-level monitoring is crucial to accelerate detection and remedial action and to minimise the damage caused by operational or cyber-security incidents.

Ease and Cost of adoption

These services are mandatory. Enterprises should apply connectivity, device, security and application-level monitoring according to their risk profile and tolerance to service or data loss/ corruption.

Learn more about IoT Management and why you should partner with Wireless Logic.

Anomaly & Threat Detection (ATD)

Solution Providers, IT/OT System Integrators and end-user Enterprises use Anomaly & Threat Detection to identify the first signs of cyber-attacks against their IoT systems.

It also provides them with threat management measures, operational visibility and supports their compliance efforts with industry and government regulators.

Standard Solution

Packet headers from device-cloud communications can be mirrored from our mobile core to our Anomaly and Threat Detection engine for near real-time AI-driven analysis with insights and threat levels communicated via the UI for investigation and remedial action. These processes will alert you to abnormal usage or end-point communications and provides warnings of malware, ransomware events.

Customisation Options and Advanced Functionality

Service extensions are also available to support tighter integration with your business systems and automation of responses, threat prevention and the production of compliance reports. These reports will provide important evidence of the monitoring and prevention measures you have in place which is information government regulators will seek should you ever experience a security breach.

The key benefits to you

If left undetected or unresolved, cyber-attacks can lead to chronic operational challenges, loss of reputation and financial penalties. Anomaly and Threat Detection reduces this risk and provides vital evidence of your monitoring strategy should you need to demonstrate to regulators.

Ease and Cost of adoption

Deployment of Anomaly and Threat Detection is seamless. It does not require any software agents to be installed on IoT devices and does not compromise your system performance or data privacy commitments.

Learn more about Anomaly & Threat Detection and why you should partner with Wireless Logic.

24/7 Global Operations

We offer 24/7 Global Operations from our service centres in Asia, Europe and North America.

SIM Assist is our comprehensive support solution which includes the "Wilo" Digital Assistant based on AI/ML/NLP to automate routine service requests and free support agents to deal with the more complex and customer-focussed support services.

Standard Solution

SIM Assist is a three-tier service and includes SIM Assist Enterprise designed for blue-chip solution provides, OEMs and Enterprises. It delivers expert help for the most complex solutions, including 24/7 support for P1 and P2 incidents.

SIM Assist Enterprise features the fastest SLAs for first response times across all tiers and includes premium features such as proactive incident reporting, root cause analysis reporting for P1 incidents and a dedicated care agent.

The key benefits to you

Once you have onboarded as a customer you can tap into the expertise of our distributed Service and Network operations teams worldwide, who provide localised and real-time support for your IoT deployments. The team is focussed on helping you deploy, scale and maintain high-availability solutions.

Ease and Cost of adoption

Our service tiers are designed to meet the demands and budgets of local, regional and global IoT deployments.

Learn more about 24/7 Global Operations and why you should partner with Wireless Logic.

Case Studies

Connectivity Service Providers play a critical role in connecting remote assets, systems and people. While the primary purpose is about connecting A to B, the role of the CSP also extends to security, privacy, reliability as well as industry specific regulations.

This is illustrated by two case studies covering Vehicle Telematics, Healthcare and EV Chargepoints which cross between automotive, energy and transport sectors and between commercial, consumer and associated data privacy requirements. This is reflected in an expansive set of regulations which must be met.

Case Study 1: Vehicle Telematics

Vehicle Telematics devices have mobility requirements and must comply with automotive regulations in addition to data privacy, safety, vehicle emissions, and operational regulations listed below.

Compliance to numerous regulations is under-pinned by reliable and cyber-resilient connectivity services.

Data Privacy & Security

Telematics systems collect personal and vehicle data, including driver behaviour, location, and performance. GDPR mandates that fleet managers ensure the secure processing, storage, and transfer of this data. Personal data must be anonymised or encrypted, and access should be restricted.

Taxation & Reporting

Telematics data is used to calculate vehicle mileage, fuel consumption and emissions for tax reporting purposes.

Safety & Vehicle Maintenance

Telematics can track vehicle maintenance, driver behaviour, safety inspections and record/report incidents such as accidents or safety violations.

Cyber Security

ISO/SAE 21434 and **NIST CSF** provides cybersecurity guidelines for road vehicles, including telematics systems. Fleet managers must ensure that telematics solutions meet these guidelines to protect against cyberattacks and unauthorised data access.

Accident Reporting & Investigation

In the event of an accident, telematics systems provide detailed data about the event, such as speed, location, and driver behaviour, which can be critical for insurance claims and investigations.

International Fleet Regulations

For fleets operating across multiple countries, telematics systems must ensure compliance with international vehicle standards, such as those set by the International Road Transport Union (IRU), and respect data privacy laws in each jurisdiction.

Data Logging, Retention & Access

Fleet managers in some jurisdictions are required to use electronic logging devices to record drivers' hours of service (HOS). Records must be retained for at least six months and make them available for inspection by authorities when requested.

