Giesecke+Devrient

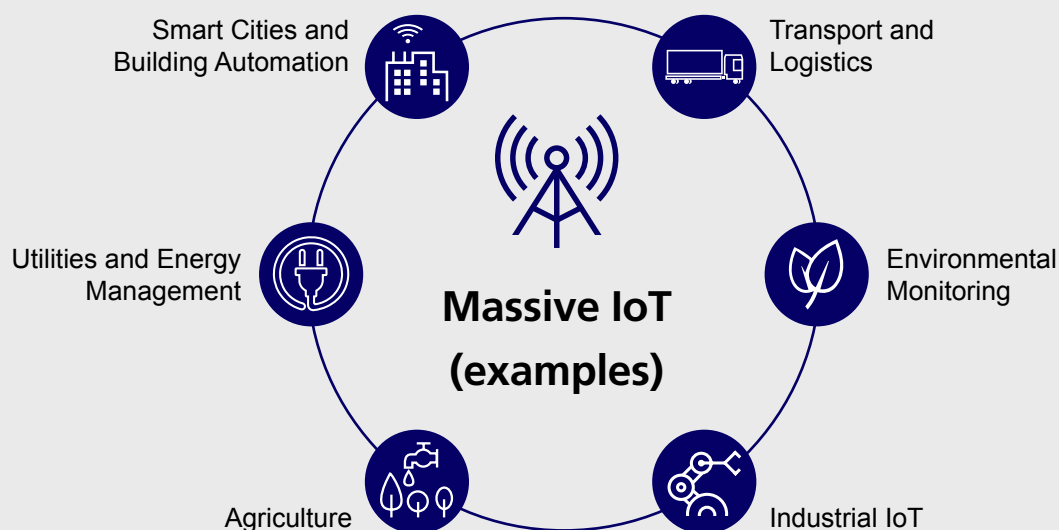# How Cellular Connectivity Empowers a Sustainable Massive IoT

In an era marked by unprecedented technological advancements and an ever-growing demand for connectivity, the concept of Massive IoT (Internet of Things) stands out as a pivotal bridge between innovation and sustainability. At the heart of this transformative idea lies the seamless integration of cellular connectivity, promising not only to revolutionize the way we live and work, but also to usher in a new era of environmental consciousness.

Massive IoT, as a subset of the broader IoT ecosystem, encompasses the deployment of countless interconnected devices, sensors, and machines. These devices can communicate with each other and the cloud for example, through cellular networks, providing a treasure trove of data and insights that can be harnessed to drive efficiency, productivity, and sustainability across industries. At the same time, Massive IoT places an enormous emphasis on sustainability, striving to minimize its own environmental footprint while enabling more responsible and eco-conscious practices in various sectors.

In the past, cellular IoT device connectivity was commonly achieved through traditional plug-in SIM cards. However, there is a growing demand for embedded SIMs (eSIM), as well as the new integrated SIMs (iSIM), particularly in the context of Massive IoT. Both facilitate entirely digital connectivity management. Additionally, they streamline the production, logistics, and warehousing of Massive IoT devices by allowing for the creation of globally consistent devices.
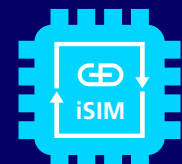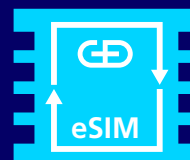

The iSIM in particular is optimized for use in NB-IoT and LTE-M applications as it is significantly smaller, more energy efficient, cost effective and sustainable compared to traditional SIM solutions.

Smart Cities and Building Automation

Transport and Logistics

Massive IoT (examples)

Environmental Monitoring

Utilities and Energy Management

Agriculture

Industrial IoT

The Challenges to Enable Connectivity for Massive IoT

Massive IoT, which involves connecting a vast number of devices to the internet, presents several challenges for device vendors, particularly in terms of connectivity. Here are some of the key challenges they face:

- **Network Coverage and Availability:** Ensuring that the devices have reliable network coverage, especially in remote or rural areas, can be a challenge. It requires collaboration with network operators to expand coverage.

- **Power Efficiency:** Many IoT devices are expected to have long battery lives. Device vendors need to optimize power consumption to ensure devices can operate for extended periods without frequent battery replacements.