Environmental & Emissions Regulations

Many companies are required to report their carbon footprint, and fleet managers must track fuel consumption and vehicle emissions through telematics systems to meet corporate or governmental sustainability reporting and clean air or emission zone requirements.

Insurance & Risk Management

Many fleet managers use telematics to qualify for usage-based insurance programs, where premiums are calculated based on real-time driving behaviour, mileage, and risk factors. Insurers often require specific telematics data, including driver behaviour metrics such as speeding, harsh braking, and acceleration. Insurers often require specific telematics data, including driver behaviour metrics such as speeding, harsh braking, and acceleration.

Driver & Vehicle Licensing

Telematics can track driver qualifications or medical certifications and send alerts when renewals or certifications are due. Fleet managers must ensure that all fleet vehicles are properly registered, insured, and meet licensing requirements based on their weight, cargo type, and jurisdiction.

Case Study 2: EV Chargepoints

EV Charging is a highly competitive market where customer experience and loyalty provide and additional dimension to the numerous legislation standards including reliability regulations designed to ensure government subsidies are used responsibly and the transition to EV and net-zero is not compromised.

A wider, although not exhaustive, list of regulations is documented below including those which provide protection for the consumer and the power grid. Compliance to numerous regulations is under-pinned by reliable and cyber-resilient connectivity services.

Electrical Safety Standards
EV chargers must comply with electrical safety standards such as IEC 61851, UL 2202/2594.

Pricing Transparency
Charging station operators are often required to clearly display pricing for energy use.

Permitting and Zoning
Installation of charging infrastructure typically requires building permits and must meet zoning regulations.

Grid Integration
Demand Response Operators may need to comply with utility or regulatory requirements related to demand response programs, allowing chargers to reduce load during peak demand times.

Consumer Data Privacy
Protection of consumer data including billing information, charging habits, and personal information collected via charging apps or networks must be assured.

Cyber Security
Given the connected nature of EV charging networks, manufacturers and operators must comply with cybersecurity regulations (e.g. ISO 27001) to protect against hacking and unauthorised access.

Interoperability & Open Access
To ensure that EV chargers work with a variety of vehicles and networks, OEMs and CPOs and must adhere to charging communication protocols including ISO 15118, OCPP (Open Charge Point Protocol).

Environmental and Energy Regulations
In some jurisdictions require energy efficiency and renewable energy integration.

Accessibility Standards
Charging equipment must be installed at heights and locations that are easily accessible to all users.

Government Incentives and Compliance
Operators are expected to meet Uptime Requirements, Maintenance Response Times, Real-time Monitoring and Consumer Protection and Transparency regulations especially when they have levered government incentives.

Key Legal Requirements for EV Charger Reliability

The Bipartisan Infrastructure Law (US) and EU Alternative Fuels Infrastructure Regulation (EU) provide funding for chargepoints to be installed along major road corridors with the requirement that chargepoints are 98% available.

Likewise, the UK governments EV Infrastructure Strategy set out goals for the development of a robust charging network by 2030 and includes reliability and uptime improvement objectives. Chargepoint Operators who do not meet the requirements summarised below, face financial penalties.

1 99% Uptime Requirement

The UK government introduced a minimum reliability standard that mandates a 99% uptime for rapid EV chargers at motorway service areas and other strategic locations. This requirement ensures that ***public EV chargers are operational and available to drivers for at least 99% of the time***.

2 Service Level Agreement (SLA) for Maintenance

Charging network operators are required to maintain charging stations to high standards of reliability and efficiency. This includes:

Maintenance Response Times:
If a charger is reported as faulty, operators must respond quickly to fix the issue, typically within hours or days, depending on the type of charger.

Real-Time Monitoring:
Operators are encouraged to use real-time monitoring systems to ensure that chargers are functioning and to proactively address any faults before customers experience them.

3 Consumer Protection and Transparency

The UK government also emphasises transparency in charger availability and performance:

Fault Reporting and Status Updates:
Operators must provide real-time data on charger availability through mobile apps or websites. This helps drivers plan their trips and avoid non-functional chargers.

Clear Contact Points for Reporting Faults:
There are also legal requirements for operators to provide clear channels for users to report broken chargers and receive updates on repairs.

4 Smart Charging Regulations

Under the Electric Vehicle (Smart Charge Points) Regulations, all home and workplace chargers must be 'smart', meaning they can:

- Adjust charging times based on grid demand.
- Support remote diagnostics and maintenance, helping reduce downtime and improve overall reliability.

These measures aim to increase consumer confidence, reduce range anxiety, and ensure that the EV charging infrastructure is dependable as the UK accelerates its transition to electric vehicles. Connectivity is an essential

Case Study 3: Healthcare

Mobile Health (mHealth) devices and services have mobility requirements and must comply with a range of regulations, operational and care related requirements.

Robust, secure connectivity underpins the operational and regulatory success of mHealth solutions, ensuring quality, compliance, and trust in healthcare delivery whether it's delivered at home, in the ambulance or hospital environments.

Data Privacy Compliance

Laws like GDPR and HIPAA mandate secure data handling. Downtime risks breaches. Reliable, encrypted networks ensure compliance by safeguarding patient data during transmission and storage.