- **Interoperability:** IoT devices from different vendors should be able to work together seamlessly. Ensuring interoperability is essential to avoid fragmentation in the IoT ecosystem.

- **Regulatory Compliance:** IoT devices often need to comply with various regulations and standards, which can vary by region. Keeping up with these requirements and ensuring devices meet them is a challenge.

- **Security:** Ensuring the security of IoT devices and their data is a significant challenge. Device vendors must implement robust security measures to protect against data breaches and unauthorized access.

- **Scalability:** Massive IoT involves deploying a large number of devices. Vendors need to design their devices and connectivity solutions to scale easily without causing network congestion or performance issues.

- **Connectivity Management:** Administering connectivity is a challenge as different solutions exist and new standards emerge. Both new devices and those already in the field need to be managed efficiently, ideally via one platform.

- **Connectivity Standards:** Choosing the right connectivity standard is crucial. Options include cellular (e.g., NB-IoT, LTE-M), unlicensed (e.g., LoRaWAN, Sigfox), and short-range options (e.g., Wi-Fi, Bluetooth, Zigbee). Vendors must select the standard that suits their application's requirements.

- **Device Management:** Managing a massive fleet of IoT devices can be complex. Vendors need efficient device management solutions for tasks like software updates, troubleshooting, and monitoring device health.

- **Data Management:** Handling the vast amount of data generated by IoT devices can be overwhelming. Device vendors must develop data management strategies, including data storage, processing, and analytics.

- **Cost Constraints:** Many IoT applications have tight budget constraints. Device vendors must design cost-effective solutions while maintaining quality and functionality.

- **Environmental Conditions:** IoT devices are often deployed in harsh environments or remote locations. Vendors need to design devices that can withstand extreme conditions and stay connected.

- **Reliability and Data Integrity:** In many Massive IoT scenarios, ensuring reliability as well as data integrity is key. Meeting these requirements can be challenging for some connectivity options.

- **End-of-Life Management:** IoT devices have a lifecycle, and managing end-of-life issues, including device disposal and data wiping, is important for sustainability and security.

**Remote connectivity and fleet
management via one portal**
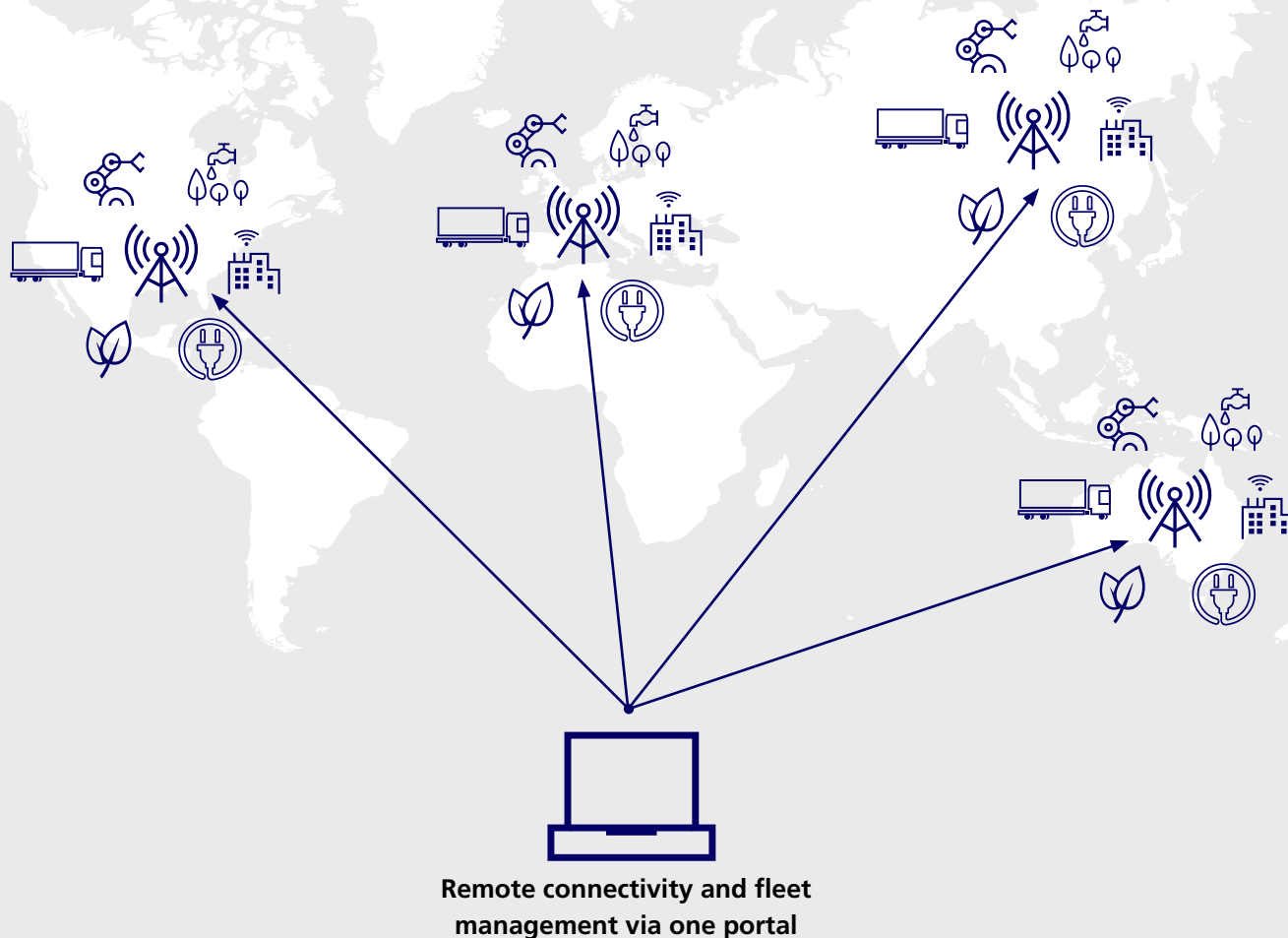
Addressing these challenges requires a combination of technological innovation, industry collaboration, and a deep understanding of the specific use cases for Massive IoT devices. G+D is well positioned to address these challenges and provides a set of solutions for the rapidly growing Massive IoT market.