Device Interoperability

Inconsistent connectivity hinders device communication in mHealth systems. Stable, interoperable networks enable seamless data exchange, adhering to standards like HL7, FHIR, and ISO 13485.

Cybersecurity and Threat Management

Cyberattacks risk data breaches and service disruption. Cyber-resilient connectivity with DDoS protection and zero-trust frameworks ensures secure, continuous mHealth operations.

Remote Patient Monitoring (RPM) Compliance

Regulations demand continuous RPM data for compliance and care quality. Always-on networks with fallback mechanisms prevent monitoring disruptions, safeguarding patient outcomes.

Regulatory Reporting and Audits

Connectivity issues disrupt timely reporting, risking non-compliance. Reliable networks ensure accurate, real-time data submission for regulatory adherence and seamless audit processes.

Real-Time Monitoring and Alerts

Downtime disrupts critical health monitoring, delaying alerts and risking patient safety. Reliable, low-latency connectivity ensures uninterrupted data flow for timely diagnostics and intervention.

Telehealth Service Delivery

Dropped calls and lag during virtual consultations affect care quality. Reliable, high-bandwidth connectivity ensures uninterrupted telehealth services and effective patient-provider communication.

Scalability for Underserved Areas

Expanding mHealth to rural areas faces connectivity gaps. Reliable wide-area networks enable scalable, equitable access to healthcare, even in low-infrastructure regions.

Emergency and Critical Care Continuity

Connectivity loss delays life-saving care during emergencies. Redundant, resilient networks and edge computing ensure real-time data access and uninterrupted critical care.

Patient Data Integrity and Reliability

Data loss or corruption impacts diagnostics and compliance. Cyber-resilient networks ensure reliable data transmission, preserving accuracy, integrity, and traceability across systems.

Consequences of downtime for your business operations and customer loyalty

We have just used two case studies to highlight the critical role resilient connectivity plays in achieving compliance and now widen the lens to illustrate the operational and business impacts of downtime which might be caused by prolonged device failures (electro-mechanical, environmental, software failures or damage), inadequate maintenance, connectivity or cloud infrastructure issues.

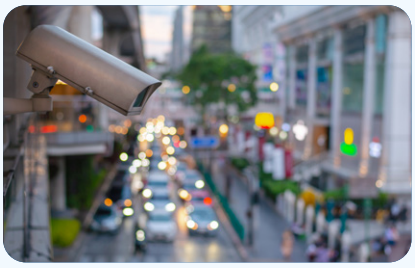
The consequences of downtime vary across different sectors but all are critical in their own way.

Energy & Utilities

- Service Interruptions
- Delayed Issue Detection
- Operational Inefficiencies
- Compliance Risks

Logistics

- Loss of Shipment Visibility
- Delivery Delays
- Inaccurate Reporting
- Increased Risk of Theft or Loss



Digital Surveillance

- Missed Security Events
- Data Gaps
- Increased Security Risks
- Compliance Failures

EV Charging

- Lost Revenue
- Impede EV adoption
- Operational Disruptions
- Compliance failures

Healthcare

- Delayed Patient Care
- Patient safety risks
- Reputational Damage
- Compliance Breaches

Digital Workforce

- Productivity Loss
- Missed Deadlines
- Communication Breakdown
- Safety/Security Risks

Retail

- Transaction Failures
- Inventory Inaccuracy
- Customer Dissatisfaction
- Supply Chain Delays

Vehicle Telematics

- Loss of Real-Time Tracking
- Inaccurate Data Reporting
- Operational Inefficiencies
- Compliance Issues

Drones & Autonomous Vehicles

- Navigation Failures
- Safety Hazards
- Mission Interruptions
- Delayed response, decisions

Contact **Wireless Logic**

Reliable Connectivity and robust security are fundamental to maintaining operational efficiencies, productivity, safety and security in businesses across all sectors.

Government and industry regulations require increased use of connected devices and are also getting stricter on uptime, cyber-resilience and data privacy.

This paper demonstrates the key role of Communication Service Providers in helping you satisfy those requirements and achieve your desired business outcomes with IoT.

Don't wait until deployment day to think about Connectivity, plan it from the beginning and enlist Wireless Logic as your strategic connectivity partner.

Contact us...

to discuss any of the content in this guide and receive a breakdown of how Wireless Logic addresses high-availability and cyber-resilience requirements for Enterprises using IoT.

Certificate Number 19387
ISO 9001, ISO 22301, ISO 27001
ISO 14001, ISO 50001

Thank you for connecting with Wireless Logic.

Contact us

Wireless Logic Group Ltd
Horizon, Honey Lane, Hurley, Berkshire SL6 6RJ, UK
Call: +44 (0)330 056 3300
Email: hello@wirelesslogic.com
Web: wirelesslogic.com/conexa

Other office locations

Austria	**Italy**
China	**Netherlands**
Denmark	**Norway**
France	**Spain**
Germany	**USA**

wirelesslogic.com