This is where G+D's 'cellular IoT ready-to-go' comes in.

Massive IoT devices typically transmit small amounts of data intermittently. This contrasts with other types of IoT applications, like high-bandwidth video streaming or real-time control, which require higher data rates. Solutions that address this market must therefore be adapted to the specific requirements. Our 'cellular IoT ready-to-go' bundles solutions and services that provide easy cellular connectivity right when the device is first turned on, as well as the ability to manage the connection and the device itself during its lifetime. The solution is customizable to always provide the best experience for the user or operator of the device.
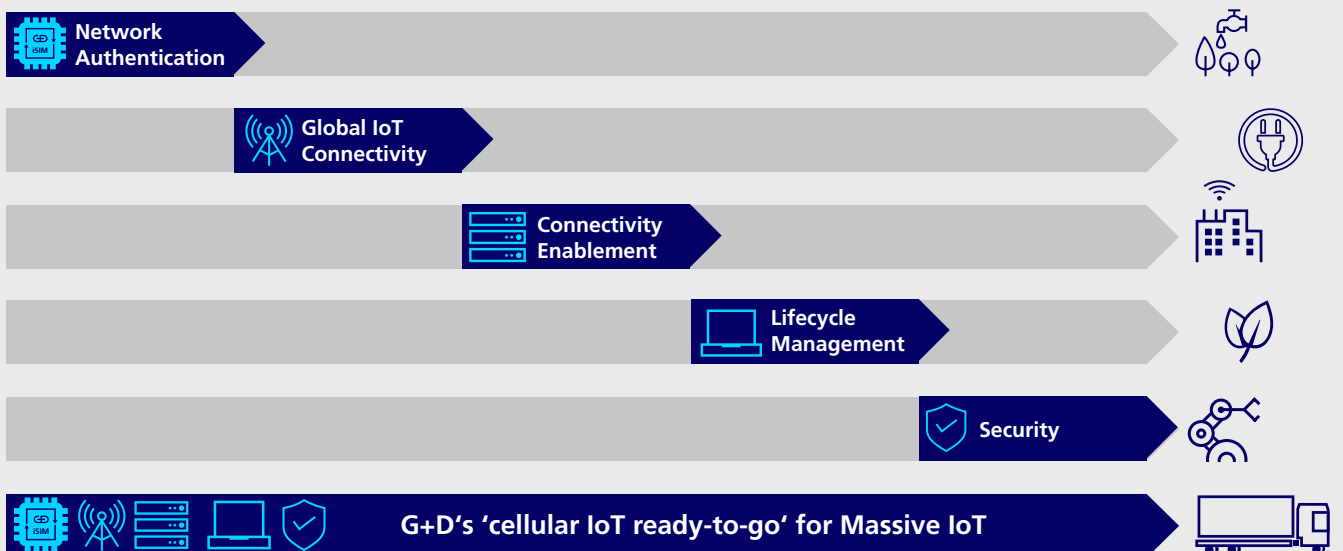
- **Global Connectivity:** Massive IoT aims to provide wide-area coverage, ensuring that even devices in remote or challenging environments can connect reliably. Our globally available Connectivity-as-a-Service packages cover more than 600 cellular IoT networks in 185 countries. In addition, satellite-based NB-IoT connectivity can be provided via the same 3GPP-compliant hardware to cover rural areas or regions with poor coverage.

- **Power Efficiency:** Devices in Massive IoT are typically battery-powered and need to operate with minimal energy consumption. This enables them to have a long lifespan without frequent battery replacements. Our new security proven iSIM, where the iSIM is part of the baseband controller, is specially designed for energy efficiency.

- **Interoperability:** Massive IoT can support a wide range of applications, from smart agriculture and environmental monitoring to asset tracking and smart cities. Interoperability between these use cases is key to successful implementation. All our solutions follow international telecom standards and are therefore designed for global interoperability, ensuring rapid deployment of Massive IoT devices.

- **Regulatory Compliance:** Meeting regional, and in some cases national, regulatory requirements is a major challenge in manufacturing devices. Especially when these are designed for a global market. Our standardized and regulatory-compliant connectivity solutions enable easy global deployment of Massive IoT devices.

- **Security and Data Management:** Security is crucial in Massive IoT, as a large number of devices can provide an attractive target for cyberattacks. Implementing strong security measures is essential to protect both the devices and the data they transmit. Security is a central component of all our solutions. Especially for the IoT, we have a number of SIM-based applications that provide cryptographic keys to sign and encrypt data or securely identify the device or associated server and cloud infrastructure. These solutions are based on cutting-edge technologies such as blockchain.

- **Scalability:** Scalability is a fundamental requirement for Massive IoT. As the number of devices grows, the network infrastructure should be able to expand smoothly to support the increased load. Our connectivity solutions and IoT device management platforms are specifically designed to manage large numbers of devices or entire device fleets.

- **Connectivity Standards:** Mobile connectivity offers several benefits, such as global interoperability that streamlines the deployment of IoT devices worldwide, enables centralized management without local or manual interaction, and supports a single stock keeping unit (SKU). Our mobile connectivity solutions for Massive IoT are designed to comply with relevant telecom standards.

- **Device- and End-of-Life Management:** Massive IoT is designed to accommodate an enormous number of devices, potentially in the order of billions, connecting to the internet. Therefore, all related processes must be streamlined to ensure cost efficiency. For example, our AirOn360® IoT Suite enables advanced lifecycle management and connectivity management for IoT device fleets. The solution also enables the final deactivation of the device remotely by completely disabling connectivity.

- **Cost Efficient:** To accommodate large numbers of IoT devices, networks and all components must be designed for efficiency. Techniques like device grouping and optimized resource allocation are used to make the most of available resources. Our iSIM solution is designed for cost efficiency, for example. Compared to local wireless networks, which often require manual administration and onboarding efforts, the iSIM enables a reduction in total cost of ownership (TCO) by supporting fully digital processes.

- **Environmental Conditions:** The specific requirements often depend on the practical application of a device. For example, we offer 3 different types of SIM hardware (Consumer, Industrial, Automotive) that meet the respective requirements.

- **Reliability and Data Integrity:** Data is the basis for nearly all applications and services in the Massive IoT and is therefore of central importance. Our Connectivity-as-a-Service packages based on NB-IoT and LTE-M are designed to meet use-case specific availability requirements. The integrity of the data can be ensured, for example, by SIM-based signatures and, if necessary, encryption.

- **Sustainability:** Sustainability is a major challenge for society and also for Massive IoT. It can help optimize CO2 emissions, for example, but should also be as sustainable as possible itself. Our iSIM, for example, enables optimization of the sustainability of Massive IoT devices through its energy efficiency and small footprint, thanks to the fewer components and materials needed for its production.

Key Components of G+D's 'cellular IoT ready-to-go'

Our 'cellular IoT ready-to-go' bundles a range of solutions and services to ensure fast and easy time-to-market for Massive IoT device vendors or equipment operators. These solutions can be tailored and adapted to meet the specific needs. Here is a brief summary of the main components.

- Network Authentication: Our SIM solutions are designed to address the diverse needs of IoT applications. We provide various form factors and SIM generations, including iSIM, eSIM, and pSIM, along with hardware variations tailored for specific applications, such as automotive, industrial, and consumer use cases.

- IoT Connectivity: We offer mobile connectivity as a service for various IoT use cases, which can be tailored to specific regions or used globally. We cover 185 countries and cooperate with over 600 network operators. Our IoT data connectivity options encompass NB-IoT, LTE-M, LTE, 5G, and satellite networks compliant with the 3GPP standards and provide coverage in remote areas. The connectivity can also serve as a backup or function as global bootstrap connectivity (GBC) when the device is initially activated to load the final subscription at the device's location.

- Connectivity Enablement: Our AirOn360® RSP platform empowers the digital connectivity journey with iSIM and eSIM management. It is best-in-class and ensures the highest levels of availability as well as geo-redundancy. We offer solutions for various device categories that comply with both the latest and legacy RSP standards, including SGP.02 (M2M), SGP.32 (IoT), SGP.22 (Consumer), and In-Factory Profile Provisioning (IFPP).

- Lifecycle Management (LCM): G+D's AirOn360® IoT Suite facilitates diverse applications for the remote management of IoT devices throughout their connectivity lifecycle. This includes functions like OTA campaign management, as well as applet administration. With our hybrid, multi-tenant management platform, IoT devices can be administrated individually or collectively as entire device fleets.

- Bring Your Own Connectivity (BYOC): We understand that not every business starts from scratch and we support our customers at all stages. G+D's AirOn360® IoT Suite allows enterprises to scale with our connectivity offering, but also to manage and monitor existing connectivity agreements with third-parties from a centralized platform. We remove the operational complexity to access and aggregate different RSP and LCM platforms.

- SIM-based Services: We offer various SIM-based applications that increase the security and functionality of IoT use cases and help protect the device and data.
  - Zero Touch Provisioning (ZTP) application, for quick, simple device onboarding without device or platform dependencies.
  - IoT SAFE offers a standardized approach for securing IoT data communications.
  - Multi IMSI gives the possibility to dynamically switch between various previously loaded IMSIs.
  - IMEI Locker allows to set management policies for the IoT device to authorize access to the network.
  - FPLMN Watch enables the allowance or denial of network access via a list stored on the SIM.
  - SIGNiT® provides data integrity for multi-party IoT ecosystems based on blockchain technology.

Further SIM applications can be offered or adapted according to customer requirements.

- Network Security: Our applications ensure the security of the network environment.
  - Site-to-Site VPN disguises the network to create an entry barrier for malicious actors and provides security when using the public Internet.
  - IP whitelisting allows to prevent unauthorized access to a system or network.

Network Authentication

Global IoT Connectivity

Connectivity Enablement

Lifecycle Management

Security

G+D's 'cellular IoT ready-to-go' for Massive IoT

We empower the IoT with Security Tech

About Giesecke+Devrient

Giesecke+Devrient (G+D) is a global SecurityTech company headquartered in Munich, Germany. G+D makes the lives of billions of people more secure. The company shapes trust in the digital age, with built-in security technology in three segments: Digital Security, Financial Platforms and Currency Technology.

G+D was founded in 1852 and today has a workforce of more than 14,000 employees. In the fiscal year 2022, the company generated a turnover of 2.53 billion euros. G+D is represented by 123 subsidiaries and joint ventures in 40 countries.

Further information: **www.gi-de.com**

Giesecke+Devrient

Giesecke+Devrient Mobile Security Germany GmbH
Prinzregentenstrasse 161
81677 Munich
Germany

www.gi-de.com
connectivity@gi-de.com

Follow us on: