



Getting to Mass IoT Deployment: Challenges and Opportunities



Proud to sponsor this important report that seeks to improve the success rate of Mass IoT Deployments...



psacertified™



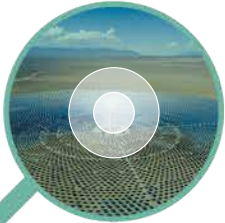
Contents



Introduction

The IoT market has moved a long way in the last decade. IoT solutions used to cater for just a few 100s of connected devices. Not any more

4



IoT Sector Activities

Which application areas are moving fastest into mass IoT deployment? What are the key issues that must be catered for when moving to large deployments?

7



Market Research and Analysis

What is the view of the market about mass IoT deployment? Exclusive interviews, survey findings and market analysis of the key trends towards mass IoT

38



Enabling Mass IoT

Examining the key issues in moving from small to large IoT deployments


59



Sponsors Deploying Mass IoT

How our sponsors are addressing the challenges of Mass IoT

77

 CLICK THE IMAGE TO GO STRAIGHT TO THAT SECTION



Introduction

As IoT becomes an increasingly important part of business operations, the size of deployments are growing quickly. IoT solutions used to cater for for just a few 100s of connected devices. Not any more.

As IoT becomes an increasingly important part of business operations, the size of individual deployments are growing quickly. IoT solutions used to cater for just a few 100s of connected devices. Not any more.

Recent research, including surveys conducted by Beecham Research, indicate the growing expectation among IoT users of individual deployments growing rapidly over the next few years. The two charts opposite, taken from a survey conducted in mid 2022, are a typical example of this.

The first question – roughly how many IoT devices and/or terminals are currently connected in or through your business? – shows that 52% currently have IoT deployments of over 500 connected devices. This in itself is significant. A few years ago, such a question would have found that well over 50% had less than just 100 connected devices. However, the finding that a quarter of these IoT users (26%) already have deployments of over 5,000 connected devices – with 19% having over 10,000 – is very significant. It is a strong indication that the IoT market overall is no longer in the early adopter phase and that it has reached the early majority phase.

The second question – how do you expect that to change in the next 24 months? – is even more revealing. Not far short of two thirds of the sample (61%) expect growth of over 10% of their deployments in the near future. Of these, 22% expect over 40% growth. Cross-referencing of these findings show that this high growth expectation is not confined to either small or larger deployments – it is across the market. This represents a step-change in development of the IoT market, towards Massive IoT (mIoT).

Figure 1.1 How many IoT devices/terminals are connected in your business?

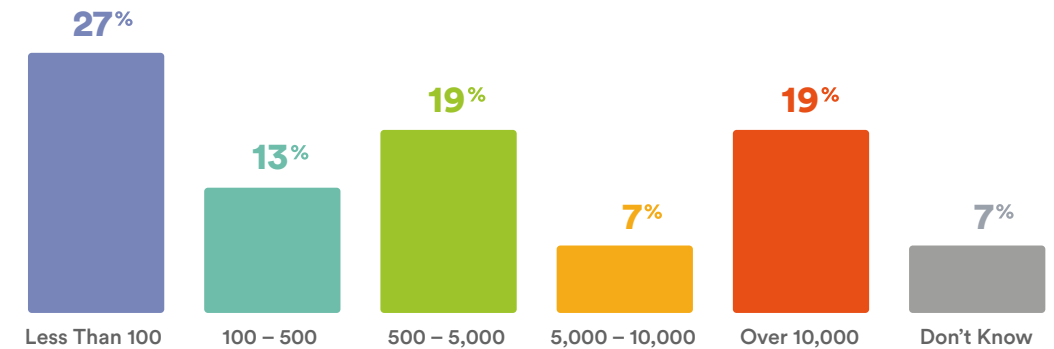
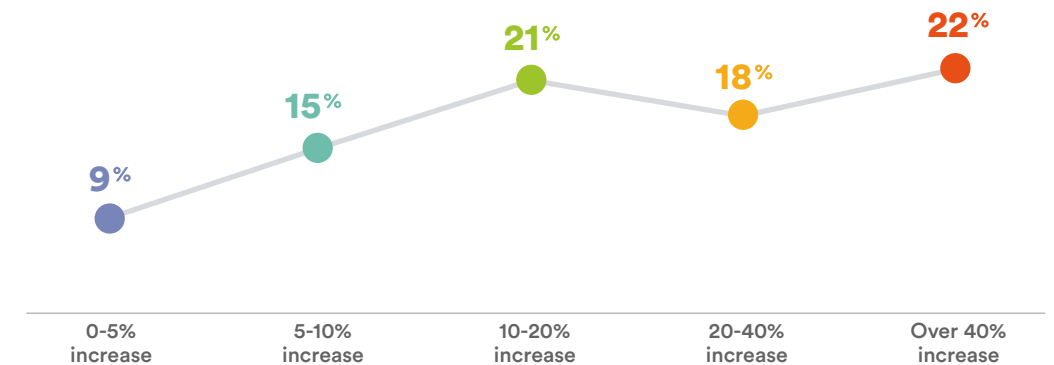


Figure 1.2 How do you expect that to change in the next 24 months?



Moving from small deployments to much larger ones is most often not just a matter of increasing the number of connections. Many small deployments were originally set up as Proof of Concepts (POCs) that were not envisaged to grow that much. What many have found is that to substantially grow a POC deployment, you may need to start again on the IoT solution. For example, most POC solutions of 10 or, say, 100 connected devices are set up manually. That does not work too well when there are 10,000 connections. A further issue is the type of these connections. Forecasts for IoT indicate that there will be billions of connected devices. Yet as many as 80% of these will be low cost, low data rate connections – very large numbers of very low cost devices. What is the most cost effective way to deploy such large numbers of low cost devices? Most likely, not the same way that initial connections were made.

These and other issues related to scaling IoT deployments are explored in this report. The potential for mIoT and the opportunities presented by it are also explored. To take one example, mIoT has enormous potential to positively impact the environment. Environmental monitoring, water conservation, food production and many others are being enabled by mIoT. For this reason, in Section 2 of this report we have highlighted IoT applications most closely associated with ESG (Environmental, Social and Governance) as examples that are now set for huge growth.

Reflecting the increasing need for ‘IoT everywhere’, these issues also impact on all connectivity types. Three of those are represented in this report – cellular, LoRa and satellite. While cellular has been central to IoT

connectivity for decades, LoRa is a relatively new entrant – only launched in the market in January 2015 – yet has already become a significant contributor to growth in low cost, low data rate connectivity. Satellite connectivity has always played a major role in the IoT market for remote locations where there is no terrestrial alternative – estimated at 90% of the Earth’s surface. Yet as IoT becomes more central to business operations, satellite is playing an ever-more-significant role, and this will continue to increase at a fast rate – by some estimates at a rate over the next 5 years of 40% annual growth. Satellite IoT is destined for huge growth.

The issues of scaling are significant for all elements of IoT solutions. This is particularly the case for IoT platforms and for overall end-to-end security. These two elements are also represented.

This report, like the others in the ‘Succeed with IoT’ series, is intended to be a reference document for those responsible for IoT projects within their companies, as well as those who develop and supply those solutions. We hope you find it useful.

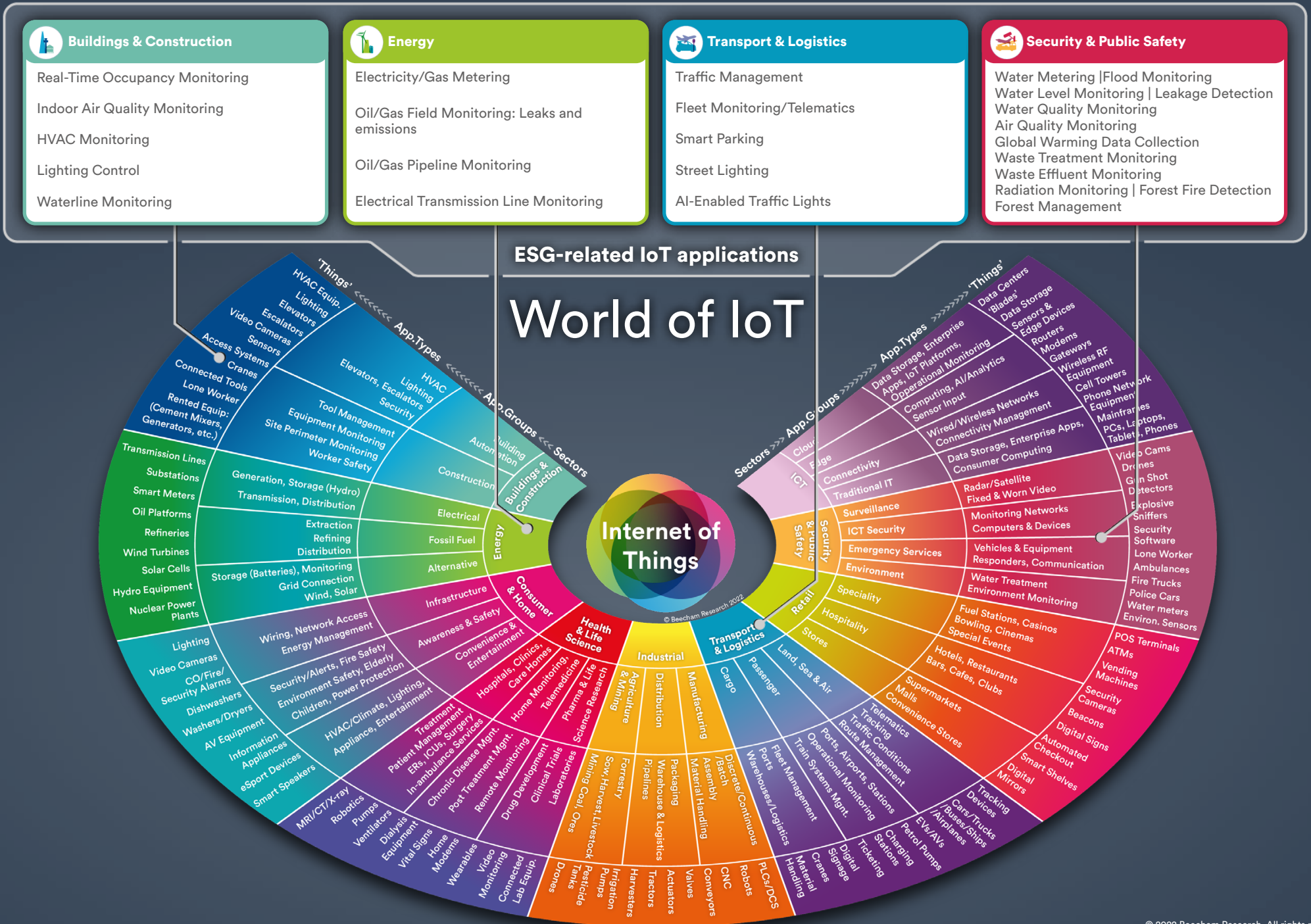


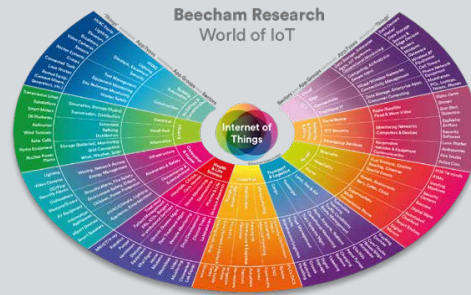
Robin Duke-Woolley
Founder & CEO,
www.Beecham Research.com

IoT Sector Activities

Which application areas are moving fastest into mass IoT deployment? What are the key issues that must be catered for when moving to large deployments? This section explores case studies and the key drivers towards mass IoT.







Beecham Research has composed this World of IoT chart from industry sectors where the Internet of Things has been shown to deliver value, improvements and efficiencies to businesses.

In this report we are examining the industry sectors and application areas where we anticipate deployments will scale to mass IoT.

The inner ring names the nine sectors in question, from Buildings & Construction to ICT (Information and Communications Technologies).

The next ring going outwards depicts App Groups: these are applications where IoT is applied in the functioning of these sector activities, e.g. building automation for the buildings and construction sector, hospitals and clinics for the healthcare sector. App types then go down to greater detail naming actual applications serving a specific purpose, e.g. building site perimeter monitoring, chronic disease management for healthcare.

Finally, the 'Things' are not applications but the end items which are instrumented and monitored through the named applications.

For example, video cameras and lone worker protection for construction, and vital signs monitoring and connected ventilators for healthcare.

This section also features a range of use cases and sponsor case studies that collectively illustrate the move from small scale to large scale deployments.

As an overlay we draw attention to the sectors where IoT applications particularly relate to topical ESG (Environment, Social and Governance) Goals. The purpose of an overlay is to bring together IoT applications from different sectors into a new grouping, in this case an ESG grouping. Another well-known overlay is Smart City. This highlight on ESG-related IoT applications is intended as an example of a relatively new application group that is likely to lead to mass IoT deployment. The sector outlines below commence with the 4 sectors usually most associated with ESG – Buildings & Construction, Energy, Transport & Logistics, Security & Public Safety – before then introducing the other sectors in the World of IoT chart.



[Buildings & Construction](#)



[Energy](#)



[Consumer & Home](#)



[Health & Life Science](#)



[Industrial](#)



[Transport & Logistics](#)



[Retail](#)

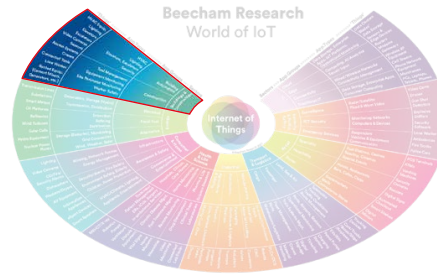


[Security & Public Safety](#)



[ICT](#)

CLICK THE ICON TO GO STRAIGHT TO THAT SECTOR



Buildings & Construction

Application Groups	Application Types	Things
Building Automation	HVAC – Heating, Ventilation, Air Conditioning Lighting Elevators, Escalators Security	‘Things’ for building automation include heating, ventilation and air conditioning equipment; remote control of lighting settings; building security, monitoring and control of elevators and escalators. ‘Things’ for Construction include wirelessly connected video cameras, sensors, tools, lone worker monitoring and tracking equipment. Connected tools enable users to remotely control the various tools, and to set and configure them to optimise efficiencies and safety.
Construction	Tool management Equipment monitoring Site perimeter monitoring Worker safety	

The Buildings and Construction sector is heading from mass IoT deployment, given the enhanced need to ensure health and safety in offices and on building sites.

Application examples highlighted in the figure particularly relevant for ESG include:

Real Time Occupancy Monitoring

As businesses and workplaces return to normal after the Covid pandemic, real time occupancy monitoring allows them to stay within safe distancing limits.

Indoor Air Quality Monitoring

Air quality monitoring will detect unhealthy levels of air pollutants. Indoor air quality is rapidly becoming a priority, as businesses continue to make

workplaces COVID-19 secure, to minimise the spread of all kinds of respiratory health challenges.

HVAC Monitoring

Controls ventilation and air conditioning equipment for a comfortable working environment.

Lighting Control

Optimal lighting settings can be remotely set and monitored, and lighting levels can be increased or decreased in line with ambient daylight levels.

Waterline Monitoring

Monitoring water supply and maintenance facilities in commercial and industrial settings.

Case Study – Smart Buildings

Connected devices are being deployed in a range of commercial and residential environments to help building owners and operators manage their properties more efficiently and cost-effectively, and even prevent problems before they arise. Lighting, heating, ventilation, security, and access can all be managed and optimized using the data and insight provided by the Internet of Things (IoT).

IoT development solutions provider, Embedded Planet, helps organizations turn their existing properties into smart buildings. Its technology enabled one owner to remotely monitor their vacant premises. Data on temperature and humidity was gathered by its sensors and the owner was alerted to any unexpected changes. This enabled them to detect a leaking pipe before it caused damage, which saved time and money.

Unfortunately, as several high-profile cyberattacks have demonstrated, the same data can create significant problems if it falls into the wrong hands. That is why Embedded Planet has developed solutions that have security built-in and are independently assessed by world-leading security experts.

For example, its Biblios wireless node with cellular, WiFi, Bluetooth, and LoRaWAN connectivity options, and a range of sensors, has achieved PSA Certified Level 1 certification. PSA Certified is a global partnership that provides a comprehensive security framework and multi-level evaluation scheme to reduce the complexity, cost, and time involved in securing a connected device.

Embedded Planet relied on PSA Certified components that already had security built-in to make its journey to security more straightforward, including utilizing the Infineon PSoC™ 64 secure microcontroller (Arm Cortex-M4) and Mbed OS operating system. Now, other firms can innovate knowing that Embedded Planet's Biblios wireless node is helping them establish a foundation of trust.





Case Study – Smart Cities

Cities are built on a complex network of infrastructure. Some of it we can see. Some of it is buried deep underground. So, how do we monitor the condition of these interconnected assets in the harder-to-reach areas and ensure the people who are responsible for maintaining them stay safe?

In smart cities, Internet of Things (IoT) devices are being used to check for hazardous conditions or signs of wear and tear. For example, city administrators can use smart sensors to monitor the temperature, humidity, water level, gas concentration, and oxygen saturation levels under manholes. The data these devices gather helps to protect workers from potentially dangerous situations and provide predictive maintenance information on utility networks.

With safety-critical environments, the infrastructure operator must be able to trust the data that is being gathered, which means it must come from a trustworthy device. Seoul-based SDT Inc. offers a secure foundation on which IoT developers can build new smart city applications. SDT's smart city solution includes system-on-modules for SDT Smart Hubs, and integrates with operating systems, connectivity, security, and cloud services to provide the starting point for a range of applications.

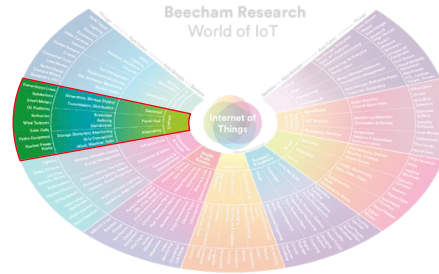
SDT has five PSA Certified products using STMicroelectronics silicon chips, which are all based on the Arm architecture. This means SDT has followed a four-step security framework to ensure its products are developed in line with industry-best practices. PSA Certified also confirms that world-leading laboratories have assessed the device as having the right level of security of built-in. Jiwon Yune, CEO and founder, SDT Inc., explains: 'Prior to PSA Certified, the biggest challenge was proving that we consider security in all layers when we are building our smart devices. Now, PSA Certified gives us security guidelines and offers our customers an independent rating they can trust.'



psacertified™



sdT



Energy

Application Groups	Application Types	Things
<p>Electrical</p> <p>Fossil Fuel</p> <p>Alternative</p>	<p>Generation, Storage (Hydro), Transmission, Distribution</p> <p>Extraction – from natural sources e.g. oil and gas from underground, ores from mines. Refining – chemical processes to produce usable fuel. Distribution – through pipelines, storage facilities, delivery by vehicles.</p> <p>Storage, Grid Connection, Wind, Solar</p>	<p>‘Things’ for energy monitoring include a wide range of connected items, e.g.: instrumenting and monitoring refineries and power plants, instrumenting and monitoring wind turbines, solar cells, hydro equipment, and nuclear power plants. For networks in their entirety or parts, preventive maintenance is one application that is key to ensuring that these work smoothly and that any problems can be highlighted before they occur.</p>

Energy networks are the wires and pipes that deliver electricity and gas to homes and businesses. They will require an unprecedented level of upgrades over the coming years to replace their ageing infrastructures; they will also need to accommodate growing populations, as well as to connect new sources of low carbon energy to the grid.

ESG issues come to fore for energy suppliers as the cost of power escalates, and governments mandate waste reduction measures across the board. Application examples highlighted in the figure particularly relevant for ESG include:

Electricity/Gas Metering

Smart meters on home and business premises to measure electricity or gas usage, helping to anticipate and plan for actual and future needs

Oil/Gas Field Monitoring: Leaks and Emissions

Instrumenting and monitoring oil platforms and their components to ensure safety and reduce emissions

Oil/Gas Pipeline Monitoring

Monitoring pipelines for leaks to ensure against costly losses

Electrical Transmission Line Monitoring

Instrumenting the components of the grid itself to measure and control output and flow, including transmission lines and substations.



Case Study – Scaling up end-to-end IoT device management and wind fleet control



A large wind energy company with over 7,500 employees has installed more than 39 GW of wind energy capacity in over 40 markets and in 2021 generated revenues of EUR 5.4 billion. The joint manufacturing capacity includes factories in Germany, Spain, Brazil, the United States, India and Mexico. Their product portfolio is focused on onshore turbines in the 4 to 6.X MW class, which are tailor-made for the market requirements of countries with limited space and regions with limited grid capacity.

Challenge

- Reduce 'cost of energy' (primary KPI of energy industry)
- Optimize total lifecycle costs of operating and managing windfarms
- Enhance operation efficiency of global wind fleet control center
- Replace SCADA-based windfarm server with IoT platform-based approach
- Provide homogenized wind fleet wide data access for analytics use cases

Solution

- Cumulocity IoT powers the global wind fleet control center with 7000+ turbines connected, >25k data points ingested per sec., 25 TB of stored data
- Operations are automatized using real-time wind turbine data
- Homogenous architecture from Edge to Cloud offers identical APIs
- Incoming data is normalized to a company namespace to provide high quality input for analytics

Benefit

- Reduced 'cost of energy' by ca. 2% and increased energy production by 1-2% by reducing manually processed alarms through automated alarm management, increasing remote control center efficiency
- Implemented Cumulocity IoT Edge based windfarm server for all new turbines providing as a flexible bases for new software on the windfarm level



[Read more here](#)





Case Study – Iridium Automates Oil Equipment in The Argentine Desert



The Challenge

The oil rigs in Argentina's Neuquén Basin are spread out across miles of desert. Operators must check the supply levels in water tanks – as well as the settings on fracking pipes – before using any equipment for fracking, but some of these facilities are so far apart that it takes two or three hours to drive from one to another.

Two companies sought to address this challenge: Tesacom, an Iridium partner in the region, and Exemys, a technology company that helps customers monitor dispersed and remote assets. The Exemys® GRD, a small and lightweight piece of electronic hardware for remote monitoring, can be attached to industrial equipment and connected to the Internet to provide status updates and enable workers to remotely adjust settings. However, these devices need a reliable connection to a robust network with coverage across the entire region. Some oil companies have used cellular networks to connect this type of equipment, but doing so is extremely resource-intensive: each location would require an antenna 3 or 4 meters in height, as well as transportation for both the materials and the construction team.

The Solution

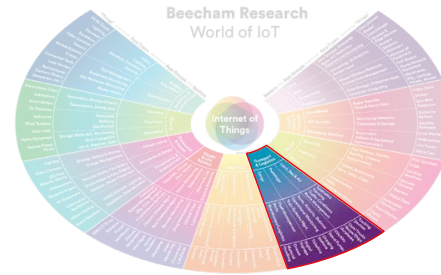
To communicate with their equipment, Exemys sought out a service provider that could offer easy-to-install devices and consistently strong coverage. Exemys reached out to Tesacom because Tesacom understands and facilitates the highly complex operations, logistics, distribution, and resource administration in the many sectors of the telecommunications industry. By combining its cellular telemetry


equipment with Iridium Edge devices, Exemys was able to establish communication with remote assets over Iridium's Short Burst Data® (SBD®) service. Through Exemys's online services, GRD users can get in touch with their equipment remotely for data retrieval and adjustments to settings.

Because Iridium Edge® offers 180° line of sight coverage, it functions fully when installed atop existing equipment, removing the need for Exemys to build antennas at each site. This also makes it much faster to get Exemys equipment up and running, cutting down on the time from purchase to full operation. As an added bonus, Exemys never has to worry about any of their Iridium Edge devices running out of power: "You can easily power it with a small solar panel," said Francisco Remersaro, Research and Development Manager at Exemys.

The Results

Workers can now remotely check the status of oil companies' tanks and pumps – as well as adjust their settings – without driving through the desert for several hours to do so. Iridium Edge offers connectivity 24 hours a day in remote locations from pole to pole. Many Exemys customers now receive automatic updates on the status of their equipment each hour, or even more often if desired.



 Transport & Logistics		
Application Groups	Application Types	Things
<p>Land, Sea and Air</p> <p>Passenger</p> <p>Cargo</p>	<p>Telematics and Tracking, Traffic conditions monitoring, Route management</p> <p>Ports, Airports, Railway Stations, Operational Monitoring Train systems management</p> <p>All of these types feature purpose build machinery whose components can be monitored e.g. predictive maintenance to detect imminent failure.</p> <p>Fleet management, Ports, Warehouses/Logistics</p>	<p>'Things' connected include connected vehicles, trucks, buses, ships, airplanes, trains; tracking devices attached to movable items, digital signage for highways and premises such as ports which need to be updated regularly; electric vehicles and their charging stations that record and transmit data for a range of necessary core management and control functions, billing, fault and maintenance management; connected autonomous vehicles or driverless vehicles which utilise new technologies including computer vision for collision avoidance; smart ticketing systems for passengers; wearables for the health and safety of workers.</p>

Analysts report a growing awareness among public transport providers of the benefits of connected transport systems; there is also increasing demand from travellers for convenience and accessible real-time information.

Application examples highlighted in the figure particularly relevant for ESG include:

Traffic Management

Traffic management is vital in local or city settings and on a nation-wide scale. It includes air traffic management and the European Space Agency (ESA) has awarded a satellite operator a contract to deliver a next-generation satellite-based data link communications system to enhance air traffic management (ATM) across Europe.

Fleet Monitoring/Telematics

Now well established, fleet monitoring is vital to saving fuel and unnecessary driving time for vehicle owners, while providing a record for the authorities regarding driving time and behaviour.

Smart Parking

Also well established, the benefits of smart parking are recognised for reducing

time searching for a space and reducing pollution. The system enables cities to automatically inform road users where to find available parking space as well as securing revenues for the authorities.

Street Lighting

Lighting accounts for approximately one fifth of the world's total electricity consumption, hence monitoring and controlling lighting usage is important for saving costs while also ensuring safety. Connected lighting makes it possible to dim lights, report faults, adjust lighting for weather conditions, optimise vehicle and cyclist detection as well as measure electricity consumption; intelligent street lighting allows city authorities to reduce energy bills.

AI-Enabled Traffic Lights

Artificial Intelligence can be used to effectively optimise traffic lights, saving costs and reducing waste. Through object detection algorithms, the AI moiety detects vehicles in images from traffic cameras.



Case Study – Enhancing Urban Environments through Smart Lighting



Public lighting is an essential element in effective city management – helping provide a safer, more secure environment in which citizenry can live and work. Massive IoT is seen as the gateway to the rapid adoption of new technologies that enable smart lighting.

A well-structured lighting system can have a big impact on people's relationship with the city. It can lead to a more bustling night life; a greater sense of security that allows shops to stay open later; or the possibility for citizens to go to a park to exercise at night or meet up with friends at the square.

Other benefits are reductions in criminal activity and traffic accidents, as shown in various studies from around the world. One study from the State University of São Paulo in Brazil, compared stretches of federal roads before and after the implementation of public lighting. For a specific stretch of road, the report showed a 35% decrease in the number of accidents and injuries, and a 60% drop in deaths.

Massive IoT applications allow for more efficient management – in terms of waste reduction, increased sustainable practices, and improvement in energy savings. In another example, in 2022, Everynet and BottomUp Telemetry partnered with the City of Recife, Brazil on an 8,000-unit smart lighting tele-management pilot — testing the possibility of dimming lights to save energy. The pilot was a success, with the city reducing energy consumption by 25% and expecting to

save nearly R\$1.5M annually – enabling them to expand the project to more than 100,000 smart lights by 2024.

Data provided by Massive IoT – and empowered by LPWAN (Low Power Wide Area Network) – allows local government officials to monitor more efficiently everything from the performance to the energy costs associated with their lighting infrastructure – allowing for corrective and predictive maintenance.

LPWAN delivers an open and robust ecosystem with the participation of mobile network operators, global MVNOs and lighting solutions partners. This resilient network enables scale and ultra-low-cost connections, empowering companies and governments to rapidly implement IoT services, without having to bear high investments and infrastructure complexity – delivering a brighter view to their citizens.





Case Study – IoT Connectivity Powers the EV Charging Revolution



The Problem

In 2022, Shell unveiled Shell Recharge in an effort to accelerate the journey to net-zero and support drivers in their switch to electric.

Before leading the advanced electric vehicle charging movement that we know and recognise today, Shell Recharge sought reliable, high connectivity providers who would make their vision into a reality and become partners for the long road ahead. With each EV charge station expected to have a lifespan of 5-10 years, it was considered imperative that suppliers understood the need to have reliable and future proof solutions.

Shell Recharge planned to open EV charge stations in Belgium, Germany, Luxembourg, Austria, the UK and Norway. However, their multi-regional deployment needed some thought. Certain regions face roaming restrictions which can affect connectivity levels.

The Challenge

Given that charge points aspire to be in action for a decade or more with minimum human intervention, it's important that they reliably perform. And they can only perform at their best if they have excellent connectivity.

Connectivity, in fact, is a critical foundation to the EV charge point operation including payment processing, software updates, scheduling, promotions, and user analytics. Shell Recharge sought an intelligent connectivity solution that would enable them to monitor and remotely manage every one of their charge points across Europe with ease and efficiency. In addition, the connectivity solution needed to port

the customer charging data back to the server and provide it to the customer through a user-friendly App and online charge portal.

Poor connectivity was not a risk that Shell Recharge was willing to take given that it reduces charger utilisation and negatively affect the customer experience, which can impact customer retention and even brand reputation. Ultimately it affects the bottom line as fewer customers can connect and charge their vehicles, and longer-term retention levels could drop.

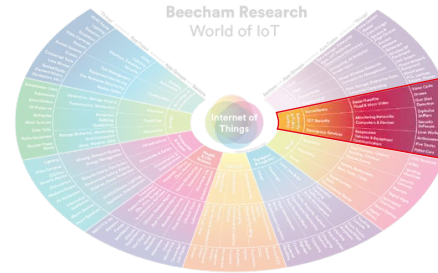
The Solution


Shell Recharge enlisted Eseye as a key connectivity partner because of our ability to deliver on connectivity in the most remote and challenging locations.

This used our intelligent single AnyNet SIM technology because we have established agreements with all the major mobile network operators and can select the best option for each charge point.

A single AnyNet Secure SIM card can be inserted into the charger at the point of manufacture and deployed anywhere in the world, and then programmed to switch network, either locally or remotely over the air, if the connection drops.

As a result, our network agnostic AnyNet connectivity solution can deliver on its promise of reliable mobile network coverage, delivering over 99% device availability globally. The AnyNet Secure SIM can be pre-loaded with up to 10 IMSI profiles meaning that Shell Recharge is assured with peace of mind knowing that their charge points are powered with consistent and reliable near 100% connectivity.



 Security & Public Safety		
Application Groups	Application Types	Things
<p>Surveillance</p> <p>ICT Security</p> <p>Emergency Services</p> <p>Environment</p>	<p>Radar and Satellite, Fixed and worn video</p> <p>Monitoring Networks, computers and devices</p> <p>Vehicles and equipment, responders, communications</p> <p>Water treatment, environmental monitoring</p>	<p>'Things' to connect include a wide range of items including Radar and Satellite, fixed and body worn video, weather balloons, buoys. Many IoT devices still come with no inbuilt security features and there is a requirement for more research into IoT device security and a forensic framework for IoT devices. Cybercrime forensics is a well-established science with active practitioners; devices themselves are good 'digital witnesses' as they can be sources of evidence data. The industry is constantly developing new tools to extract relevant data from devices which have been compromised.</p>

This sector comprises both Surveillance and ICT security, monitoring Networks, computers and devices. Large scale networks constitute larger attack surfaces, requiring enhanced safeguards.

Topical ESG issues raise the need for enhanced surveillance and protection of the public and the environment, including in the following areas:

Water Metering/Flood Monitoring

Climate change is bringing more abnormal and more frequent weather incidents, with higher risk of flooding where heavy rains follow long periods of dry weather and compacted soil. Flood monitoring using IoT can give advance warnings of floods.

Water Quality Monitoring

Extremes of weather in mid-2022 resulted in sewage being discharged into UK rivers and the sea. Water systems must be continually monitored for their ability to be safe for consumers as well as their ability to support aquatic life. A recently developed probe-based water quality monitoring system remotely measures the quality of water in rivers, lakes and reservoirs; it provides real-time data on the levels of dissolved oxygen, organic carbon and detects bacterial contamination.

Air Quality Monitoring

Clean air is now viewed as a social justice issue. Air pollution remains responsible for nine million premature deaths every year. Cities around the world are taking steps to improve the air quality for their inhabitants. Clean air zones and reduced traffic areas have helped but citizens living in the most deprived areas are often exposed to much higher and therefore more dangerous levels of air pollution. Air quality monitoring projects have proliferated in cities, including a smart system that measured and captured air quality conditions during the Birmingham Commonwealth Games in summer 2022.

Global Warming Data Collection

The Earth has experienced climate change in the past without help from humanity, however the current climatic warming is occurring much more rapidly than past warming events. Governments and agencies like NASA are urgently collecting data on global warming parameters including CO2 levels, global temperatures and sea ice quantities.

Waste Treatment Monitoring

This includes wastewater treatment as well as household and business waste disposal management.

Analysis of urban wastewater in Europe detected traces of coronavirus in domestic effluent before virus cases were detected in the area.

In cities, IoT-based tracking and scheduling of waste collection trucks both increases efficiencies and decreases the environmental impact related to the waste collection process.

Forest Fire Detection

Climate change and extreme heat incidents have triggered wildfires in many parts of the world, resulting in huge losses. The year 2022 turned into a record year for forest fires. IoT can detect small fires early before they spread; networks of sensing nodes strategically placed in forest settings can collect and process data and multispectral images. The systems can cover very large areas, including tourist areas.



Case Study – How Massive IoT Addresses the Challenges of the Modern City



The social and environmental challenges and solutions facing cities today are intertwined. In an era of rapidly changing demographics and urbanization, cities are responsible for consuming 78% of global energy, according to the UN, as well as being the major contributor to greenhouse gas emissions. Meanwhile, global electricity demand is predicted to grow 50% by 2040 and food demand to increase more than 50% by 2050.

Reducing the environmental impact of cities has become a top priority for governments. Smart City initiatives address this by more efficiently monitoring and managing the environment, resource consumption and waste, among other things.

Finding Ideal Smart Tech in Massive IoT and LoRaWAN

LoRaWAN, the go-to IoT networking protocol, stands ready to aid cities in their evolution. It is the ideal IoT technology for interconnecting Smart City services due to its long range, wide area reach, as well as other factors including security, low bandwidth and latency connectivity, durability, an extensive ecosystem of service providers,

out-of-the-box availability and much more. It allows for quick, massive rollouts serving a multitude of use cases. Device batteries can last up to 10 years, connect indoor and outdoor over wide areas, and deploy at such low cost that there is virtually no other viable alternative for Smart City projects.

LoRaWAN enables a variety of innovative city services designed to improve and enhance citizen's quality of life through cost-effective solutions. One such example is waste management solutions. In 2020, Everynet partnered with Lysir and Sensoneo to deliver a unique smart waste management solution in Reykjavik and Hafnarfjorour, Iceland. The collaboration focused on combining Everynet's carrier-grade and neutral-host national network with Sensoneo's unique smart waste management solution to allow waste companies, businesses and the cities to monitor waste bins, optimize collection frequencies and routes, lower their environmental footprint, and improve the quality of services. All relying on data transfer via LoRaWAN technology.



Case Study – How Massive IoT Informs Flood Management



Cities around the world are incorporating smart technologies driven by the Internet of Things (IoT) to optimize city functions, drive economic growth and improve quality of life for its citizenry. One example is the town of Cary, North Carolina where they are building the smart city of the future.

Historically Cary, like many towns in the United States and abroad, had no automated visibility to rising water levels during a storm. They simply relied on citizens to alert them of rising waters and flood situations through phone calls, text messages and the like. Town staff then processed these notifications and deployed public work personnel through a manual process. This approach often resulted in valuable time lost to mitigate property damage and loss of life during a flood.

Now, as part of their Smart and Connected Communities effort, Cary is implementing a SAS-enabled solution to address the challenges of stormwater flooding. By strategically placing a grid of water-level sensors and rain gauges at several key points around their 60-square mile town, they are gathering critical data about local water levels. This scalable solution integrates with existing business systems and moves the town from reactive to proactive – and in the long-term predictive – in their flood management efforts.

The Power of SAS Analytics and LoRaWAN Connectivity

The town's flood prediction system is built through a partnership with SAS and Semtech, leveraging Azure IoT, SAS analytics and LoRaWAN connectivity provided by Everynet's national network in the United States, to capture, analyze and share important data on water levels. While still early in its deployment, the solution is yielding positive results including the ability to:

- Visualize flooding events in real time.
- Automate the transmission of work orders and critical notifications to stormwater personnel.
- Share water/flood level data with regional partners.

Applying SAS Analytics for IoT, the town of Cary has enhanced their ability to acquire and manage new data, generate and deploy predictive models, manage the lifecycle of those models and move to a proactive stance in stormwater flood management.





Case Study – Iridium Short Burst Data® Improves Climate Monitoring Accuracy



The Challenge

Space-based remote monitoring of ocean temperature, color, and height is a key part of meteorological research. The European Commission established the Sentinel satellite program in 2014 to gather these kinds of data in conjunction with existing data from weather balloons, land stations, floats, ships, and data buoys.

However, calibrating and validating this system requires real-time data from the ocean to ensure that the satellites are accurately measuring the data remotely. To this end, the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) funded TRUSTED, a project to create a network of more than 100 marine drifting buoys with high-resolution sensors to capture sample data for comparison with the remote satellite data.

The Solution

Iridium partner CLS, in collaboration with its partners, was awarded the contract to develop a new buoy system, called the Surface Velocity Platform drifter with Barometer and Reference Sensor for Temperature (SVP-BRST).

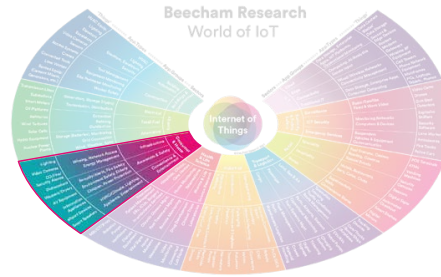
Using the Iridium 9602 transceiver and Iridium Short Burst Data® (SBD®) service, these buoys transferred High-Resolution Sea Surface Temperature (HRSST) data, as well as the buoy position to CLS who

processed the information for use with the Sentinel system. The completely global coverage of the Iridium network was critical in confirming that the buoys were capturing an accurate, truly global sampling of oceanographic data. Further, Iridium SBD allowed for insight into real-time data regarding weather events and ocean disturbances as they happened.

The Impact

The data transmitted through the Iridium network validated the Sentinel system and confirmed the accuracy and consistency in remote ocean monitoring, the key goals of the TRUSTED project. The buoy prototypes were deployed in April 2018 and the full network of buoys was deployed over the course of 2019, providing data measurements for 18 months.



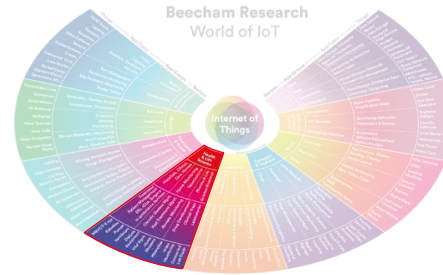


Consumer & Home

Application Groups	Application Types	Things
Infrastructure	Wiring, Network access, Energy Management	‘Things’ comprise home appliances, information appliances, smart speakers, washers and driers, fire alarms, video cameras, Carbon monoxide alarms, fire alarms, security alarms against intruders, as well as remote health monitoring devices.
Awareness and Safety	Security Alerts, Fire Safety, Environment Safety, Power Protection, Elderly and children safety	
Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment.	

The Consumer/Home sector is already set up for large scale use using Cloud servers, and domestic wearables (e.g. fitness) are ever increasing in

use. Remote healthcare is also relevant here (overlapping with the hospital environment), as well as smart meters for the Energy and Water industries.



Healthcare

Application Groups	Application Types	Things
Hospitals, clinics, Care homes	<p>Treatment – diagnostics, drug therapy and monitoring.</p> <p>Patient Management – patient monitoring, measuring and transmitting vital signs data.</p> <p>HRs – Electronic Health Records storage, maintenance and updating.</p> <p>ICUs – Instrumented Intensive Care Units.</p> <p>Surgeries – Connected healthcare centres.</p> <p>In-Ambulance services – connecting equipment to preserve patient’s life and readying the hospital for start of treatment with relevant data.</p>	<p>‘Things’ include robotics to aid surgery, connected ventilators to allow nurses to watch patients while at safe distance; connected vital signs measuring equipment, connected wearables outside the hospital, remote video monitoring to monitor patients in rehab; connected laboratory equipment to enable remote monitoring and automatic data collection to ensure against failure of that equipment. Connected laboratory equipment for ensuring it is in good working order and predicting breakdowns.</p>
Home Monitoring, Telemedicine	<p>Chronic Disease management – patients at home through continual recording and transmission of vital signs data to the clinic’s IT system</p> <p>Post treatment management – recovering and rehabilitating after in-hospital stay.</p> <p>Remote Monitoring</p>	
Pharma and Life sciences research	<p>Drug Development including manufacturing – instrumenting assembly lines</p> <p>Clinical Trials – including remote monitoring of participants.</p> <p>Laboratories – laboratory asset management and tracking.</p>	

Healthcare in Hospitals is characterised by dense networks, with short range technologies, and this will become more so.



Case Study – Iridium Connected® Drones Deliver Vaccines in Remote Areas



The Challenge

Vanuatu is a Pacific Island nation made up of more than 80 islands stretching over 1,300 kilometers. Due to dense forests and a lack of infrastructure, the distribution of medical supplies – particularly vaccines – is a persistent challenge for the country. In Erromango, the country's fourth largest island, one in every five children is not immunized because of this challenge.

Additionally, vaccines must be kept cold and administered at specific, regular intervals to maintain their efficacy. However, local storage of these vaccines isn't possible due to unreliable local power supplies and fast delivery is impossible without local transportation infrastructure. Health workers would have to walk across treacherous terrain and take long drives and boat rides carrying vaccines in coolers.

The Solution

On-demand drone delivery was a logical solution to the problem of vaccine distribution. UAV manufacturer Swoop Aero collaborated with UNICEF and Vanuatu's Ministry of Health to develop a program for drone-based vaccine delivery in the area. However, even with this innovative solution challenges remained. The drones' original remote command and control (C2) functions were managed over local cellular networks, but engineers found that this was unreliable and frequently disconnected.

Instead, Swoop Aero worked with Iridium partner M2M Connectivity to integrate the Iridium Core 9523 transceiver into their drones' C2 systems. The small, lightweight transceivers were easier and less

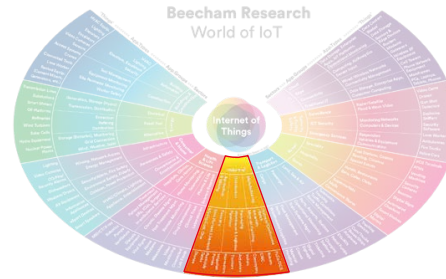
expensive to integrate than other solutions, and offered even more reliable connectivity through Iridium's global, two-way Short Burst Data® (SBD®) service. Additionally, the transceiver used very little energy, allowing the drones to use most of their battery power for powering the engines and refrigeration.

The Impact

With the Iridium Connected® drones, local nurses and healthcare workers were able to deliver vaccines and essential medical supplies to local populations faster and more easily than ever before. Public health in the archipelago will continue to improve as more residents are vaccinated.

Beyond Vanuatu, Iridium Connected drones also offer Swoop Aero the ability to expand their mission to support critical medical services in developing nations around the world.





Industrial

Application Groups

Manufacturing

Distribution

Agriculture & Mining

Application Types

Discrete/Continuous/Batch, Assembly, Materials handling

Packaging, Warehouse and logistics, Pipelines

Forestry, Sow, Harvest, Livestock, Mining, Coal, Ore – mine site management

Things

‘Things’ comprise a very wide range of equipment that include connected assembly lines, robots, valves and pumps for manufacturing; drones, forklift trucks for transporting pallets, conveyors and drones for warehousing and logistics; RFID for smart packaging and tracking items; connected pesticide tanks to monitor levels, connected harvesters, connected tractors to ensure machine in good working order, where messages are sent back to the manufacturer to help design improvements; connected animals in agriculture to enable remote checking of their condition e.g. a cow in oestrus; field robotics are finding increasing use as agricultural workers are becoming scarce; instrumented mining equipment, caterpillars and excavators for predictive maintenance in the mining industry, as well as noise, vibration and pollution sensors to protect workers.

The industrial sector has huge scope for massive IoT. The smart factory is dense with a range of technologies, particularly with the greater need for real time working and IoT at the Edge. The agriculture sector is seeing

more and more connected applications to boost efficiency, yields and reduce the wasteful application of resources.

Case Study – Opening doors for SMC with Cumulocity IoT

 software^{AG}

SMC specializes in manufacturing of pneumatic equipment for its end users. With Cumulocity IoT SMC can integrate with any “thing” and incorporate IoT data into any cloud service, core system or application. With no coding required, the solution was set up and running in under 20 minutes. The solution’s sophisticated analytics and preventive maintenance save the company and its end-users costs associated with leakage-caused air loss.

Challenges

- Air leakage in machines results in extra costs for end-users
- Need to deploy an effective IoT-driven solution
- Bridging the gap between data detection and data capture

Outcomes

- Decreased costs by saving 20% compressed air previously wasted
- Prevented and detected leakage, avoiding downtime
- Centralized smart analytics, predictive maintenance, and energy efficiency monitoring

Solution

- Cumulocity IoT enables SMC to integrate with any “thing” and integrate IoT data with any cloud service, core system or application.

Energy transparency as a new business model

In the highly competitive manufacturing sector, companies like SMC are constantly looking for ways to stand out from the crowd. SMC observed a trend in the growing interest from their end-users in predictive maintenance with frequent questions around what is happening in the machine. Manufacturing customer expectations are constantly evolving. SMC reached out to Software AG, and it became quickly apparent that Cumulocity IoT could offer SMC many advantages. Within four months of implementation, SMC and Software AG were able to develop the Smart Field Analytics offering and go live with its first use case in Germany. The partnership has created subscription-based revenue streams for SMC and helped steer the business in a whole new direction of growth with a growing list of development prospects.

“In the past our company was regarded primarily as a component supplier, but now we are a solution provider including hardware, software and services, meeting our customers’ needs in ways they never expected before.”

Oliver Prang, Expert Digital Business Development,
SMC Germany

 [Read more here](#)





Case Study – IoT Platform

The data gathered by Internet of Things (IoT) devices could make even the most well-established industries more efficient, productive, and sustainable. However, the same connected technologies could also put asset owners and operators at risk. As industrial IoT (IIoT) applications (such as manufacturing, agriculture, construction, energy, utilities, medical and transportation are being transformed), cyberattacks are becoming increasingly more common – not only in cases where devices are decades old, with hardly any security measures built-in.

Leading IoT hardware and software components supplier, Eurotech, is helping companies to benefit from the digital transformation of industry, while ensuring their assets and the data they generate remains secure. To combine multi-core performance with the required communication technologies and advanced security features, Eurotech has developed the ReliaGATE 10-14 multi-service IoT Edge gateway. It's powered by the NXP Semiconductors i.MX 8M Mini, (which is based on the Arm Cortex-A53) and is designed to provide connectivity to industrial assets, field protocols and cloud connectors including Eurotech Everyware Cloud, Microsoft Azure, AWS and others. The IoT Gateway also comes

with preinstalled optimized Linux operating system and a powerful IoT Edge Framework, Everyware Software Framework (ESF), which provides a flexible no-code/low-code application development environment for edge computers and IoT gateways.

The offering helps customers and system integrators to reduce their time to market and development efforts without compromising security. With this IoT Gateway Eurotech achieved PSA Certified Level 1 compliance, which means they have met the fundamental security requirements that help to protect a device. The PSA Certified framework and independent assurance scheme helped Eurotech to deliver industry-leading security for their edge device, an important step to meeting the requirements of the operation technology security standard IEC 62443-4-2. This Eurotech approach of security certified integrated hardware and software, helps significantly to remove the barriers to security and make building a more secure IoT solution quicker, easier, and more cost-effective.





Case Study – Internet of Cranes® Provides Intelligent Control Through Real-Time Data



The Problem

The monitoring and maintenance of crane fleets has traditionally involved the operator fielding a team of technicians who needed to travel to the site to carry out the necessary work, often responding reactively to incidents. Fassi Gru recognised the potential of emerging Internet of Things (IoT) capabilities to increase the efficiency and effectiveness of this process.

A leading manufacturer of articulated and hydraulic cranes, Fassi has customers all over the globe and the ability to produce 12,000 cranes on average per year. As a pioneer in its sector, it has always sought to create innovative services to support operators. In 2015 Fassi began developing a unique system that would take advantage of IoT technology to provide intelligent control for the remote management of cranes, by making all information related to operation, performance and status available in real-time.

The goal of the system – christened the Internet of Cranes® (IoC) – was to enable operators to create efficiencies and improve crane performance. Remote access to vital data would enable rapid response diagnosis and assistance, from either the operator or the Fassi support team, and swift resolution of malfunctions. It would also make predictive maintenance possible.

The Challenge

Fassi's vision for its IoC system was that operators should have up-to-the-minute data at their fingertips, and the ability to rely on an assistance service that was permanently active. This required constant,

dependable internet connectivity globally. When the IoC project was initiated, cellular coverage was fragmented across the globe – with a mix of 2G and 3G networks, and carriers using a range of communication frequencies.

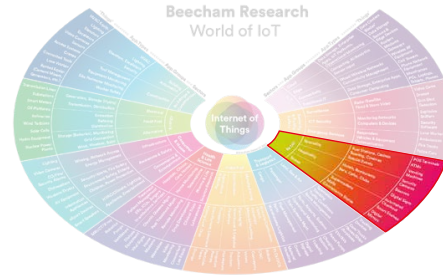
The Solution

Micro Systems partnered with Eseye to take advantage of its AnyNet SIM cards with multi-IMSI technology to deliver the universal connectivity required to operate Fassi's IoC system to its full potential, through a single device.

The global mobile network alliance Eseye has built allows it to offer the widest range of interconnects and provide the most comprehensive localisation strategy in the IoT market today. This grants the AnyNet SIM with the unique ability to connect directly and automatically to the best available network.

The bespoke electronic board designed by Micro Systems is connected to the web by Eseye's AnyNet SIM card. The SIM is installed directly on the board during the production phase, and easily activated by the end customer.

A dedicated web portal allows operators and the Fassi support centre to view and manage the data from each individual crane. The integration of Eseye's SIAM (SIM Information and Account Management) portal allows the operator and Fassi to monitor SIMs in a single virtual space – including details on the activation/suspension date, phone number, monthly traffic and location.



Retail

Application Groups	Application Types	Things
<p>Speciality</p> <p>Hospitality</p> <p>Stores</p>	<p>Casinos, Bowling, Cinemas, Special events</p> <p>Hotels, Restaurants, Bars, Cafes Clubs</p> <p>Supermarkets, Malls, Convenience stores</p>	<p>'Things' include point of sales terminals, Automated check-out machines, Automated Teller machines; connected vending machines to ensure they are replenished when needed; Security cameras, Digital Signs to direct passing customers which must be kept current, Beacons to alert shoppers via their smart phones to special in-store offers; smart shelves or intelligent shelves have sensors built in to gather data, such as the number of items on a shelf, their packaging etc. Digital mirrors help customers visualise how a garment will look by recording and displaying real and virtual outfits.</p>

This sector may be leading to mass deployment, perhaps with short range technologies such as Bluetooth, Wi-Fi and even shorter range – such as RFID tags.



Cellular Connectivity Accelerates Payment Processing Revolution



The Problem

Yoco is a fast-growing Cape Town-based financial technology company that provides mobile card payment devices to upwards of 120,000 small business owners across South Africa. With a mission to ‘target the underserved and the underbanked through economic inclusion’, its aim is to drive the country’s economy forward by helping entrepreneurs to be successful. Yoco’s card readers are designed for SME retailers who are too small to qualify for a payment device from the established banks. They make processing online payments simple, and work anywhere – from a mall to a street corner.

There are around five million entrepreneurs in South Africa, and their need for straightforward, flexible payment solutions has never been met by the big established banks. In fact, 70% of the merchants Yoco serves today had never been able to accept card payments before.

The Challenge

Rapid transactions are key to small retailers’ profitability and depend on payment devices being ready to go at all times. The challenge Yoco faced was how to ensure continuous connectivity to the internet without adding complexity.

For instance, standard payment machines use SIM cards designed for consumer devices, that are tied to one mobile network. Each network has different coverage levels, and devices that rely on a single network won’t work in 15-25% of locations.

This meant that while Yoco’s standalone terminal might work well in one

area of the country, it might struggle to connect in a more rural location or on the bottom floor of a mall.

Another challenge to overcome was the mobile operators’ strategy of dropping connections to idle devices in order to maximise utilisation of networks. This results in a short wait for the connection to re-establish when the device is turned on. To get around the problem, some payment devices implement software configurations that ‘ping’ websites as frequently as every 30 seconds to prevent the connection dropping, but this consumes a lot of unnecessary data.

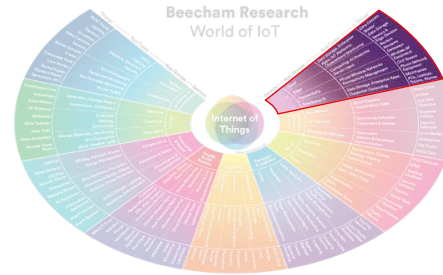
The Solution

Yoco selected Eseye’s AnyNet+ multi-profile, intelligent SIM after running a successful pilot. A single SIM is inserted into each device before it’s shipped, and programmed to switch network automatically and seamlessly. It can also accept over-the-air switches as required.

Based on how the device would be operating post-deployment, Eseye simulated a range of normal and challenging environments to check it was connecting properly, how much data it used, and how quickly it recovered in the face of problems such as a network failure.

Eseye’s in-house hardware experience and knowledge helped Yoco to identify issues early, so these could be addressed before going into full production.

As part of the onboarding process, Eseye helped Yoco prepare the Neo for deployment, putting the entire solution – including hardware, modem, module, and SIM – through rigorous and thorough lab testing to make sure everything performed as expected.



ICT		
Application Groups	Application Types	Things
<p>Cloud – The Cloud is where large scale data transmission, processing and storage takes place;</p> <p>Edge</p> <p>Connectivity</p> <p>Traditional IT</p>	<p>Data storage, Enterprise apps, IoT platforms, Operational Monitoring</p> <p>Computing – Edge computing takes place near where the sensors record and transmit the data providing real-time information, which enables decisions and actions to be taken immediately, both manually and automatically.</p> <p>AI/Analytics – AI and analytics uses a wealth of data stored and collected to provide a rich set of information for decision making. There is some debate however that questions the trustworthiness of data generated purely from AI algorithms, as compared with data captured at source.</p> <p>Sensor input – from connected sensors at the Edge.</p> <p>Wired/Wireless networks, Connectivity management</p> <p>Data storage, Enterprise apps, Consumer computing</p>	<p>‘Things’ include the entire computing and networking estate – fixed and wireless – that can be instrumented and connected; data centres, data ‘blades’, all types of computer from mainframes to PCs and laptops; phones, sensors and edge devices; routers, modems, gateways, wireless equipment – cellphones, cell towers (masts), networking equipment. All of these ‘things’ can be monitored for traffic and signs of imminent failure (predictive maintenance) and other uses.</p>

The computing and IT sector has potential for massive IoT; scaling from small deployments to large ones involving many connected devices means

addressing many more issues, from authentication and end-to-end security to handling faults and to data analysis.

Ishikawa Diagram – AIM: TOWARDS MASS IoT

To date IoT networks have not been massive. However real-world deployments have not only helped the researchers and application developers create protocols, standards, and frameworks, but also helped them understand the challenges that come with the management of massive deployments. Large scale deployments will normally have a mix of new and legacy devices that use different technologies and serve multiple purposes; this reflects the way IoT has evolved.

The Ishikawa or Fishbone or Cause and Effect diagram is an analytical tool named after its Japanese inventor Kaoru Ishikawa. It explores the range of factors

contributing to a specific outcome or state of affairs, in this case, massively scaling IoT deployments. Each ‘bone’ represents a type of factor, and the factors selected for analysis are divided into influencers (smaller bones) that all contribute to the outcome.

The value of this tool is to try to get a wider view of the scenario which includes not only technology and factors that spring to mind most readily, but also regulatory, political, environmental, legal, societal developments as well, to allow readers to get the full picture of how that outcome is made possible.





Streamlining IoT Architectures

Designing Networks for Scaling

Once a deployment starts to scale it will be increasingly difficult to perform even the most basic operations such as onboarding, configuration, security patches, and maintenance manually. When there are numerous devices with multiple sensors and actuators that generate massive amounts of data every second of everyday, organisations must design for growth from the outset, with the flexibility to rapidly scale up if the service is successful.

Device Estate Management

Here, visibility and control of the entire device estate is essential, and the solutions require the highest possible operational efficiency and reliability. As the device pool grows larger it is imperative to have an overall device management system for faster installs and provisioning. Networks have to be able to integrate other sensors and operational information. Reducing provisioning costs is important for making the business case work; the amount of manual provisioning involved is clearly going to be a factor in the deployment cost. In addition a platform that can manage it all is mandatory.

More Low-Cost Low Data Rate Connections

The market needs low data rate and low-cost devices. There will be many more low bandwidth connections, with over 80% of all connections being low data rate – meaning large numbers but not much money coming from each. The only real way to manage this in future is using more automation; enabling speedier processing and providing more traffic capabilities to manage increasing data traffic as millions more mobile and IoT devices come online. Edge computing will play a significant role.

IoT connections have traditionally been manually installed, but this is only really feasible for small numbers of connections unless there is a special team assembled, such as for smart metering projects. So, large deployments will either mean dedicated teams or connectivity embedded in hardware during manufacture. Connecting hardware during manufacture has traditionally been seen as something for OEMs to do if they want to add connectivity and a service to their products. This is different; it is specifying connectivity to a third party

manufacturer as part of a specification for a wider project – sensors in roads or other infrastructure, for example.

Remote Upgrading

This is essential, since long term deployments will necessitate regular updating of devices' SIM cards. The functionality of the SIM gets updated, not the physical SIM, and iSIMs are integrated in the chipset, they are not on a card.

In addition to relating to SIM cards, remote upgrading may be application-related, connectivity-related, or in particular security-related. The ability to upgrade software/firmware remotely is dependent on the type of connection available. Low data rate connectivity may take a very long time to upgrade a piece of firmware, unless it is organised for efficient upgrade. Also, if many devices need to be upgraded at once, this needs to be managed and coordinated in case of failures. Managing a large population of devices remotely is a whole different ballgame to managing a few.

Operations Support Systems

Back office operations include order processing and provisioning, including support for multiple carriers. Improved fault handling and consistent quality of service across all markets supports smooth operations. There is a need for fast service in the field for faults arising. With a large deployment, managing failures needs to be more automated to ensure service can be resumed quickly.

Hardware and Software Design

Makes possible large-scale integration of multivendor devices. Architectural design to support scalability, multiple and rapid message flows, enhanced memory, faster processors etc. beginning with the device, to cover gateway, IoT middleware, and ending with the third-party application or integration. Experience has shown that a large number of IoT projects are from enterprises trying to upscale their solutions but finding they need to start again. An IoT solution designed for a small deployment may be totally unable to scale to a large deployment. Typically, initial installations are Proof of Concept or maybe a stage beyond that. Often the hardware – but particularly the software in an IoT platform



Streamlining IoT Architectures (cont.)

– may be completely inadequate to upscale. It may mean starting again rather than growing what is already there.

Interoperability

This entails bringing together multiple technologies and data handling. In large scale solutions, the need to share data more and more leads to the requirement for more interoperability. Interoperability and Internationalisation are closely related; as deployments get larger, the need for interoperability between different supplier systems – often across borders – increases quickly. This includes not only the solutions themselves but the end-to-end security to protect it.

Internationalisation

For expansion across markets, this entails ensuring consistent quality of service across all of these, including accommodating different partner ecosystems.

Standardisation is a key enabler for this. For each new market, deployments must consider new suppliers and partners, new regulations, long term changes e.g. sunseting of networks etc.

For the healthcare sector, devices will be subject to regulatory approval for treatment of patients. The requirements for conformance may differ from country to country.

Automation/Autonomous Devices

Automation of tasks is essential especially for deployments at distance; autonomous devices perform specific tasks without intervention; automated provisioning for example saves cost of manual provisioning.



Players

ICT Suppliers

Comprising hardware, software, networking, systems integrators, solution providers; Managing multiple vendors of devices and machines can be challenging, particularly in long term deployments where vendor lock-in could become a problem.

Makers of sensors and devices ideally should improve the defect rate of finished items; as the device estate grows, individual numbers are significant; if the defect rate is 100 parts per million, with 5 million units, 500 will not work.

In fast moving verticals(including healthcare), vigilance is especially important to stay ahead of changing developments, so the need to looking to solution providers for security-related and privacy related issues.

Wireless Service Providers

MNOs MVNOs, satellite operators – need to ensure they can scale also in new markets and keep up with new generation connectivity technologies.

Security Infrastructure Providers

With greater scale, the risk of security breaches escalates; this can only be addressed with more automation.

Data Scientists/Programmers

Updated skills will be needed to support scalability over time, applications and new technological developments etc that change with time.

End Users/Subject Matter Experts

Important that these understand and stay ahead of new technology, and new industry developments.

Regulators

Country specific regulators; some regimes are stricter than others; multi-market deployments must keep abreast of changing regulations wherever they operate.



Players (cont.)

Partner Ecosystem

Anticipating new partners over long-term deployments is needed in terms of e.g. upgrading security, sensor types, managing new suppliers, resources etc. As deployments grow in size, it may become unrealistic to assume that one supplier can run it all. IoT solutions are usually a result of partners working

together. For very large deployments, that ecosystem needs to be considerably larger and with a wide range of ecosystem partners working together; that is a much larger project management issue and there is a greater need for interworking. Security, sensor types used, etc. all become bigger issues to coordinate, often internationally.



Technologies

Wireless Frequencies

The use of spectrum for multiple frequencies include LoRa, WiFi, 2G to 5G, Cat/M, NBLoT, LTE, Sigfox, satellite. For extensive and long-term deployments, support for multiple frequencies is needed; there could be a case for converging public and private networks. Some spectrum is free, e.g. that used by LoRa.

Lifecycle Management

End to end lifecycle management – to consider 2G sunsetting, 4G to 5G upgrades – for very long projects, the services and their components will change. For product and service planning, a holistic approach would address all activities from product planning, development and testing, and extend beyond the product release to include post market surveillance.

Root of Trust Security

With ever-increasing incidents of intrusion, denial of service, spoofing attacks, etc., businesses must take a strategic view of IoT security. Security by Design secures vulnerabilities throughout the entire IoT technology stack and identifies the layers where attackers may have access.

Data Integrity

It is important to ensure that data is not degraded from collection to processing as the path becomes longer. Data integrity is about trusting the data received, that it

has come from a known and recognised source and has not been interfered with along the way. End-to-end security is specifically required to achieve this. With technology changing the way application related information is handled, having good data security has never been more important.

Cloud and Edge Processing/Computing

Edge computing describes a distributed version of computation that brings data processing closer to the data source. Cloud processing by contrast is based on a centralised model, where data would be sent to a data centre or the Cloud. Edge computing is not a replacement for centralised data-storage models, but rather these architectures should work together to be beneficial. In expanded IoT networks, many functions can be moved to the Cloud.

IoT Analytics

IoT analytics and tools comprises a range of techniques to gain insight from the masses of data collected from the networks of sensors. They include Machine Learning, Artificial Intelligence, Augmented Reality/Virtual Reality/Machine Vision. These tools will assist in supporting a speedy decision if an anomaly is detected.

In particular, AI and ML in IoT is about the management of the networks in addition to application data. AI will become increasingly important for network



Technologies (cont.)

management to cater for faults arising, including security breaches. The larger the deployment, the more open it is to attack (with a larger attack surface) yet less capable of being managed manually. AI might for example anticipate threats, even shut down part of the network if necessary. AI-enabled medical devices can quickly adapt to new information and changing conditions.

eSIM/iSIM

The eSIM/iSIM is a programmable SIM card embedded into a device that allows users to switch to another connectivity provider more easily, also enabling remote upgrading of devices in the field.

The traditional SIM card (UICC) has been used for three decades as the trusted, tamper proof element for secure authentication of users and mobile devices to cellular networks. Right now eSIM technology provides a unified approach to global, future-proofed connectivity that can help organisations scale IoT deployments into networks that comprise hundreds of millions of connected

devices. eSIMs and the newer iSIMs allow multiple connection profiles per device, thereby providing easier switching: easier set up is more important than switching between networks plus enhanced security. In addition, over-the-air provisioning enables zero-touch provisioning of massive IoT devices deployments at the touch of a button; this reduces logistics to a simple, single-SKU approach that reduces time to market and reduces costs.

In addition to the traditional use of the SIM for secure access to cellular networks, IoT SAFE can now extend the SIM to also provide security of the data. This is not limited to eSIM/iSIM, but is available for traditional SIMs as well.

Condition Monitoring/Preventive Maintenance

A key use case for large scale deployments; the ability to monitor the performance of connected equipment in real time makes it possible for operators to resolve issues proactively before a breakdown occurs, thereby preventing delays in operations and unplanned downtime.



Economic and Regulatory Imperatives

Cost Economics/RoI

Given the major additional challenges in rolling out mass IoT deployments as indicated under 'Streamlining IoT architectures', a return on investment exercise performed at the start will avoid surprises as regards costs and other factors.

Standards (for interoperability)

Standards for interoperability relate to data sharing across borders; countries differ in how strict their regulations are e.g. for personal data privacy. Separately, the safety of medical devices has been traditionally assessed on the basis of predetermined risk assessment practices; ISO 14971 is designed to help medical device developers.

Net Zero Carbon

All industry must reduce their carbon emissions to zero – different countries have specific goals and recommendations.

Waste Reduction

As a result of industry and governments recognising the planet's ever reducing resources, these now mandate the urgent reduction of waste, including the excessive use of fuel, power, water.

Market Research & Analysis

What is the view of the market about mass IoT deployment? Through exclusive research for this report, including interviews with senior industry management and survey findings, this section provides market analysis of the move to mass IoT.



Industry Expert Interviews

In the section below we provide some actual examples of replies (shown on the right side of the page), and our summary of all the replies given (on the left). Our respondents were senior executives from companies that covered a broad range of specialised IoT based services, including;

Global device makers and M2M solutions providers, Satellite Operators, Provider of radio and satellite communications, MVNO M2M enablers, Smart buildings solutions and services providers, Smart city solutions and services providers, Smart transportation and safety solutions providers and Connectivity providers.

Question 1. Are you deploying or planning to deploy very large populations of IoT devices in the near future?

Our respondents were deploying IoT device populations ranging from a few hundred through millions of units. Massive deployments are not achievable with people, requiring enhanced Cloud processing.

- “Deployments are centralized, let's say, one factory with millions of devices that are dispersed among cities.”
- “We are at an advantage from an infrastructure perspective, because we are using LPWAN technologies and upstreaming large quantities of data.”
- “We make more intelligent devices that need the cloud infrastructure costs or the communication costs that can support all the raw data coming from massive IoT to the cloud. A significant amount of processing that the data needs is to be conducted on it, within the device.”
- “Our philosophy and approaching Massive IoT is to make bigger and bigger cloud services and faster and faster communications for all systems.”
- “Now we are moving to the age of a controlled solution which is not achievable with people.”
- “It is critical that cloud technology can deal with hundreds of thousands to millions of units. It is no longer about the extremely expensive IoT Device that has a high-speed LTE connection, it is about very large numbers of units with a few messages.”
- “In satellite world I would say it is pretty different than cellular market or LoRa Networks because we are dealing with a niche market, where the territorial networks are making limitations in terms of coverage. In terms of volumes at the moment, I would say a typical IoT project would start from 200 units to 5000 units.”
- “We already have large scale IoT Projects, connected cars, and this is our biggest market. 0.7 million cars in Europe; second market segment is IoT Devices in connectivity for predictive maintenance for aircraft; the third market segment is tablets where we have more than 1 million devices connected.”

Question 2. Which connectivity technology/ technologies are you using for these?

A wide range of connectivity choices and mixes are employed, given the availability of the technology capabilities for the context, location and application. 5G implementations have started to appear.

Question 3. What was the basis for your choice of technology? Do you see problems arising with these technologies, or others that you have chosen not to use?

Our respondents provided a wide range of implementation experiences, based on available resources in the country. Important to take into consideration the lifetime of the project, during which time available resources e.g. enabling technologies may change. Practical experiences of value to readers planning massive IoT expansion projects.

“ Now we have tools to deploy massive IoT services globally, whether we are using cellular, LoRa, Zigbee or Satellite or any of those technologies. Customers do not need to know the technical specifics and we basically make them work. ”

“ In the very short term, we are focusing on LoRaWAN because there is an existing and pretty mature ecosystem. ”

“ We are using primarily 3G and 4G, we have started to deploy 5G, in some countries where networks are 5G compatible. We cover about 180 countries with 3G and 4G. We have about 10 countries with 5G. We are just starting to deploy LTE/M in 40-50 countries, and we are experimenting with NB-IoT. ”

“ A transitioning has started from wired or propriety long range wireless to Internet-based device management for faster installs and smarter controllers. ”

“ Remote control and processing need broadband through fibre, cable and cellular failover. Wi-Fi can be used to monitor and connect. ”

“ They do not just use one technology and that's why we bridge 2G, 3G, 4G and 5G all together and allow local SIMs globally. ”

“ Sometimes in buildings the cellular coverage is not sufficient so you could use Sigfox as a back-up. LoRa and Sigfox could be a good back-up and at the same time one can be the diagnostic tool on the other one. ”

“ So many devices in the field are 2G only and 2G is going to remain in many countries. Now what we see is that there is the problem that in some countries 3G is going to stop before 2G. ”

“ The main influencers vary such as data direction, software customisation, building penetration and outdoor reach. Problems arise when existing networks can't be scaled up. ”

“ This self-developed cloud-based platform enables many IoT services and challenges traditional networks. ”

“ 3G is going to be a problem in some countries, so the future is 4G and 5G. ”

“ We have a wide portfolio of solutions from flood defence to leaking water detection, bin collection, street lighting to transport volumes (different public and freight services). They can use a mix of connectivity technologies (smart city). ”

“ Firstly, the choices of technology are based on cost, newer technologies are of course more reliable. The second criterion is the power consumption, it depends on the kind of deployment. ”

Question 4. What issues do you see in deploying and supporting these large deployments? Do you foresee scaling issues? If so, how do you plan to meet those?

Advice for successful implementations, including identifying pitfalls; starting with understanding the business case, preparing the proof of concept, costing, anticipating local regulations, anticipating conditions and changes under which the implementation will operate etc. A good Cloud platform can put up to 2 million devices per minute.

Question 5. Do you anticipate challenges in the following activities? If so, what are these and how do you anticipate handling them?

Breaking down advice into phases of implementation, key advice for success in e.g:

Provisioning – a product that can be used in multiple markets; automation avoids the cost of manual provisioning

Installation – ensuring that the devices are as fault free as possible – encouraging quality control in their manufacture; when rolling out

“ Probably the number 1 challenge is taking on more than that businesses can manage themselves. Number 2 is the vast number of IoT platforms at a Proof of Concept (PoC) level, anyone in the world can have a POC for a long time not earning money. The ability to actually scale that is by creating production systems that operate continuously and can grow flexibly. ”

“ With our cloud platform we can put up to 2 million devices per minute, we can scale our gateway to 20,000 per minute and we can add 50,000 users. ”

“ Compliance with local regulations, security rules; how to comply with regulations in Europe, in US. Facing multiple integrations, you multiply your cost of integration. ”

“ The plan is to make servicing more efficient and lower the cost of investment to the customer. Many deployments are not just larger but also have smarter controllers for smaller areas. ”

“ The systems are highly scalable. Smart analytics and remote monitoring helped in the past to bring new control centres on board and install with less hardware. ”

“ Venues with large crowds are demanding. Peak usage needs to be predicted for future use cases. ”

“ Traditional telco's have started to accept that core functions can be moved to the cloud and that there is a need to converge public and private networks. ”

“ Networks need careful planning and good back-haul is essential to future proof the different use cases and to make the outcomes available. ”

“ Provisioning is the number 1 challenge for customers, they want to have a product that they can use in multiple markets, they also want to have one product that they can use for multiple customers. The amount of manual provisioning involved is clearly going to be a bigger factor in the deployment cost. Reducing provisioning cost is the most critical aspect for making your business case work. Highly skilled technicians are not cheap. ”

“ First when you do a very large deployment for sure you will have problems. If you look at the defect rate, if it is 100 parts to million ppm, so if you have 5 million units, you will more or less 500 devices that will not work. ”

“ Maintenance is an interesting one, because the vast majority of IoT out there is specifically deployed to improve maintenance. The purpose of IT is literally to support IoT maintenance. IT needs to either be completely maintenance free or near to it. What is very important is that updating is designed from the very beginning, that means you integrate that on the hardware design (to be updated remotely) And very importantly it is using a powerful network management platform. ”

Question 5. Cont...

thousands of devices as opposed to hundreds, a small number of defectives become important.

Maintenance – over the air upgrading should be designed in from the start to avoid serious costs. Technology upgrades, perhaps unanticipated at the start; implementors must ensure that connectivity products have a lifetime that matches the customers' expectations. Existing devices will have to be retrofitted and upgraded during the time. In planning, need to also consider timeframes, available power and frequencies that vary locally.

Security – It is a multi-layer topic, security with devices, networks, data storage etc; implementors are part of this end-to-end security process, including securing the infrastructure; however, it is the client who is responsible for security.

“ We think that embedded devices which will be Massive IoT are not always IP connected unless they need that sophistication, making sure that you have the ability to manage and control it so managed security services are just critical. It is a multi-layer topic, security with devices, networks, data storage etc, of course we will part of this end-to-end security process, but we are not responsible for each component. We are in charge of securing the infrastructure, the communications between the device to the satellite secure up to our ground segment, so we will secure the data from the device to the LoRa network servers only. Other parts are not under our responsibility. ”

“ In IoT Security is a huge issue, security at the end is the responsibility of the customer. ”

“ The big problem in the IoT world and the Mass IoT deployments, you know for sure that none of your products will be there 10 years. We are really focused on is making sure that's you have connectivity products that have a lifetime that matches the customers' expectations. ”

“ The exiting devices will have to be retrofitted and upgraded. ”

“ They are constant challenges and need to be considered in every design. ”

“ We are anticipating changes in all of those areas in new projects or with the expansion of current operations. ”

“ New technology is often easier to install but requires planning and convincing. Timeframes, available power and frequencies vary locally. ”

“ They are everyday challenges with local telco-companies. Our platform automates those time-consuming steps needed to stay connected. ”

“ All of those need planning, a good level of automation and detailed documentation. The aim is a seamless service for many users. ”

“ Often the choices of technology are based on a lifetime project, so in many cases you will need to change all the products. ”

Question 6. To what extent do you see Over-the-Air updates as significant for these activities?

OTA upgrades are a must-have and save a great deal of time. They are one part of the minimum-security standard for remote controlled systems.

Question 7. Do you see the need or opportunity to use AI/ML to assist with these activities? If so, in what way?

All but one respondent said that AI and ML help detecting an issue sooner, achieving a speedy decision; only one said their need was coming but not immediately. Complex systems with many participating parties need some level of AI for basic functions and access alone.

“ You take, let’s say a LoRaWAN typical OTA set-up, it is about 17 hours to do devices, we can achieve the same thing in 2/3 minutes. You can support incremental updates, the vast majority of IoT companies haven’t put their time and effort into their device. ”

“ They are one part of the minimum-security standard for remote controlled systems. ”

“ They are essential in any small or large system. ”

“ It is a must have. It is part of the security approach and strategy. ”

“ Updates are a security requirement for most devices and this established concept is the foundation for modern flexible connectivity today. ”

“ That is an essential requirement to keep all elements of the networks healthy and secure. ”

“ In depends a lot on the application, some applications will need more updates on security design that others. ”

“ AI and ML are just more sophisticated tools that allow what a data scientist can traditionally do off-line maybe rather slowly or very quickly, so the speed of achieving a decision is dramatically improved with AI and ML. ”

“ Yes AI, ML are interesting to improve services, anticipate any possible issue to be detected in advance. ”

“ For sure it will come, but we don’t need it immediately. ”

“ AI can greatly assist in the planning and running of those systems. Many clients value optimised systems to lower operational costs and limit the environmental impact. ”

“ AI is at the heart of the solution. The output of the different spectra from our cameras is constantly monitored by AI. ”

“ It is needed to run systems that act quickly and highlight abnormalities to decision makers. ”

“ Complex systems with many participating parties need some level of AI for basic functions and access alone. AI can help greatly to communicate the outcomes efficiently and to make things interactive. It plays a big part in improving the services and capturing the client’s experience. ”

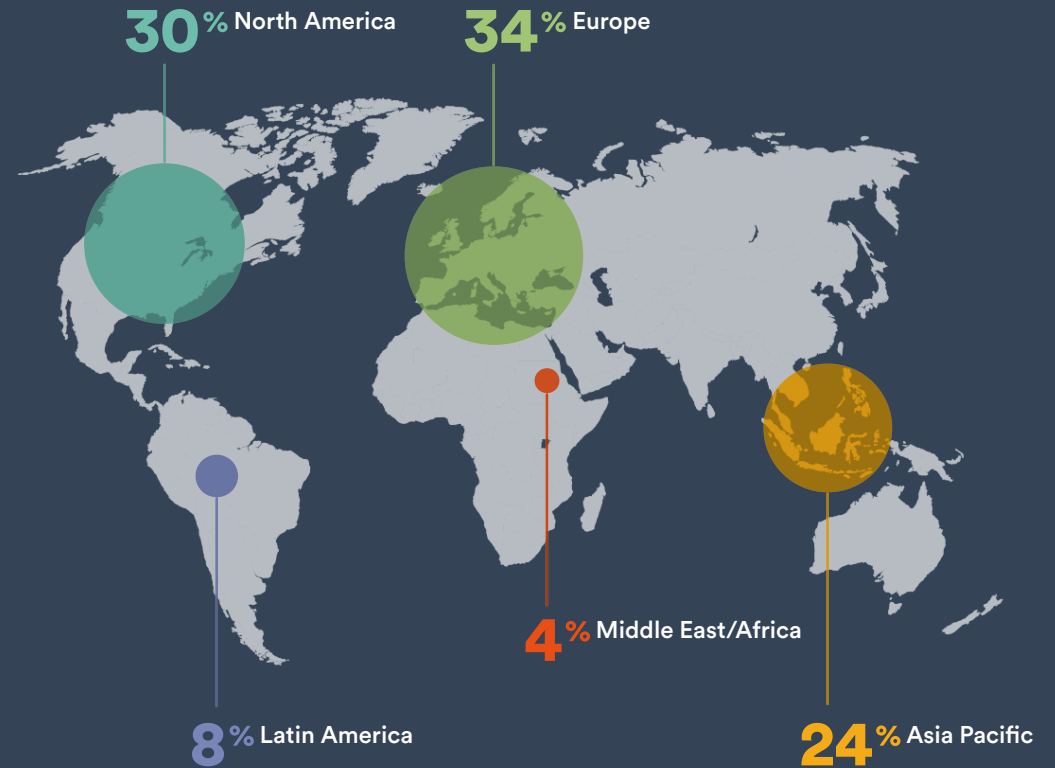
Industry Expert Survey

This section analyses the results of an online survey conducted for this report. The main objective was to study the use of wide area IoT connectivity and associated services

Your Business Unit

Figure 3.1 The number of respondents in Europe at 34% was slightly more than North America at 30%, – with slightly fewer in Asia Pacific (24%) and fewer in Latin America and Middle East (8% and 4% respectively).

Figure 3.1 What region is your business unit based in?



Your Business Unit (cont...)

Figure 3.2 While in practice 98% of companies have less than 100 staff, for this survey only 61% had under 100 staff in their business units; 20% had between 100 and 1000 staff with 7.5% up to 5000 staff; A much larger than normal representation of 11% had over 5000 staff in their dedicated business unit.

Figure 3.3 About one third were C Level and Managerial: director/VP nearly 20%; with only 13% Other levels.

Figure 3.4 46% of the respondents saw their role as IoT solution providers. Equal proportions (ca 11%) of respondents gave their primary roles in relation to IoT as enterprise users, product makers, service providers. A small minority described themselves as researchers and unspecified. For this particular survey, the larger%age of solution providers was a primary objective as they tend to have a clearer view of the overall market

Figure 3.2 How many staff are employed by your business unit?



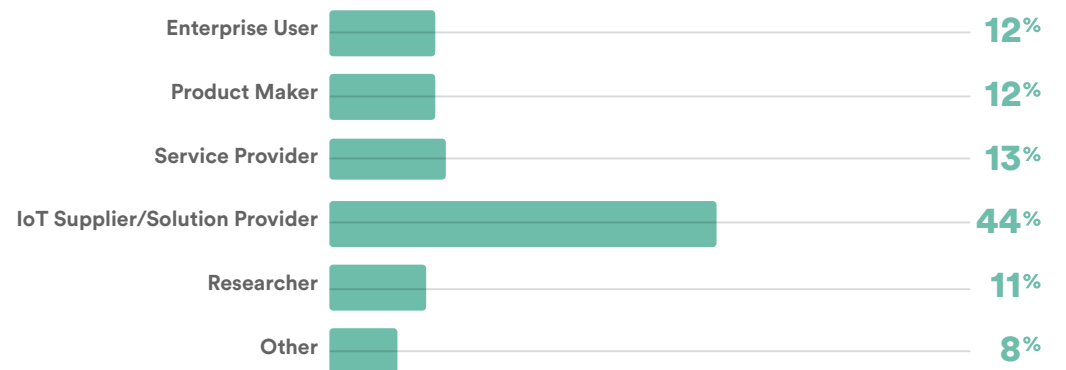
- 61%** Less Than 100 Employees
- 20%** 100 – 1000 Employees
- 8%** 1000 – 5000 Employees
- 11%** Over 5000 Employees

Figure 3.3 What is the organisational level of your position?



- 35%** C-Level
- 18%** VP, Director
- 34%** Manager
- 13%** Other

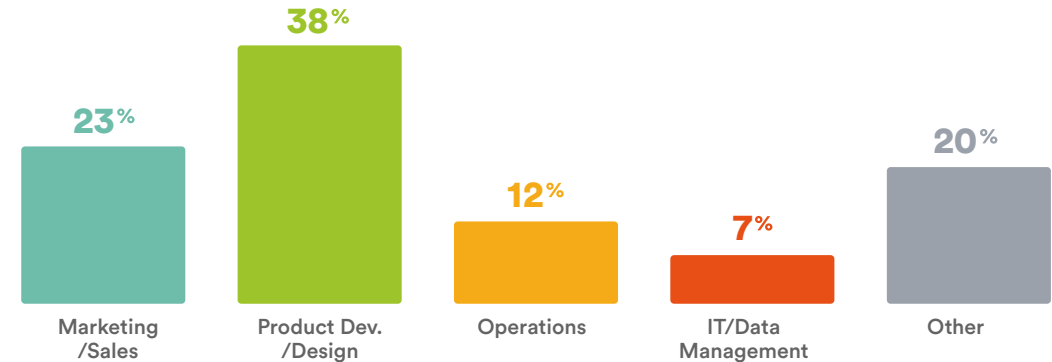
Figure 3.4 What is the primary role of your business unit in relation to IoT?



Your Business Unit (cont...)

Figure 3.5 A wide range of roles were noted, dominated by product development/design nearly 40%, followed by marketing 23%; operations 12%, IT data management scored least at 7%. Circa 20% of responders answered 'others'.

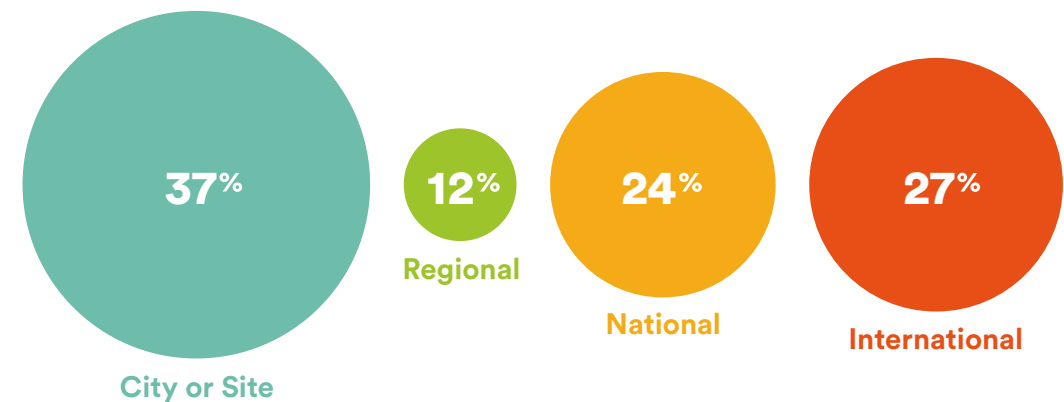
Figure 3.5 What is your principal job function?



Your Largest IoT Deployment

Figure 3.6 Deployments varied in their geographical extent; City wide deployments are the most frequent 37%; 12% of deployments were regional; significant more deployments were larger - 25% of national and international each; national and International deployments together amounted to just over 50%, more than city wide deployments. This is an important point to note, because while initial deployments tend to be small and local, large deployments tend to be national and international, introducing a new set of challenges.

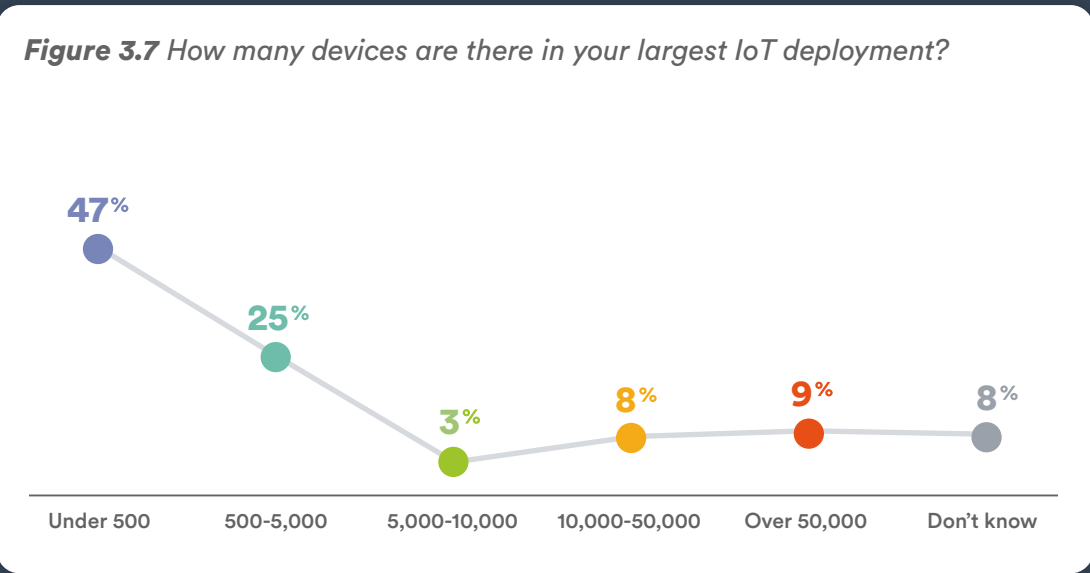
Figure 3.6 How widespread is your largest IoT deployment?



Your Largest IoT Deployment (cont...)

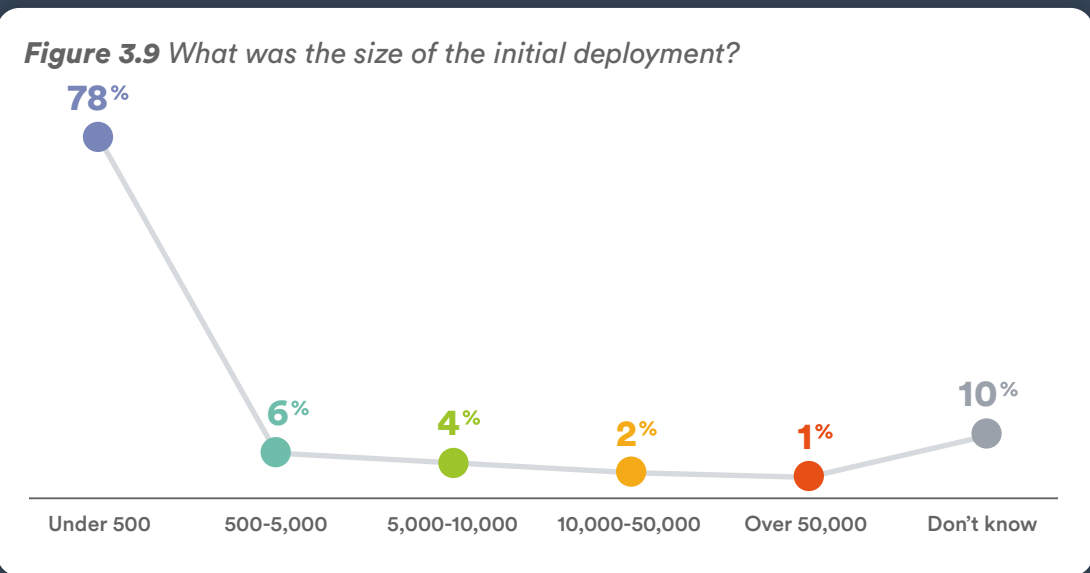
Figure 3.7 47% said under 500 devices, the largest category. 24% said 500 to 5000 devices; 11% said 5000 to 50,000 with 9% over 50,000. Hence nearly half implementations were small – under 500 devices – though a significant 20% recorded 5000 to over 50,000 devices.

Figure 3.8 A significant finding was that by far the largest proportion of 34% expected an increase of 40% over the next 3 years, with a further 40% expecting a 10-40% increase. This represents very substantial expected growth over the period, with many deployments moving from small, initial solutions to much larger ones. Beecham Research has in



fact conducted several such surveys over the last 6 months – all showing similar results in expectations for rapid growth. After demonstrating that results can be achieved with IoT projects, now implementors recognise that more insight, greater granularity and successful outcomes can be achieved if IoT networks are expanded and more data gathered. This demonstrates that IoT is now moving quickly from the early adopter to early majority phase.

Figure 3.9 Supporting this conclusion, far and away most respondents had begun with under 500 devices (77%). A very tiny number (less than 1%) began with over 50,000 devices compared with 9% today which now have over 50,000 devices (see Figure 7). While 77% reported an initial deployment of under 500 devices, 47% said that this was the size of their deployment today, meaning that many implementations had grown from the start to the time of the survey.



Your Largest IoT Deployment (cont...)

Figure 3.10 Replies recorded implementations in a wide range of industries; principally in industrial/manufacturing (20%) and construction and buildings (16%); logistics, healthcare and energy together accounted for nearly 30% (ca 10% each); also cited were deployments in agriculture, smart city, transportation, point of sale and environment/public safety.

It was the low scores and replies under the ‘other’ heading that were informative; they included education sector, mining, automotive and smart home, spectrum monitoring, domestic, finance. Some respondents cited LoRaWAN deployments covering several sectors.

Details of changes for growing deployment

Figure 3.11 48% of respondents reported that substantial changes were needed, changing most elements of the solution completely. A further 45% needed to modify some elements. Only 7% of respondents thought that deployment expansion necessitated no changes. This is a particularly significant finding, as it demonstrates that moving beyond small, initial deployments almost always requires substantial change. A previous survey by Beecham Research found that growing solutions beyond the Proof of Concept phase often led to project failures. This is because while the PoC may show the value of collecting certain data, it is usually not engineered in any way for volume and most often the solution needs a complete change to scale successfully.

Figure 3.10 How many devices are there in your largest IoT deployment?

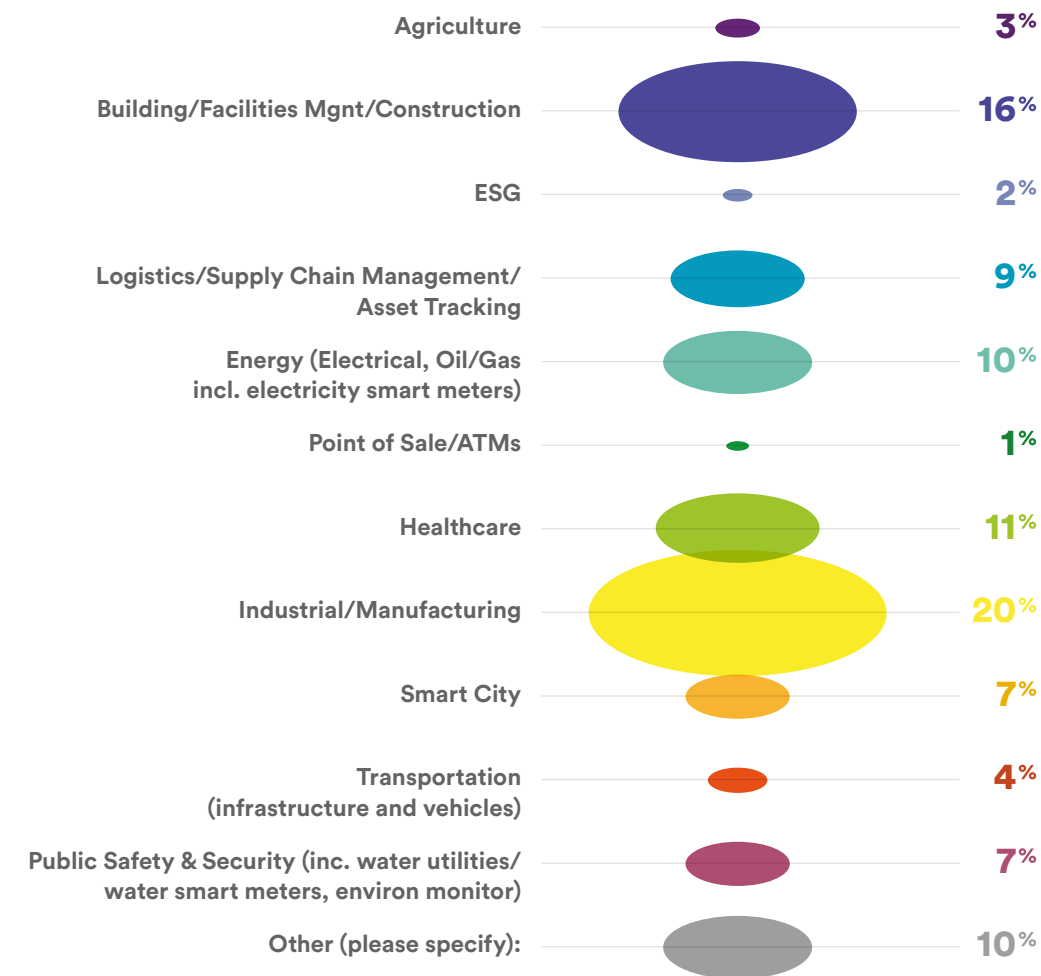
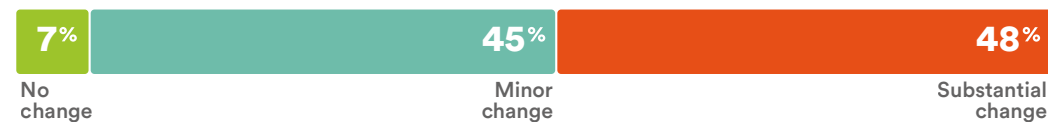


Figure 3.11 To what extent have you had to change your IoT solution to grow it to a larger deployment?



Details of changes for growing deployment (cont...)

Question 3.12 *Please briefly describe these changes for handling larger deployments*

A very interesting sequel to **Q11**. Some examples were proffered under the headings blow:

Changes right through the deployment:

Many things must be changed for larger deployments like currency, language, changes to pricing and pricing models, new telecommunications requirements, licensing and certification, patents and trademarks, shipping and logistics, security and infrastructure, onboarding and training. Standardization, Cybersecurity, Connectivity, Upgrades to sensors, Gateways, and Analytics software. Building a platform to onboard the solutions and end to end lifecycle management. Additional functionality, supporting cyber security and diagnostics during deployment stage, had to be added. Scaling from a proof of concept environment to a production environment with a different vendor selected and component change. Staffing and infrastructure. Need to build complete backend solution from data transit in the cloud to storage and dashboard. Automated deployment and commission. Building an OT network from scratch including new fibre backbone. Infrastructure, process and people change management. Enhanced security, Increased data handling, Improved reporting. More emphasis on Cloud connectivity, cloud provider agnostic, redundancy, security, compute and storage resources.

Making things faster

Increase the scaling capability of the software to handle more messages per minute. Enhanced memory and faster processor. Large number of sensors, actuators gateways databases in cloud etc are needed to make it very large. Device Management of cellular connectivity based IIOT devices.

Software Changes

Building platform to onboard the solutions and end to end lifecycle management

Changing wireless architectures

We have had to deploy a wireless antenna that receives all frequencies to handle a broad spectrum of clients using different frequencies for their IOT applications. We have patented technology for the transmission of wireless frequencies. We have developed an antenna that is not in the marketplace on a broad basis but will grow over time

Business model deployment approach?

B2B to B2C

Improved governance

More enterprise level governance, adapting for different deployment patterns at site with different infrastructure. Introducing a platform for End to end lifecycle monitoring. More enterprise level governance, adapting for different deployment patterns at site with different infrastructure. Better administration of large-scale deployments - copying data, templates etc. Focus change from business to make it work overtime and ensure the data is collected trusted and well used

IoT Connectivity

Figure 3.13 While cellular connectivity was noted by 42% of respondents as their leading technology followed by WiFi at 33%, what was most significant was the LoRaWAN score at 24%. This is significant because, while cellular and Wi-Fi have been used for decades in M2M and IoT solutions, the first LoRaWAN specification was only published in January 2015. This indicates a substantial growth of LoRaWAN to date. The anticipated high growth in Satellite over the next 5 years (40% pa+) does not yet feature in this result.

Figure 3.14 High security deemed very important by 71%, important 29%: a total of 100% of respondents assigned some degree of importance. Overall simplicity also scored highly, with 63% very important. Only 2% deemed this not important. Low cost always scores highly, so it is interesting that it comes lower than security and need for simplicity. Remote update for ongoing maintenance also had a higher 'very important' score than low cost at 55%. This reflects the growing recognition that remote update is essential for managing large populations of connected devices. Low power applies to some but not all IoT solutions, with 46% considering it to be very important and a further 40% considering it to be important. Large support ecosystem was considered very important by 40%, so below all the previous parameters. This will no doubt be seen as more significant as the number of large deployments increases. International use was considered very important by 34%, which reflects the fact that many IoT solutions are still local, or national. This will certainly cross over and become increasingly important as more solutions operate internationally.

Comments

"I would give priority to security of connectivity and communication."

"Users usually would like to have a "simple" system that they can manage with comfort."

Figure 3.13 Which of the following connectivity technologies will you use the most for your large scale IoT deployments?

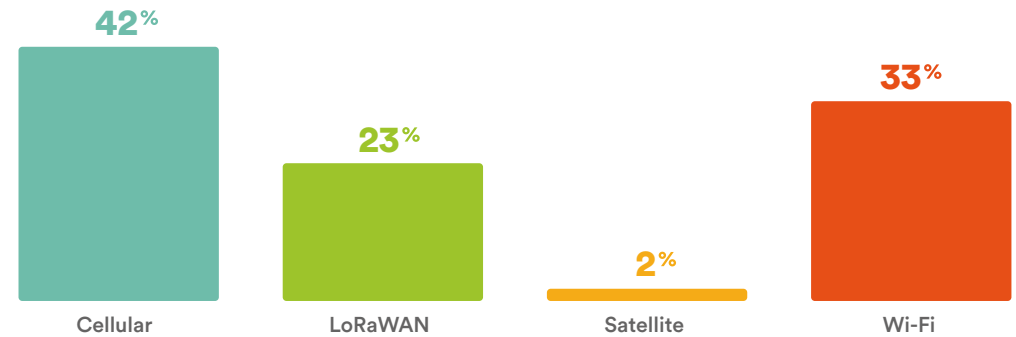
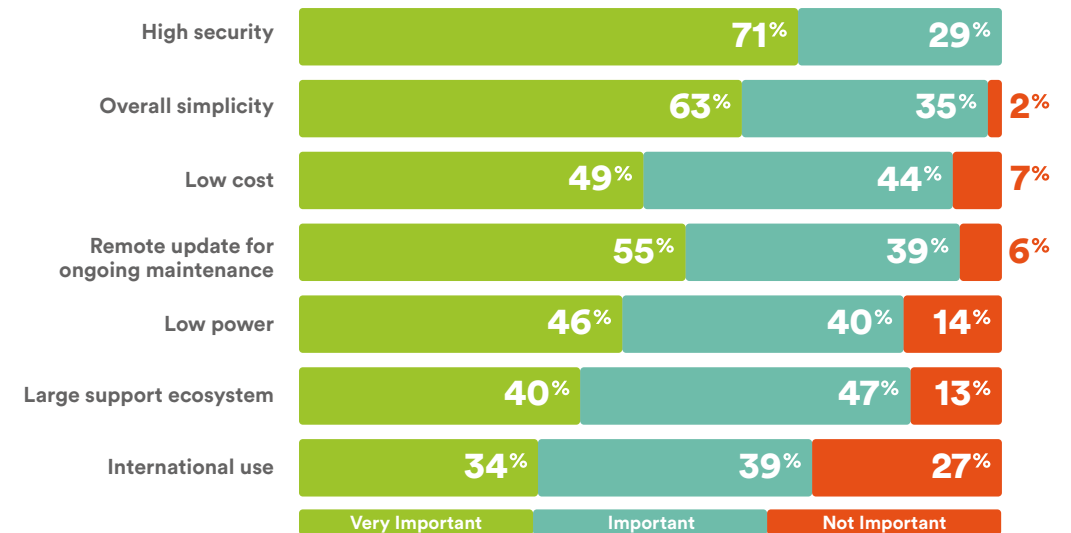


Figure 3.14 How important do you consider the following to be for choosing this connectivity technology?



IoT Connectivity (cont...)

“We designed our system to be secure and easy to use from the original design concept, so we haven’t had to change anything as we have grown to be large scale.”

“We need solutions to be simple at use to reduce the support cost... main issue we see is coverage vs cost of it.”

“Our OS solution is connectivity agnostic - WiFi, Bluetooth, LoRa, 802.15.4 (Zigbee, Thread, Matter), Cellular or custom.”

“As you scale you get diverse ecosystems, people country and need to be flexible with what is existing.”

Use of AI/Machine Learning

Figure 3.15 It is significant that the highest score for ‘very important’ was gained for detecting and handling faults, at 61%. Use of AI/ML is usually viewed as most important for data management and processing, which was second highest at 55%. This is a recognition that AI/ML has a major part to play in the management of large deployments. It was also seen as very important for detecting and handling security breaches, at 48%, which is also consistent with this.

Figure 3.16 A further finding from an earlier survey is also significant to take into account. The aim of this question was to establish how far respondent business units have progressed in implementing IoT solutions. It is interesting to note that remote monitoring and control in real time scored higher than tracking of moveable assets and remote monitoring (non-real time). Cross referencing revealed that most of those involved in real time monitoring were IoT Suppliers and Solution Providers, with Enterprise Users and Product Makers more likely to be tracking moveable assets or non-real time remote monitoring. This move towards real time monitoring and control is happening at the same time as IoT deployments are getting larger.

Figure 3.15 How important do you expect AI/Machine Learning to be for the following activities within the next 3 years?

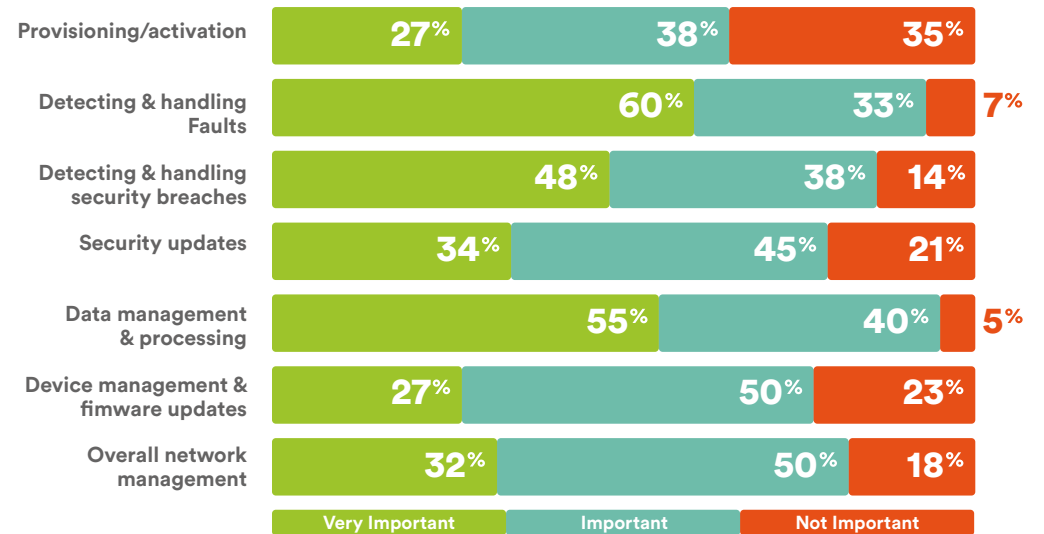
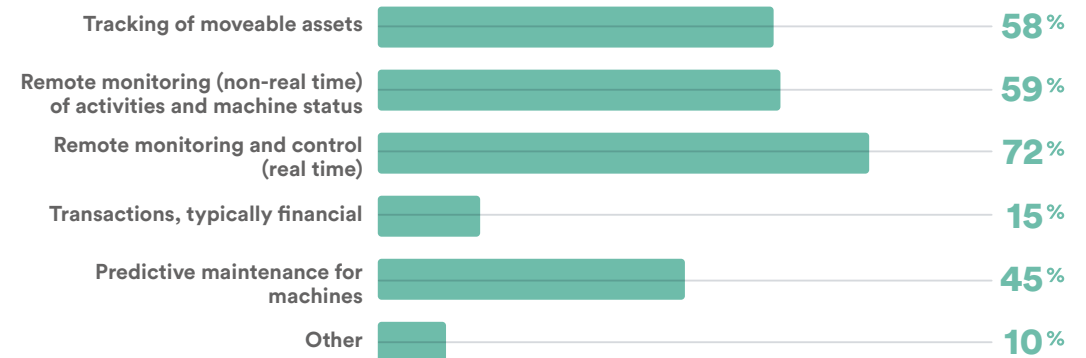


Figure 3.16 What types of IoT applications is your business currently using or expecting to use within the next 24 months?



Market Analysis

The findings from Beecham Research's interviews and online survey regarding Mass IoT Deployment are supplemented by further market analysis as follows.

For several years now, the media have abounded with forecasts for the number of connected IoT devices. For example:

According to the report 'IoT Global Forecast & Analysis 2015-2025' from Machina Research, there will be 27 billion IoT connections in 2025.

Today (2022) there are 8.6 billion IoT connections, according to ABI Research. By 2026, that number will nearly triple to 23.6 billion and securing these will involve substantial investment.

The GSMA predicts that by 2025, there will be 25 billion IoT devices.

All of these forecasts predict some 25 billion connected devices by the mid 2020s, give or take a couple of billion. They concern all types of connection – see Survey – including LoRaWAN, WiFi and satellite. Figure 3.13 of the survey showed that, for the respondent sample, cellular connections formed 42% of the connectivity technologies used for large scale IoT.

Another survey from Berg Insight stated that the number of global cellular Internet of Things (IoT) connections grew by 22% to reach 2.1 billion in 2021-2022; it predicts 4.3 billion IoT devices will be connected to cellular networks worldwide by 2026. Annual shipments of cellular IoT modules increased by 39% in 2021 to reach 428 million units. Connections grew across all the major markets of China, Europe and North America during 2021 as the world recovered from the Covid-19 pandemic.

Inevitably, such large forecasts imply that there will be very large single IoT deployments over the next few years.



Opinions from Analysts

The question is, what applications will all these devices support? What business and market sectors will gain greater insights into their operations from all these connected devices?

IoT projects are now mainstream, in that they now exist in all market sectors (see Sector chart in Section 2) and have been shown to bring benefits. Now therefore the time has come to expand these projects from proof of concept to large scale deployments. At lower costs, more sensors will be deployed, providing more data across a wider range of use cases; early results show that this is not straightforward (see Section 3 interviews)

This question is echoed by a view from Marina Ruggieri, IEEE Fellow and professor of telecommunications engineering at the University of Roma. In an article from Information Age October 2029, entitled, “How do you solve a problem like mass IoT connectivity?” she explains:

“For this sustainable future led by the IoT to take root, mass connectivity must be enabled; the major challenges that network designers and developers will be experiencing in the near/medium term could also become very effective enablers for the IoT mass connectivity.”
“Network ‘softwarisation’ is key to cope with the sustainability, privacy, security and interoperability concerns related to IoT connectivity.

Another enabler in the medium term would be a suitable role of robots in the network functions and the cooperative environment that humans and robots are going to establish therein. It sounds like science fiction, but that future is much closer than we expect...

However Before tackling the problem of IoT connectivity, it’s important to understand what the mass IoT market will be composed of? Will the IoT market largely be made of industrial or consumer connections, or both?

Today, it is true that industrial connections compose the majority of the IoT market: industrial IoT. Internet connected devices that can help deliver real-time information on individual machines and the collective. Mainly, this is to improve the product lifecycle management (PLM) of the equipment and reduce dreaded downtime. But, it is not just on the factory floor where the IoT market will infiltrate. IoT could improve the quality of people’s everyday life, particularly in those domains where the future of human beings looks more challenging. IoT could, then, become a great opportunity to align mass market with the best interest of a sustainable future.”

What technologies will be best suited to large scale future rollouts?

Various commentators have ideas as to what wireless technologies will be best suited to future expanded IoT systems. Below is a view from the LoRa Alliance. In an article entitled “What is the net environmental impact of dirt-cheap massive-scale IoT?” published in Enterprise IoT Insights Feb 2022, Derek Wallace, vice president of marketing at the LoRa Alliance in charge of the non-cellular LoRaWAN standard, explains:

“At lower costs, more sensors will be deployed, providing more data across a wider range of use cases. Lower-cost sensors will create new use cases and enable massive scaling of many existing ones. Massive IoT has enormous potential to positively impact the environment: the number of green use cases is staggering, including environmental monitoring, water conservation and food production.

The whole point with new(ish) LPWA solutions, of course, is they are geared to last for ages; up to 10 years in the case of LoRaWAN. But solutions must be tailored right. It is important to plan and actively manage IoT deployments to achieve optimal results with minimal cost and impacts. The industry must ensure massive IoT is delivered in a way that is sustainable.

What does the LoRa Alliance see from its developer ecosystem, to make IoT greener-by-design? “New technologies like energy harvesting will have a profound impact once they’re used at massive scale.

Innovation is a constant and ensuring that massive IoT is sustainable is at the forefront of development activities. Our ecosystem is committed to deploying products and solutions that are fit-for-purpose, optimized for long-life, and which will continue to evolve to not only support environmental monitoring, but to minimise the impact on the environment in parallel.”

Ericsson reports on how different wireless technologies will proliferate in expanded future networks

According to the June 2022 edition of the Ericsson Mobility report, the number of IoT devices connected by NB-IoT and Cat-M technologies is expected to overtake 2G/3G connected IoT devices in 2023.

NB-IoT and Cat-M networks primarily consist of wide-area use cases involving large numbers of low-complexity, low-cost devices with long battery life and low throughput, and they continue to be rolled out around

the world. The number of IoT devices connected via 2G and 3G has been in slow decline since 2019, and NB-IoT and Cat-M technologies are the natural successors. The number of devices connected by these Massive IoT technologies increased by almost 80% and reached close to 330 million in 2021.

The number of IoT devices connected by NB-IoT and Cat-M technologies is expected to overtake 2G/3G connected IoT devices in 2023, and to overtake broadband IoT in 2027, making up 51% of all cellular IoT

connections at that time. The growth of Massive IoT technologies is enhanced by a recently added network capability that enables Massive IoT co-existence with 4G and 5G in FDD bands, via spectrum sharing.

About 124 service providers have commercially launched NB-IoT networks and 55 have launched Cat-M. These technologies complement each other, and around 40 service providers have launched both technologies.

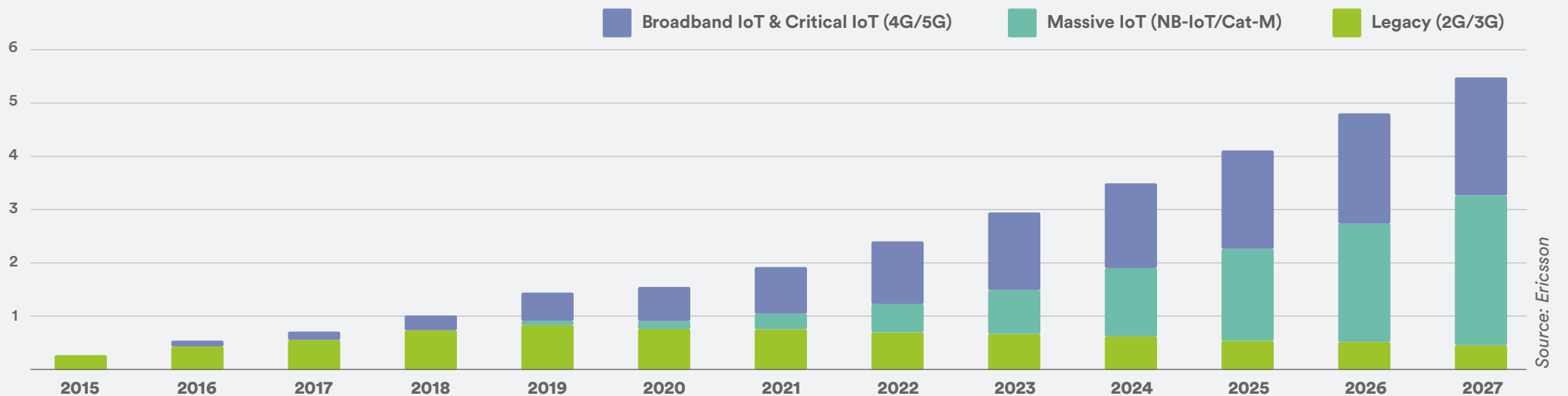
In 2021, broadband IoT (4G/5G) overtook 2G and 3G as the technology that connects the largest share of all cellular IoT connected devices, accounting for 44% of all connections. Broadband IoT mainly includes wide area use cases that require high throughput, low latency and large data volumes. By the end of 2027, 40% of cellular IoT connections will be broadband IoT, with 4G connecting the majority. As 5G New Radio (NR) is being introduced in old and new spectrum, throughput data rates will increase substantially for this segment.

Global satellite IoT subscriber base to reach 21.2 million by 2026 (Berg Insight)

According to a research report from specialist IoT analyst firm Berg Insight published in September 2022, the global satellite IoT communications market is growing at a good steady pace. Despite the impact of the COVID-19 pandemic, the global satellite IoT subscriber base grew to surpass 3.9 million in 2021. The number of satellites IoT subscribers will increase at a CAGR of 40.3% to reach 21.2 million units in 2026.

According to the analyst, only about 10% of the Earth’s surface has access to terrestrial connectivity services which leaves a massive opportunity for satellite IoT communications. Satellite connectivity provides a complement to terrestrial cellular and non-cellular networks in remote locations, especially useful for applications in agriculture, asset tracking, maritime and intermodal transportation, oil and gas industry exploration, utilities, construction and governments.

Figure 3.17 Cellular IoT connections by segment and technology (billion)



Source: Ericsson

The terrestrial technologies will grow in importance in the next five years and collaborations between satellite operators and mobile operators, as they explore new hybrid satellite-terrestrial connectivity opportunities.

Real world examples of large scale IoT projects

Below we shall present some real-world examples of implementations in progress that entail expanded IoT networks, in different market sectors.



1. Cellular Connectivity of Electric Vehicle Charging Stations is a fast-growing market, says Ericsson

In October 2022 Ericsson released a Connected EV Charging report in collaboration with EV charging provider Blue Corner. It states cellular IoT plays a central role in connecting electric vehicle charging stations – a fast-growing market driven by a global push for phasing out gas-powered vehicles.

The report explores how cellular IoT connectivity can help EV charging providers improve their charging station deployment, operations, maintenance, and service provisioning. Specifically, IoT supports the authorisation of users, payment processes, station monitoring and maintenance, and smart energy management, while also providing valuable data to improve planning and develop new customer services. Another advantage of cellular IoT connectivity is its built-in security measures to

protect data and sensitive information, creating additional value add in addition to reliable coverage no matter the location.

By implementing cellular IoT, mid-size EV charging providers can increase revenue by 40%, as a result of interoperability revenue share. As consumers, governments, and the automotive industry look toward a more sustainable and efficient alternative to fossil-fuelled vehicles, EV charging providers recognize a business growth opportunity.

The report demonstrates the value of cellular IoT connectivity in keeping up with the fast-paced growth of EV charging networks. Through cellular IoT, EV charging companies can manage complex stakeholder ecosystems, from drivers to hardware providers by enhancing network functionalities, while simultaneously building a solid, future-proof foundation to scale their business.



2. Medical Electronics market forecast to grow rapidly (Market&Markets)

The global medical electronics market is expected to reach USD 8.8 billion by 2026 from USD 6.3 billion in 2021, at a CAGR of 6.9% during 2021-2026 period according to Market&Markets. The forecast includes components e.g. displays, and applications e.g. diagnostics.

The rapid growth of the global medical electronics market is attributed to the some of the driving factors such as the ageing population and increasing life expectancy, increasing adoption of IoT-based smart medical devices, escalating demand for portable medical devices and wearable electronics, growing use of radiation therapy in diagnosis and treatment of diseases and existing favourable healthcare reforms and financial assistance by governments for senior citizens.



3. Smart water metering rollout in India

India-wide LoRaWAN public network operator SenRa has been chosen by the India water management company Cranberry Analytics as its partner in a smart water metering project in Goa.

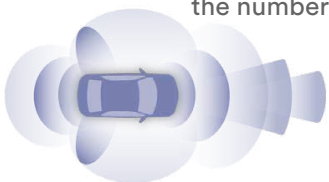
The project's initial phase will replace 3,094 consumer-grade mechanical water meters with LoRaWAN-enabled ultrasonic smart water meters. SenRa will be deploying its public network across the area to enable the streaming of the smart water meter data.

Cranberry Analytics' smart water metering solution provides a more sustainable approach to managing water supply and distribution by analysing water consumption data on a daily basis to detect anomalies in water distribution and consumption. Through correlation of that data with other data streams, it helps cities in effectively planning water distribution, mitigating water wastage (NRW), and improving consumer billing.

SenRa's commercial grade public network is currently connecting tens of thousands of smart meters in cities and industrial facilities across India.

4. The connected car market is edging towards a mass-media tipping point

A forecast published by analyst firm Omdia in October 2022 predicts the number of connected cars on the road will reach 571 million by 2025,



compared to 231 million in 2021. According to Omdia, it represents something of a tipping point because at that scale, it becomes comparable to the TV set-top-box market.

The pace of growth will accelerate further as connected cars become the norm. ABI Research predicted in April that 70% of new vehicles sold in 2028 will be connected cars. Meanwhile, Transforma Research said in June that the number of connected vehicles on the road will reach 2.5 billion in 2030.



5. Large-scale LoRaWAN® smart street lighting project launched in Montevideo (Source: IoT Business News, January 2022)

Sydney-based National Narrowband Network Company (NNNCo) has signed a contract with technology provider Wellness TechGroup, to provide IoT network coverage to 70,000 smart streetlights in Montevideo.

The project will employ NNNCo's LoRaWAN® network. NNNCo is a leading LoRaWAN® network operator with a carrier licence. It will cover 200 square kilometres and provide smart street lighting to more than 1.3 million people, improving community and road safety, and reducing carbon

emissions. This initiative will also establish an infrastructure-based network that can accommodate other smart city initiatives.

The partners will replace Montevideo's existing lighting system with LED technology and roll out an interoperable remote management system, which is designed to reduce carbon emissions by 31,500 tonnes of CO₂ per year, a decrease of approximately 80%. The project will also improve the quality of public lighting service and provide greater efficiency and operations management to the whole city.



6. Wearables and accessories market will experience continuous growth, says ABI Research.

ABI Research finds demand for wearables and accessories will experience continuous growth to 2027 despite having slowed during 2021, due to economic and geopolitical factors impacting consumer's priorities.

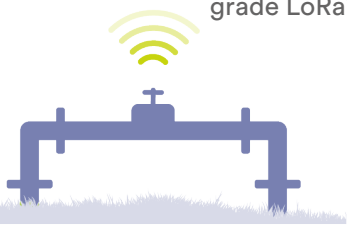
More than 300 million wearables devices were shipped by the end of

2021; more than 650 million of these devices are expected to be shipped worldwide by 2027, a CAGR of 13.2% between 2022 and 2027. This growth is foreseen to be driven mainly by two segments, namely sport, fitness and wellness trackers and smart home-enabled smartwatches. The reason behind the rise of these two segments is the continuing direct consequence of the pandemic on consumer habits.

7. Severn Trent Water partners IoT to digitally transform its water network (Report published in Information Age 21 Feb 22)

Severn Trent Water is looking to bolster its operations and reduce environmental impact through using real-time IoT data.

The project will see partners Connexin and Itron roll out a new smart water network from 2022. This will include the installation of over 150,000 Itron LoRaWAN-enabled smart water meters, along with a large-scale, carrier-grade LoRaWAN network.



These solutions will enable Severn Trent Water to effectively and remotely gather, access and analyse data from across the network in real-time. Access to real-time data on water usage, in turn, will help the regional utilities provider improve services, reduce costs for both customers and the provider, and help protect the environment.

Through this partnership, Severn Trent Water can monitor consumption more accurately to ensure customers are being charged correctly, identify leaks or burst pipes faster, and address these at the earliest point. Data capabilities such as these allow utilities companies to reduce wasted resources, through leveraging improved monitoring of how much water is exactly being used. Additionally, emission and monitor asset conditions can be monitored to ensure the network is operating effectively, which reduces repair and damage costs.

Conclusion

As these examples show, substantial growth in individual IoT deployments is expected across all sectors.

The survey results also indicate the expected high growth, as shown earlier in this section in Figure 3.8. Figures 3.7 (size of largest deployment now) versus Figure 3.9 (size of initial deployment) also indicate that growth in large deployments is already underway.

Figure 3.11 shows that 48% of respondents reported that substantial changes were needed to grow their IoT solution to a larger deployment, with a further 45% needing to modify some elements. This was a significant finding and illustrates that many initial deployments used particularly for Proof of Concept are most often not appropriate for scaling to larger deployments.

In the next Section, we explore some of the key issues in scaling IoT deployments for Mass IoT.

Enabling Mass IoT

This section explores some of the key issues and challenges in moving from small to large IoT deployments, including insights on actual deployments.

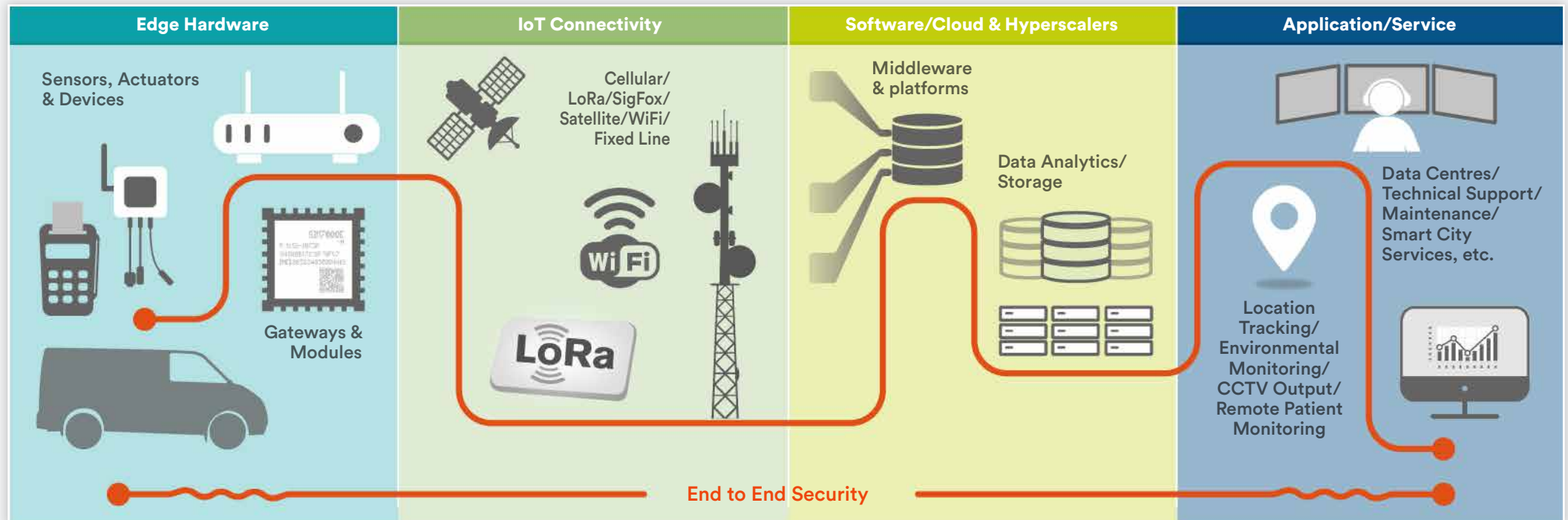
Scaling Issues, Solutions & Enabling Technologies

The IoT' business proposition is very simple. Deploy sensors and devices that generate parameter and event data. Process and analyse the data into insightful, actionable information and intelligence. Employ the intelligence in the applications and services of the corporate ecosystem. However, the enabling value chain, shown in figure 1, comprises a relatively complex mix of computing and communications technologies, which introduces a number of interrelated issues when scaling solutions to massive IoT (mIoT) levels.

These issues will impact all players in the chain: device and hardware manufacturers, systems integrators and service providers, application and software developers. In turn, the role that IoT plays in the economy will expand, both quantitatively and qualitatively.

To date IoT networks have not been massive, but real-world deployments have allowed researchers and application developers to create protocols, standards, and frameworks that helped them understand the issues that come with the management of massive deployments that are being enabled by 5G.

Figure 4.1 Typical Elements of an end-to-end IoT value chain



This section of the report examines the principal issues, how they are being addressed and considers the advances in operational performance that are being developed and deployed. They include:

- Scaling and securing solutions from 100s to 100,000s of devices
- Provisioning and maintaining those solutions with large numbers of devices
- Managing complex ecosystems for massive deployments
- Data sharing and interoperability
- Handling large deployments of low-cost connections
- Scaling the security mechanisms; handling security breaches
- Managing OTA updates from low data rate connections
- Fast service in the field – dealing with faults
- The role of ML and AI.

Scaling, securing and provisioning

Massive IoT is predicated on the ability to scale deployments into networks that comprise tens and even hundreds of millions of connected devices. Eventually this figure will be measured in billions. These large-scale IoT deployments will normally have a mix of new and legacy devices that use different technologies and serve multiple purposes. For example, the data aggregation role of gateways is changing. Adding intelligence allows the same hardware to do processing and analytics tasks.

This development reflects the way IoT has evolved and it will impact on the scope of the deployment. Interoperability is therefore key. Each application needs a clear value proposition and all applications need to be integrated on platforms that can scale when required, for example, extend the deployment from the initial PoC stage and continue to ensure efficient operation.

Once a deployment starts to scale it will be impossible to perform even the most basic operations such as onboarding, configuration, security patches, and maintenance manually. When there are numerous devices with multiple sensors and actuators there will be a massive increase in traffic, the content of which will change every second of every day. Therefore a management platform that can accommodate this demanding requirement is required.

It is worth noting that providing service for devices in the field is challenging, but IoT can monitor the performance of connected equipment in real time. This enables issues to be resolved proactively, before a service issue occurs, thereby minimising delays in operations and unplanned downtime.

It is clear that organisations must design for growth from the outset, with the flexibility to rapidly scale up if the service is successful. Here, visibility and control of the entire device estate is essential and the solutions require the highest possible operational efficiency and reliability.

For more than three decades the traditional SIM card (UICC) has been used as the trusted, tamper-proof element for secure authentication of users and mobile devices to cellular networks. Right now eSIM technology provides a unified approach to global, future-proofed connectivity that can help organisations scale and secure mIoT deployments. eSIMs and the newer iSIMs allow multiple connection profiles per device, thereby providing easier switching between networks plus enhanced security.

When it comes to massive deployments of IoT devices, eSIM is a simpler approach to device provisioning and future-proofed connectivity. If a device's lifetime is 10 years, a lot can change in a decade when it comes to connectivity. Legacy networks sunset changes can happen, or an organization might choose to change carriers or networks within the device's lifetime. In addition, OTA provisioning enables zero-touch provisioning at the touch of a button. This reduces logistics to a simple, single-SKU approach that reduces time to market and reduces costs.



Cumulocity IoT Device Management Enterprise-Grade Solution

Device Connectivity & Management are critical first-level capabilities for an IoT platform, providing fast, model-less device integration. One of the major hurdles for a solution to overcome is the low degree of standardization in the market, particularly in asset-intensive industries.

The major challenge for large-scale IoT deployments is identifying a platform with sufficient device management capabilities. Solutions that can connect, manage, update and automate analysis for a few dozen devices can not necessarily function when connected to tens of thousands or more. So how can you be sure a platform meets enterprise-grade needs?

Cumulocity IoT is an enterprise grade solution with reliable, and robust features that support your scaling needs, including support for multitenancy, white-labelling & internationalization.

The first key differentiator of Cumulocity IoT is our Device Management Solution. We offer a rich set of Comprehensive & Self-Service capabilities that provide an end-2-end solution and pre-defined, proven IoT lifecycle management processes. These solutions allow customers to reduce Total Cost of Ownership (TCO) and shortens the time-to-value of deployments.

The second key differentiator is the device vendor & protocol agnostic approach we take. Cumulocity IoT provides consolidated lifecycle management processes for heterogeneous IoT endpoints without device vendor lock-in. We support 100's of devices (including gateways) and many different protocols (MQTT, REST, LWM2M, Proprietary, LoRa, Sigfox, NB-IoT, etc...). The simple UI makes it easy to add new device types and SDKs to integrate new protocols.

Finally, we enable easy automation of operational procedures and integration with 3rd party systems. Our Analytics Builder allows users to automate maintenance tasks. Users can also leverage real-time alarm anomaly detection and correlation with Cumulocity IoT Machine Learning.

Figure 4.2 Providing enterprises with the capabilities they need to manage their large-scale heterogenous global IoT device estates

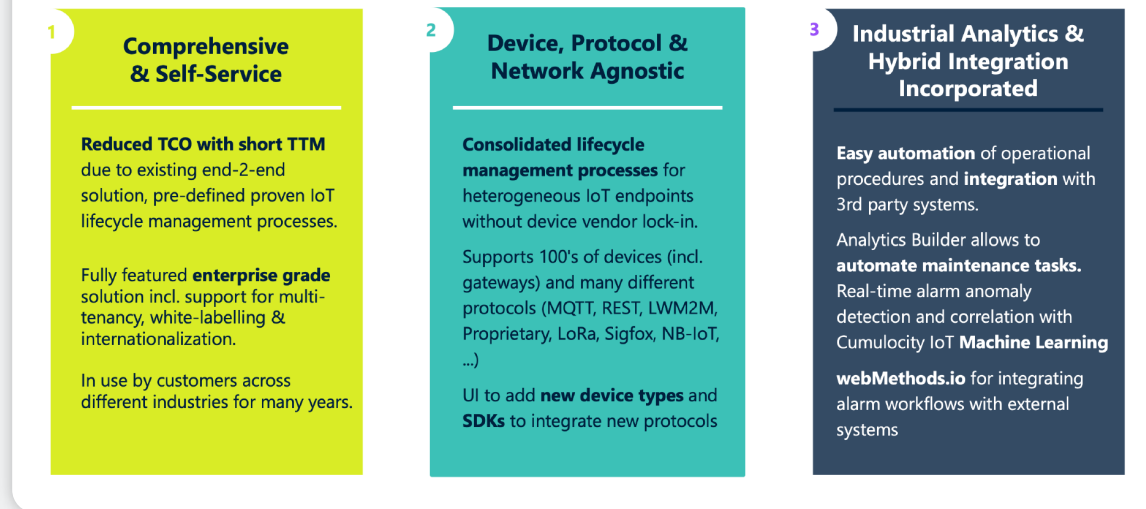
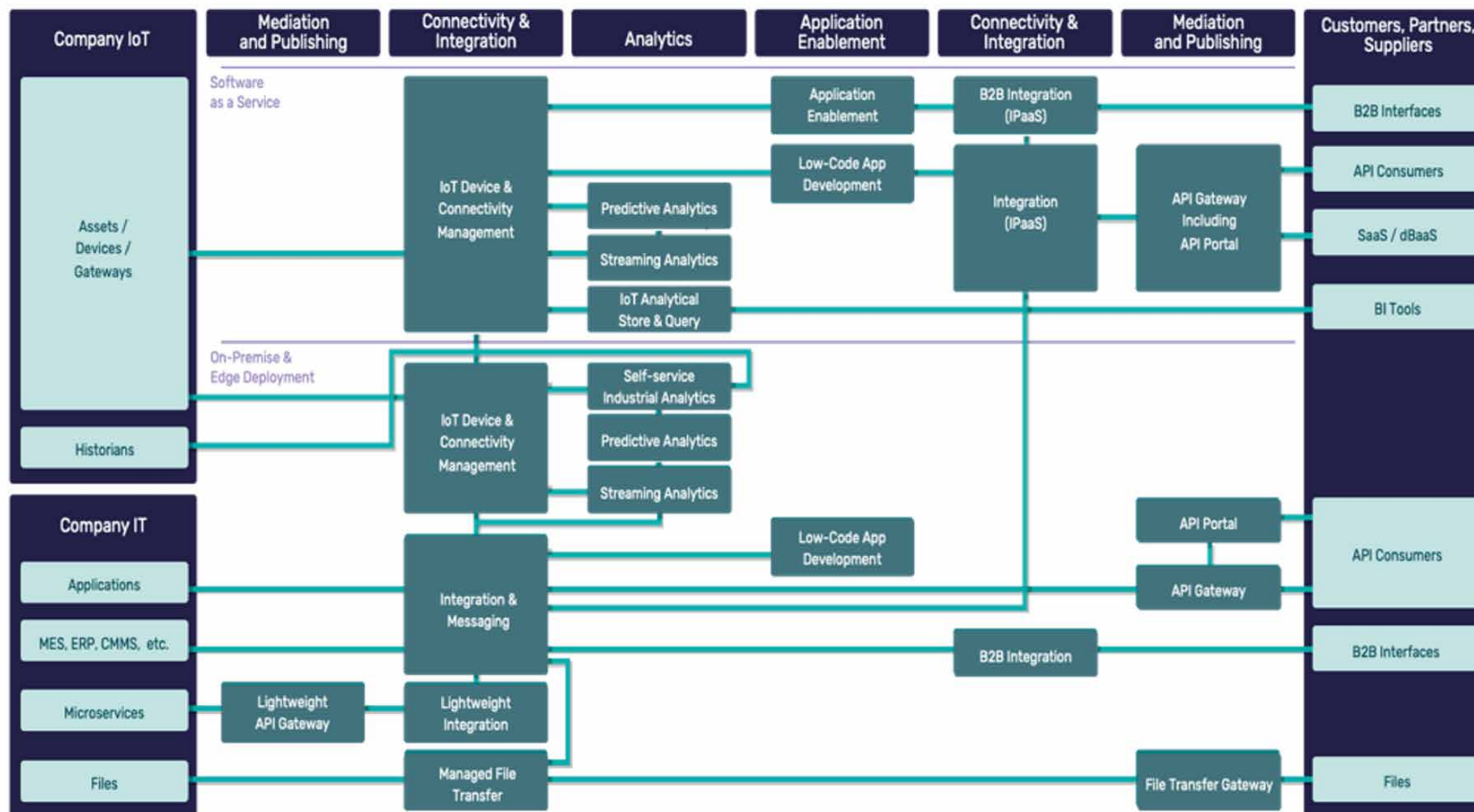


Figure 4.3 IIoT Reference Architecture. Holistic view: from Devices to meaningful insights and actions in OT systems and 3rd party applications



Interactive version:
IIoT Reference Architecture

Benefits

- End-to-end data flow from devices and OT assets over analytics and IT integration to applications
- Starting point for customers to derive their IIoT enterprise architecture
- Not Software AG centric

Impact for the customer

- Understand multi-cloud, hybrid and distributed deployments
- Understand integration points with hyperscalers, existing IT and OT and partners
- Understand interplay or real-time and batch analytics with underlying data management



Succeed with IoT today

Meet Cumulocity IoT QuickStart

What if you could quickly prove ROI from the Internet of Things? Now you can. Cumulocity IoT QuickStart is a consultant-led service that takes you through four critical phases of your IoT project:



Start & scope

including a discovery workshop to explore your IoT goals



Architect & design

with a deep-dive workshop looking at "as-is" and "to-be" architectures



Develop & test

with continuous support from Software AG consultants



Review & extend

including measuring outcomes against success criteria

Together, let's make your IoT project a success

www.softwareag.com/iot



Managing Complex Ecosystems

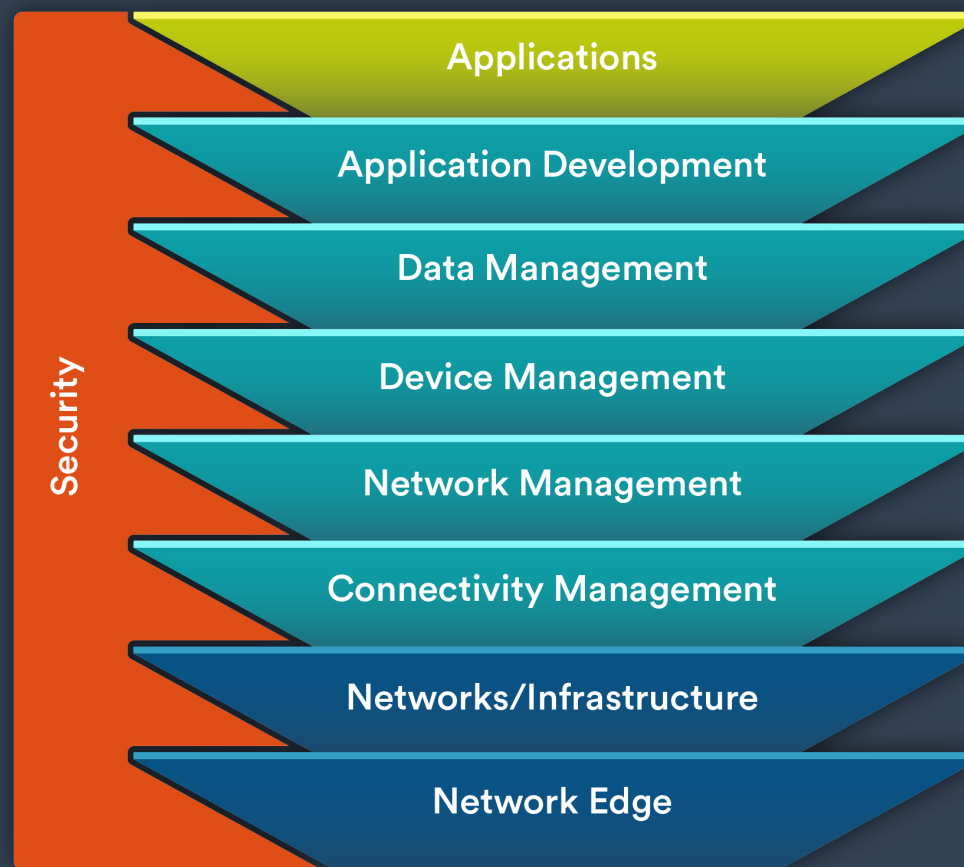
Large scale IoT deployments, with its mix of new and legacy devices and different technologies cannot be implemented by a single supplier. The demanding requirements of these solutions has resulted in a significant expansion of IoT ecosystems, which have to be managed and secured as an integral component. eSIM technology deployed on third-party devices enables secure connectivity and flexible management platforms (see next section) facilitate the addition of new partners and new functionality.

Data Management and Data Sharing

As shown in figure 2, small- and medium-sized deployments employ individual platforms for connectivity, network, device and data management. However, large scale IoT deployments will normally employ different new and legacy devices that use different technologies and serve multiple purposes. Therefore data management in mIoT deployments has evolved to meet this new requirement; it recognises that better collaboration and processes are needed, e.g. the ability to cover the entire lifecycle of the data that is acquired and used. It has become a new discipline, one that will play a key role in big data analytics, machine learning, and artificial intelligence. Data management is anything but simple in a world of ever-increasing data volumes and the proliferation of types of data and data sources.

In this environment interoperability is a key requirement and individual solutions need to be integrated on platforms that can scale and handle large device deployments efficiently. This is why there is growing interest in data sharing technology and data sharing platforms. Until recently the term 'data sharing' had been mainly used in the academic context of scientific research, but the exchange and sharing of data is key for innovation and transformation at scale. Data sharing ensures a faster evolution towards digital business and it enables applications that create far more value for the initiators, participants, and target groups.

Figure 4.4 | This set of platforms enable the management of today's IoT solutions, but mIoT and the need to share data raises the bar.



A recent survey of the data-sharing trend by Forrester Research found that more than 70% of global data and analytics decision-makers are expanding their ability to use external data, and another 17% plan to do so within the next 12 months. Gartner has indicated that data and analytics leaders who share data externally generate three times more measurable economic benefit than those who do not, hence the expanded role of ecosystems and their complexity. The company predicts that by 2023, organisations that promote data sharing will outperform their peers on most business value metrics. At the same time, Gartner points out that less than 5% of data-sharing programs will correctly identify trusted data and locate trusted data sources.

Security Concerns

The number of devices connected to IP networks will be more than three times the global population by 2023. This equates to 29.3 billion networked devices by 2023, up from 18.4 billion in 2018. (Cisco annual forecast.) This is significant because of the increased cybersecurity risk, i.e. more devices in more dispersed locations and the fact that in edge computing data and data processing are exposed to the outside world. Regular network security architectures focus on enterprise data centres but this model is no longer suitable for the dynamic requirements of massive IoT deployments.

It is no longer a question of whether an organisation will be attacked, but when. Unfortunately, many companies still rely on legacy point product solutions, which are inadequate. They cannot detect and respond to today's advanced attack strategies. Moreover, there is a cybersecurity skills shortage. Relying on manual threat analysis and detection, as well as security-as-you-go strategies, cannot keep pace with the advanced capabilities of today's cybercriminals.

Zero Trust

Zero Trust is basically a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. It is a conceptual model and an associated set of mechanisms that provide security controls. These security controls do not depend solely on traditional network controls or network boundaries. It requires users, devices, and systems to prove their trustworthiness, and it enforces fine-grained, identity-based rules that govern access to applications, data, and other assets.

In a nutshell, zero trust is security by design. It has identity and cryptographic keys built into a device's hardware and contained in a secure boot environment. Typically, it is built into highly integrated chipsets and is therefore not accessible. Chip makers combine trusted hardware such as a processing engine, crypto accelerators, fuses, private storage and random number generators with a small amount of trusted software to provide the trusted functions. Increasingly, chip vendors are providing a reference Root of Trust with their chips to make life easier for device manufacturers.

IoT SAFE

IoT SAFE (IoT SIM Applet For Secure End-to-End Communication) is a GSMA applet that runs on Java OS, which in turn runs on the eSIM's OS. IoT devices rely on establishing trust with a cloud to exchange data securely, but there are different proprietary security solutions and this creates fragmentation in the market. IoT SAFE addresses this issue, by delivering a repeatable, standardised, scalable solution. It effectively 'bakes' secure connectivity into the device at the point of manufacture and enables even the smallest devices to connect, authenticate and exchange trusted data immediately with the cloud.

IoT SAFE specifications deliver scalable "security by design". They meet the scalability requirements of an IoT security framework by utilising standardised and field-proven SIM and eSIM technology.



psacertified™

Implementing Root of Trust in Silicon

As our health, homes, workplaces, and urban environments are all being transformed by new technologies, we must ensure every connected device, and the data they generate, can be trusted. Security must be integral to devices, and this requires an ecosystem-based approach to build in security.

A Root of Trust (RoT) is not a new concept, but it's something that may be new to innovators building products for the IoT. It creates the foundation for Internet of Things (IoT) security and creates a space where all trusted operations can happen securely, essentially forming the 'security gate' for every trusted function within a device.

It is implemented into the silicon as a combination of trusted hardware such as crypto accelerators, private storage and random number generators, and trusted software, to provide the security functions. A software interface is then implemented to hide the complexities so that IoT device developers can easily leverage these functions.

One of the most important functions of the RoT is enabling secure boot. The RoT ensures the software on the device is authentic and has not been tampered with before the device software and other system software can run. As Mike Dow, Senior Product Manager for IoT security, from PSA Certified Level 3 partner Silicon Labs, explains secure boot: 'ensures when the processor boots that the code is authentic and hasn't been modified- all things stem from that.'

A RoT also maintains confidentiality - it keeps private crypto keys safe by protecting them with hardware mechanisms and separating them from the system software. The RoT's secure storage and crypto functions also support authentication of the device, verify claims, and encrypt or decrypt data.

As PSA Certified was founded to make IoT security development quicker, easier, and more cost-effective, outlining and agreeing the PSA Root of Trust (PSA-RoT) was one of the first missions of the project. The PSA-RoT is an easy-to-use, on-chip RoT that the chip ecosystem align on. It has been adopted by the majority of the top silicon vendors at the different PSA Certified levels.

Figure 4.5 PSA-RoT on-chip security





System software vendors and device manufacturers can then build on the certified PSA-RoT and certify their products based on these implementations. This deepens the understanding of the RoT within the technology ecosystem and then creates a value chain based on a standardized and trusted foundation.

“Security in IoT and digital transformation solutions can’t be an afterthought and has to be an integral part of any development. Building a solid security foundation clearly relies on robust and well developed security standards like the PSA Certified and IEC 62443. PSA Root of Trust clearly is one of the core elements.

Robert Andres Chief Strategy Officer at Eurotech.

It’s not just PSA Certified that believe that the RoT adds value and trust across the whole ecosystem, as many industry leaders are also recognizing the PSA-RoT as the de facto for security. Alexa Voice Services (AVS) now require that chipsets going into devices have hardware-based security

capabilities that meet PSA Certified Level 1, or equivalent. Plus leading cyber-insurance provider Munich Re explained that ‘the defined Root of Trust protocols that talk to nuanced issues can provide confidence and an easy win for insurers’, and end market schemes ioXt and UL have both recognized the PSA-RoT as the foundation to fast-track product evaluations.

To realize the potential of digital transformation, and to trust the new data-driven services, we need best practice IoT security that is standardized and accessible. A foundational RoT, such as the PSA-RoT, implemented into the silicon and leveraged through the system software provides an easier route to certification for device manufacturers, as they can build on a pre-certified secure foundation that they, and their customers, can trust.

Figure 4.6 PSA Certified chip and component ecosystem



Edge Compute

Massive IoT deployments will generate massive amounts of data, so much that unless it's aggregated and processed into smaller volumes of information it becomes unmanageable. Moreover, if the information doesn't reach requisite destination, the result can lead to confusion and wrong conclusions. This challenge has been anticipated and addressed by edge compute.

Edge computing processes and analyses IoT data at or close to the source in near real time. Cloud computing processes and analyses IoT and related business data at a central facility. Advances in chipset technology have increased the computing resources of the compact hardware devices deployed at the edge, enabling them to function as small nodes in large intelligent networks. As well as being a cost-efficient way of processing the data, edge computing enables a clear division of “transient (non-persistent)” data that can be deleted after processing at the edge and “historic” data, which can come from multiple stakeholders, that is processed and stored in the cloud/data centre. In addition, edge computing that employs edge servers having significant a storage and computational capability enables many more decisions to be made at the local level. Therefore, since less data needs to be sent to the cloud or a data centre, solutions are easier to scale.

Edge computing requires dynamic security controls that are able to adapt to heterogeneous environments without centralised monitoring and administration. The recent emergence of IoT devices with embedded execution environments allows practitioners to deploy and execute custom

application logic directly on the device. This development can be provided by highly integrated chipsets, which are a fully featured system on a chip (SoC) that incorporates all the key components needed to quickly build fully functional IoT applications. They feature chip and device hacking-protection as well as a robust service access layer.

SASE (Secure Access Service Edge) is an emerging cybersecurity concept. Gartner coined the term in an August 2019 report. It is predicated on the fact that current network approaches and technologies do not provide the levels of security and access control digital organizations need. Gartner says SASE will transform the “legacy perimeter” into “a set of cloud-based, converged capabilities created when and where an enterprise needs them and edge computing is one of many drivers. An IoT edge computing platform is just another endpoint identity to be supported. The key difference will be the assumption that the edge computing location will have intermittent connectivity and the risk of physical attacks on the system. Thus, the SASE architecture should support offline decision making with local protection of the data. Gartner expects that, “by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.



Creating an open, resilient, secure environment for Massive IoT applications

As the adoption of Massive IoT expands both geographically and across vertical markets, it's critical to understand which technology options are best suited for specific use cases. For a great number, LoRaWAN is the answer.

Ideal use cases to operate on LoRaWAN include smart metering, flood/water management, smart lighting, smart parking, logistics and a host of other “smart” applications designed to address environmental challenges and improve daily life.

Everynet operates the largest, neutral-host, LoRaWAN national networks in the world – helping to enable these and other uses cases. Their networks are open, highly resilient and entirely server agnostic. Further, they offer carrier-grade network deployments on a robust tower infrastructure – having partnered with the largest tower companies in the world. The network also delivers a range of tools to ensure reliable message delivery, including:

- Carrier-grade network
- Entirely server agnostic
- Ultra-low-cost, no CapEX
- Open ecosystem
- Global 24/7 NOC

LoRaWAN Security: A Safe IoT Ecosystem

As the Massive IoT market expands, so too do concerns related to technology security and potential cyberattacks. Fortunately, LoRaWAN technology has been designed from the start with security in mind. It has a strong authentication process, is resistant to interferences, jammers and other threats, in addition to implementing end-to-end cryptography.

The reason for this is simple: the system, which integrates LPWAN networks, is structured to work as a low energy, low cost, easy to implement, highly scalable solution. And, since several devices are installed “in-field” for long periods of time – in some cases, for decades – network components have always been developed with a view towards security today and well into the future.

An example of this long-term use of IoT devices are public utility services, which are vital to modern societies. In India, a company has installed smart hydrometers for measuring water consumption, offering automated end-to-end mechanisms, including wireless communication, safe data transfer and real-time analyses. Similar experiences are ongoing in countries such as China, Indonesia, France, Spain, Italy, Brazil and the United States.

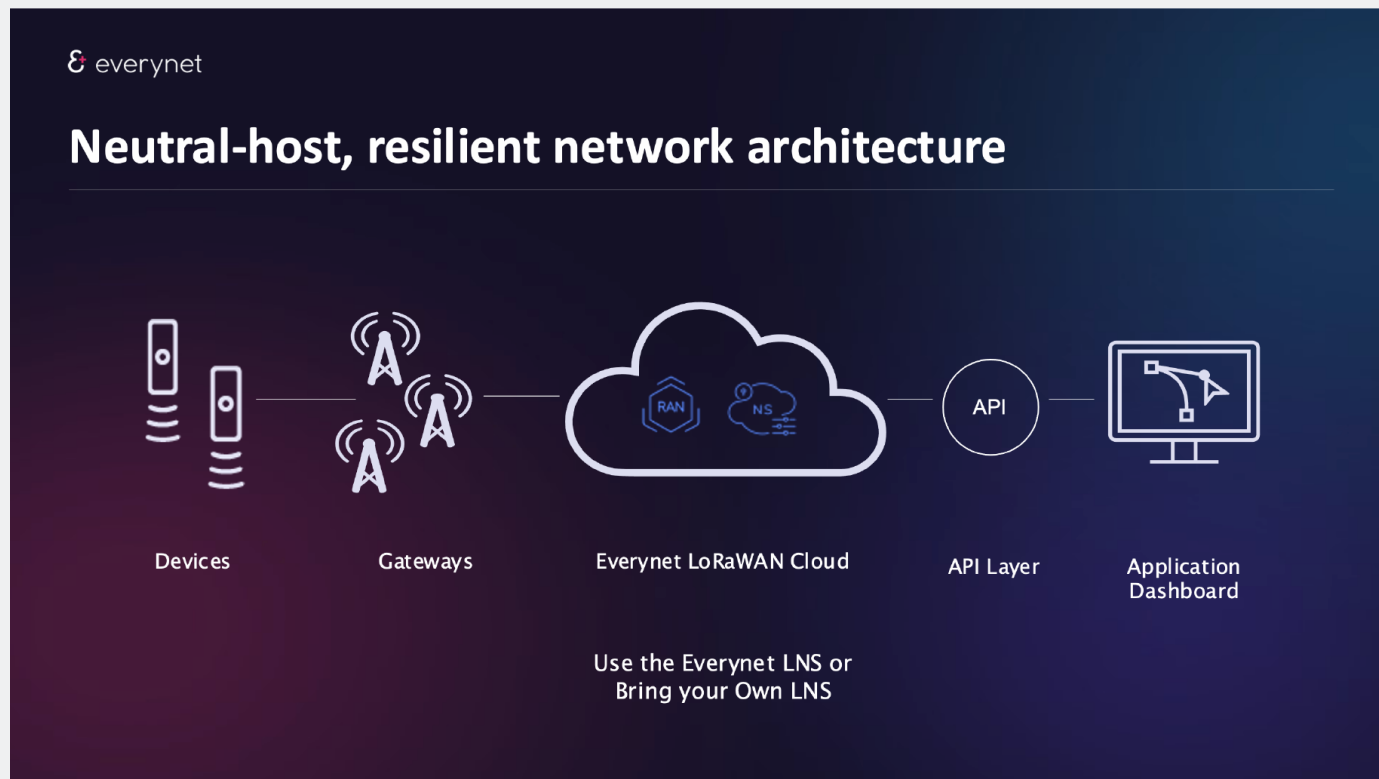


The technology is secure and includes mutual authentication, which is established between a LoRaWAN end device and the LoRaWAN network, as part of the network joining procedure, which guarantees only genuine and authorized devices will be joined into the network.

In addition, LoRaWAN MAC (Media Access Control) and application messages are authenticated at the source and go through end-to-end cryptography. These resources, when combined, prevent network traffic from being altered, captured or reproduced by cyber criminals.

“At Everynet, we focus on building a solid ecosystem that will support companies and cities around the world in their transformation journeys and contribute to the delivery of the best services,” explains Vitaly Kleban, co-founder and CTO of Everynet. “We want to play an increasingly strategic part, offering large scale IoT at ultra-low cost, with efficiency and security.”

This vision contributes to the maturing of the market as a whole and for society to benefit from the use of an innovation that has a lot to offer, creating a smart environment, with data precision and efficiency gains in several sectors.



Delivering Massive IoT

Everynet operates the largest, neutral-host, Low Power Wide Area (LPWA) LoRaWAN national networks in the world. We build and maintain carrier-grade networks enabling the delivery of Massive IoT globally.



Long-range
connectivity



Long device battery
life – up to 10 years
autonomy



Low-cost
chipsets and
networks



Small packet data
communications at
massive volume

Follow us:

 [Everynet](#)  [@EverynetIoT](#)  [Everynet Official](#)

www.everynet.com sales@everynet.com



Terrestrial Connectivity

Connectivity services are used to transport information / intelligence from the edge to a central facility, i.e. the cloud or a private data centre. The massive IoT connectivity environment employs different technologies: no single technology provides ubiquitous coverage, nor does one candidate meet the performance requirements of all vertical sectors. Regular cellular technology — 4G and 5G — provides ubiquitous terrestrial coverage and most IoT applications employ either NB-IoT or Cat-M1, which are low data rate services.

However, ABI Research estimates that by 2026 LoRa will be the leading non-cellular low power, wide area network (LPWAN) technology and it will be employed in 25% of all LPWAN network connections and more than 50% of all non-cellular LPWA network connections. Figures from IoT Analytics show LoRa connections increasing 31% year-on-year from 2020 to 2024.

LoRa (Long Range), which proves a low power, terrestrial wireless platform for IoT, is based on semiconductor technology developed by Semtech. It operates on unlicensed frequency bands. The LoRa Alliance is recognized as an International Telecommunication Union (ITU). According to Semtech LoRaWAN consumes three to five times less power than an NB-IoT networks and batteries using NB-IoT don't last as long. It is worth noting that both NB-IoT and Cat-M1 are both 4G technologies that are compatible with 5G and that inevitably they carry legacy baggage.

Satellite Connectivity

All satellites use orbits, which can be as high as thousands of kilometers above the Earth's surface (GEO Geostationary Orbit), or up to hundreds of kilometers (LEO Low Earth Orbits). Massive GEO satellites sit on the geostationary orbit, which allows them to rotate in sync with our planet.

A growing number of LEO satellite operators are launching new space constellations, with some specifically oriented towards IoT. Dual mode terminals that switch between terrestrial cellular and satellite networks have existed for several years and new combinations are on the horizon.

Low-cost, low data rate connections

Massive IoT is predicated on the deployment of low data rate and low-cost devices. There will be many more connections, with over 80% being low data rate. The only real way to manage this scenario and the huge increase in data traffic is to employ more automation, enable speedier processing and provide more traffic management capabilities.

IoT connections have traditionally been manually installed, but this is only really feasible for small numbers of connections unless there is a special team assembled, such as for smart metering projects. So, large deployments will either mean dedicated teams or connectivity embedded in hardware during manufacture. Connecting hardware during manufacture has traditionally been seen as something OEMs do if they want to add connectivity and a service to their products.

In mIoT it's significantly different. Connectivity is specified by a third-party manufacturer as part of their specification for a wide area project. OEMs therefore need to enable the cost-effective integration of connectivity into their products that third parties can employ.



Iridium CloudConnect

Iridium CloudConnect is a value-added service co-developed by Iridium and Amazon Web Services (AWS). It provides a means for IoT and messaging traffic to be transferred directly to cloud instances where customers are storing data.

Cloud-based solutions are becoming the de-facto way for businesses to deliver IT applications and services. Iridium CloudConnect makes use of Amazon's hosted cloud-computing platform, AWS. Now launched, this service enables organizations building or using IoT capabilities through AWS to extend their reach globally through the Iridium® network.

Iridium CloudConnect and AWS intersect at two fast-growing areas of technology. An early player in the cloud-hosting space, Amazon now leads this market sector. Iridium CloudConnect and AWS together provide a powerful tool for developers looking for a single communications platform to manage connected devices. It allows existing AWS customers to expand the reach of their IoT solutions with the global coverage and connectivity of the Iridium network, while continuing to use industry standard protocols and practices. Iridium customers now have access to IoT data in their AWS solution without added development efforts and impacts.

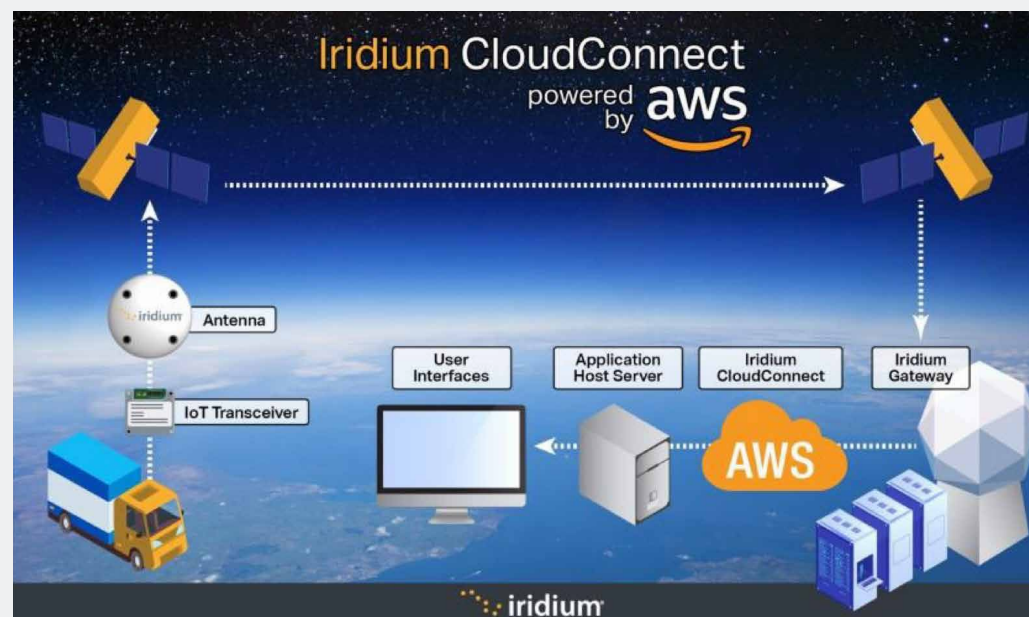
Iridium CloudConnect makes use of AWS, Amazon's hosted cloud-computing platform. It enables companies building out IoT capabilities on AWS to extend their reach globally through the Iridium® network. Iridium CloudConnect is an adapter service that transfers Short Burst Data® (SBD®) from an Iridium-based device directly to a specified cloud service, initially AWS. Iridium CloudConnect and AWS together provide a powerful tool for developers looking for a singular communications platform to manage connected devices. It also allows existing AWS customers to expand the reach of

their IoT solutions with the global coverage and connectivity of the Iridium network, while continuing to use industry standard protocols and practices. At the same time Iridium customers now have access to IoT data in their AWS solution without added development efforts and impacts.

Iridium CloudConnect supports Iridium SBD message exchange with AWS SQS. Current and future projects will expand support for AWS IoT Core services and other cloud

platforms through a variety of IaaS options, offered by utilities in CloudConnect and in AWS marketplace and developer resources.

SBD data sent from a device through the Iridium CloudConnect service remains within the closed carrier networks and dedicated private connectivity to Iridium and AWS, allowing customers to exchange messages between devices and IoT backend without using the public internet.



ML and AI

AI and ML have become mission-critical technologies. They are able to quickly analyse millions of events and identify many different types of threats, from malware exploiting zero-day vulnerabilities to identifying risky behaviour that might lead to a phishing attack or a download of malicious code. These technologies learn over time and employ histories of behaviour to build profiles on users, assets, and networks, allowing AI to detect and respond to deviations from established norms.

The enterprise IoT attack surface is massive and continuing to grow. Enterprises can have millions or even billions of time-varying signals that need to be analysed to accurately calculate risk. That is not a human-scale problem anymore. The solution comes from the development of AI and ML technologies that can learn about and analyse potential cyber threats in real-time. They employ algorithms that build models of behaviours, which are used to make predictions about cyber-attacks as new data emerges. Together, these technologies are helping companies improve their security defence by increasing the speed and accuracy of their response to an attack.

As indicated earlier, providing service for devices in the field is challenging. Research conducted by Beecham Research indicates the highest score (61%) for 'very important' was the detection and handling of faults. Use of AI/ML is usually viewed as most important for data management and processing,

which was the second highest score at 55%. This is a recognition that AI/ML has a major part to play in the management of large deployments. At 48% it was also seen as very important for detecting and handling security breaches.

In addition ML and AI play a complementary role to edge compute. Edge compute converts massive amounts of IoT data into local intelligence. Both AI and ML require vast volumes of data to train models. ML applications employ algorithms that predict outcomes based on input data and the accuracy of the prediction improves over time as the result of new input data. Narrow AI (aka weak AI) focuses on specific tasks and does them much better than humans. Narrow AI automates the boring, repetitive parts of many jobs and lets people take care of the parts that require care and attention.

It is worth noting that although organisations understand the importance and potential impact of AI, they often struggle to move from pilot to production. The top challenges that organisations must address in order to scale AI initiatives are: costs (i.e., hardware accelerators and compute resources), lack of skilled personnel, lack of machine learning operations tools and technologies, lack of adequate volume and quality of data, and trust and governance issues.

Looking Ahead

The next phase of cybersecurity growth will be driven by the need to maintain trust and ensure security throughout an expanding data ecosystem. Given the expected exponential growth in the number of edge devices where sensitive data can reside and be processed, maintaining the flow of trusted data is not a simple process.

Organizations and people will continue to be challenged by a broadening and diversifying threat landscape. Stealing sensitive data, social engineering and phishing attacks for financial gain, and holding operations to ransom are commonplace. Cybercrime is a profitable industry but at the same time cybersecurity represents a growth opportunity for vendors across all technology sectors. For example, artificial intelligence software can detect cybersecurity threats and predict attacks before they happen. It is used to examine everything that is not normal behaviour and enable a proactive approach to identify, prioritize and prevent cyber-attacks by integrating multiple data points.

As the modern threat landscape continues to expand, ML and AI are being increasingly employed as part of a security strategy. Given the speed and complexity of modern cyberthreats and the current cybersecurity skills shortage, many network security teams need the assistance of machine learning and other AI-based capabilities in order to detect, secure, and mitigate modern attacks. In addition, they need to understand which AI capabilities should be incorporated into their security stack now to maintain a consistent security posture while their network continues to evolve and expand.

However, it should come as no surprise that while organizations are adopting AI to bolster their security efforts, cybercriminals are also adopting technology like agile software development, automation, and machine learning to potentially leverage AI themselves to better identify and more quickly exploit network vulnerabilities.

Conclusions

mIoT is a means to an end. That said, it is hard to overstate the importance of that end since IoT is increasingly driving our information-centric economy. It's enabling the dissemination of that information to authorised parties in corporate ecosystems, systems that have been expanding in line with changes in the way that business is conducted. They include remote working and learning, telemedicine, and delivery services. In addition there are new considerations for health and safety.

Dissemination is facilitated by the massive deployment of low power devices that are expected to run for ten years or more on batteries. LoRa was designed for that operating environment and the LoRaWAN device market is anticipated to grow at a CAGR of 36.5% between 2021 and 2026.

Massive IoT deployments equates to massive amounts of data that could become unmanageable. This challenge has been anticipated and addressed by edge compute. Recall that this development processes and analyses IoT data at or close to the source in near real time.

ML and AI solutions analyse massive amounts of IoT information and use it to generate insightful intelligence that helps unlock the full potential of IoT. They enable networks and devices to learn from past decisions, predict future activity, and continuously improve performance and decision-making capabilities.



Sponsors Deploying Mass IoT

How our sponsors are addressing the challenges of mass IoT. Short profiles of our research sponsors and their offerings in the IoT market. For more detail, please contact them direct.

WEBSITE



Eseye empowers businesses to embrace IoT without limits. We help them to visualise the impossible and bring those solutions to life through innovative IoT cellular connectivity solutions that enable our customers to drive up business value, deploy differentiated experiences and disrupt their markets.

Our pioneering IoT cellular connectivity solutions, versatile hardware, technical consultancy and round-the-clock support allows businesses to overcome the complexity of IoT device design, development and deployment. We guide them every step of the way, so they can move forward with IoT projects without the fear of getting it wrong.

Our next-generation eUICC+ connectivity enables enterprises to unlock the potential of global IoT, without limits. The AnyNet+ eUICC SIM with unique

multi-IMSI technology offers ubiquitous global connectivity and makes it possible for devices to achieve over 99.8% connectivity uptime wherever they are in the world.

Supported by our unique AnyNet Secure® SIM technology, Infinity Platform and a powerful partner ecosystem, we help more than 2,000 customers to seamlessly connect millions of devices across 190 countries, agnostic to over 700 available global networks.

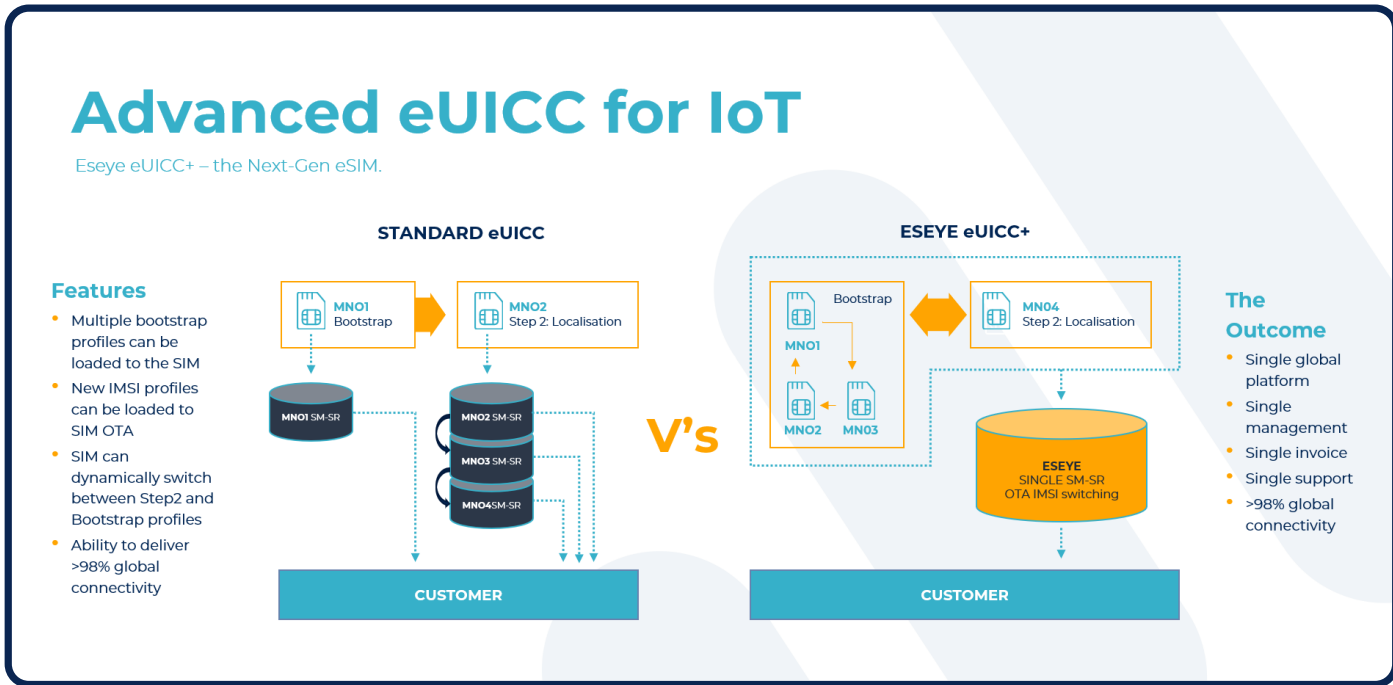


Figure: Standard eUICC approach (left side), is what most MVNOs and IoT solutions providers have adopted. Although a new profile can be loaded into the Step 2 profile to change the network, you can't fall back to the bootstrap. This can cause issues with devices getting 'stuck' without connectivity options.

With Eseye we have developed an advanced implementation of eUICC. We have the 3 bootstraps IMSI's and we can push new profiles Over the Air (OTA) into the Step 2 profile. This provides 1 SKU that can be deployed globally and be localized with a fallback of over 700 mobile networks for near 100% reliable connectivity.

Find out more at www.eseye.com

[WEBSITE](#)

Infinity: from device to cloud

Simple global connectivity

The Infinity platform enables large enterprises and SMEs to utilize Eseye's eSIMs to power their global IoT deployments, while offering ultimate flexibility and control of commercial arrangements. You can customize your carriers, choosing multiple MNOs to build the right mix for your needs and get the best coverage in each location. The system's SDN makes it easy to onboard new operators.

The AnyNet+ SIM can be loaded with multiple network user profiles, which allows the device to switch dynamically to another cellular network on any loss of connectivity. Infinity allows cellular IoT devices to intelligently switch to any one of over 700 GSMA-compliant carriers to maximize device uptime.

5 key components – all powered by the Infinity IoT Platform™

1. Device Management: provision and manage device connectivity

This is an essential database of information about each device's capabilities and connectivity requirements. Working hand in hand with other Infinity components, it supplies the information they need to manage functions and processes such as subscriptions, network optimization and security.

Infinity makes it easier to provision xSIMs, firmware and bootstraps, manage security keys, and trigger automatic recovery processes. All of this can be done over the air, while ensuring all data and processes remain protected and compliant.

2. Connectivity and Network Optimization: optimize network access and routing

This component enables managers to ensure secure, reliable, and low-latency communications from device to cloud.

Network connectivity processes and rules can be set within the IMSI on the xSIM – e.g., available networks, permission to access networks, strength of signal, rate plans and security. This enables all devices to connect easily and automatically to pre-set network choices and receive the right

amount of bandwidth and network speed for optimal functioning.

Should connectivity fail, the SIM will trigger the device to search and connect to the next most preferred network provider.

If connectivity or network rules change, these can be updated over the air, with no need to visit the device physically, keeping running costs low.

[WEBSITE](#)

3. Security and Policy: manage protection from the device to the cloud

The Infinity platform enables you to ensure the confidentiality, integrity, availability, and authenticity of devices – including the environment where the xSIMs reside, and any application keys – while minimizing the risk of unwarranted connectivity rejections.

Data sovereignty rules can be applied to direct and store processed

data in the right geographically based clouds to ensure compliance with regulations, such as GDPR.

Infinity's security component can be configured for role-based access, authorizing users to access only the areas they need. Integration with reporting and analytics allows you to easily identify and address abnormal patterns of device communication behaviour.

4. Subscription and Service Management: manage all network operator subscriptions, service plans and campaigns assigned to a device

Infinity Subscription and Service Management (ISSM) tracks all technologies and protocols supported (e.g., LTE, NB-IoT, CAT-M) by service provider and related portfolios, packages, and contracts, including pricing. It provides usage, billing, and call information so you know exactly how much you're spending and where, and will alert you if this exceeds the set thresholds.

From a service management perspective, Infinity enables order management, services provisioning, trouble management and service level agreement reporting such as device availability.

5. Reporting, Analytics & AI: manage and optimize performance

This component includes a set of pre-canned reports and visualization tools for:

- Connectivity and network optimization
- Security and policy
- Subscription management

Real-time data feeds are provided for thresholding, alerting and usage, pricing, availability, performance, and SLA failings. Enabled by Eseye's APIs and data lake, data from the Infinity platform can be analyzed, configured by us or our partners, and added to your own reports and applications. Infinity makes use of AI technology to predict and rectify issues and optimize connectivity.



WEBSITE

Expanding global connectivity and enabling beneficial change through the delivery of Massive IoT

Everynet operates the largest, neutral-host, Low Power Wide Area (LPWA) national networks in the world. We build and maintain carrier-grade networks – offering fully managed, ultra-low-cost connectivity as a service to large and small enterprises alike – enabling the delivery of Massive IoT globally.

Our networks are built on LoRaWAN technology, the globally accepted specification within LPWA networking protocols. Everynet networks are open, highly resilient and entirely server agnostic – increasing speed to market and revenue. And with zero CapEx, we help our partners scale

and achieve profitability on day one. It's this fast, simple network access that helps to expand connectivity worldwide – enabling enterprise users to reduce waste and increase efficiency through proactive monitoring and maintenance.

At Everynet, we focus on three key pillars for success:

Network Resiliency

Our networks are highly resilient, designed from the start to withstand the harshest conditions.

- Carrier-grade networks deployed on the world's leading tower infrastructures
- Managed dual carrier backhaul dynamic failover
- Network power surge protection proven against lighting strikes and hurricane-force winds
- Network RF coverage tools ensure connectivity at the device level
- E2E security and encryption
- Global 24/7/365 NOC operating in seven languages

Ultra-Low-Cost, Flexible Model

Our open, server agnostic, LoRaWAN-based network offers a range of benefits, including:

- Access to Everynet's massive markets, without building your own network
- Flexible LNS allows you to bring your own LNS and connect to Everynet RAN via API
- Disruptive business model gives you customer/end user ownership
- Low power, long range connectivity – above and below ground
- Long device battery life – lasting up to 10 years

Go To Market Support

We partner with our wholesale and ecosystem partners to ensure their success from the start.

- Wholesale Partners
 - GTM programs leveraging global best practices, tools and onboarding
 - Marketing, messaging and use case development
 - Accelerated revenue generation
- Ecosystem Partners
 - Access to LoRaWAN open ecosystem, global and local solution providers
 - E-Thingz Certification Program
- Customer Success
 - LoRaWAN technical support, API tools and onboarding



WEBSITE

Global access. Practical applications.

We play an active role in enabling the creation of Smart Infrastructure globally, currently operating LoRaWAN networks in 10 countries with roaming in 25 more. We have a curated ecosystem of partners within the infrastructure and telecommunications sectors, including partnerships with American Tower Corporation, Crown Castle, Telkom Indonesia, Cellnex, and Lysir. Through these partnerships, we provide access to more than 100,000 towers worldwide – and we continue to grow.

Leveraging these partnerships we have established ourselves as the LoRaWAN public network operator in Brazil, Indonesia, Ireland, Italy, Spain, the United Kingdom and the United States/Puerto Rico; as well as Andorra and Iceland. Thanks to large projects in the fields of gas, water and energy utilities we have developed a network design expertise capable of overcoming the inherent challenges within the water management and utility sectors.

Technology focused on beneficial change

By simplifying the adoption of Massive IoT, Everynet brings together ecosystem partners and enterprise users to cost-effectively deploy, manage and scale LPWAN solutions to solve the world's most critical problems.

Everynet partners with the entire LoRaWAN ecosystem. Since our inception, we have developed a comprehensive portfolio of device manufacturers and application providers, each of whom have been certified to meet our operational standards and with whom we collaborate both locally and globally to deliver end-user solutions.

Putting our global experience into practice, we have built highly resilient networks that are capable of withstanding environmental challenges like extreme temperatures, high humidity, torrential rains and power loss. All parameters are managed by our global NOC, ensuring network availability for our customers and partners.

It's this combined focus on technology and network resiliency that enable Everynet national networks to deliver Massive IoT globally – providing the real-time data connectivity necessary to manage critical issues such as air quality, energy monitoring and water management, that face our world today.

[Learn more at www.everynet.com.](http://www.everynet.com)





WEBSITE

Iridium IoT Products and Services

Iridium is a global satellite communications company, providing access to voice and data services anywhere on Earth. With its constellation of satellites, Iridium's network connects people and devices in the world's most remote places – and close to home.

Our Network

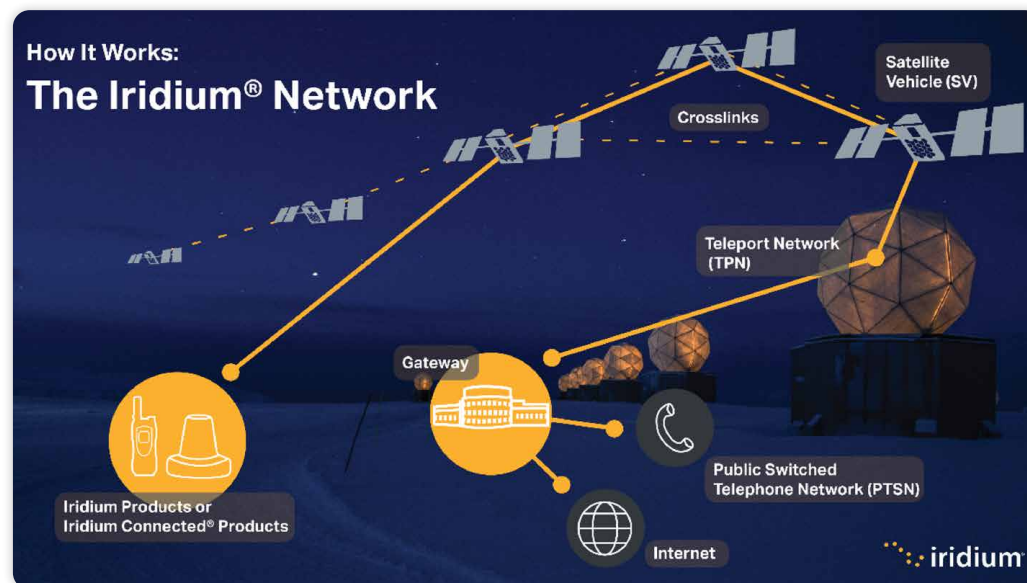
Iridium's unique constellation architecture makes it the only network that covers 100% of the planet. Satellites are cross-linked to provide reliable, low-latency, weather-resilient connections that enable communication anywhere in the world.

The satellites of the Iridium® network cover the entire earth with connectivity unmatched by any other communications provider. The first Iridium satellite was deployed in 1997 and the network was fully operational in 1998. In 2019, Iridium completed an upgrade to the Iridium constellation, replacing all satellites without ever disrupting service. The constellation includes 75 satellites – 6 active in each plane of 11 planes with 9 spares. The spares can be moved into any of the planes to replace any of the active satellites as needed and can be hot-swapped.

Other networks use geostationary orbit (GEO) at about 35,000 kilometers (22,000 miles) from the planet. The Iridium constellation is in Low-Earth Orbit (LEO), approximately 780 kilometers (485 miles) above earth, providing stronger signals and faster connections through smaller antennas with lower power requirements. Additionally, the unique structure of Iridium's Low-Earth Orbit allows satellites to converge at the poles, ensuring coverage in the remote high-latitude regions where no other satellite provider has coverage.

Iridium's LEO network uses L-Band frequencies to communicate with the users. These frequencies are more resilient to weather than the frequencies used by most GEO networks, providing reliable communications even in adverse conditions in the air, on the sea, or on the ground.

Together, the satellites create a global mesh of coverage. In space, each satellite is cross-linked to four others, providing advantages in reliability and resiliency. These cross-links provide network optimization and redundancy, ensuring that data can be rerouted and transmitted at the fastest possible speeds no matter what happens on earth or in space. The gateway processes the message or call, then delivers it to the carrier, Internet, or customer.





WEBSITE

Onboard each satellite are systems controlled by an expert team of engineers at our Satellite Network Operations Center in Leesburg, VA, allowing them to upload new instructions or software troubleshoot anomalies, and optimize user experiences.

This also means that when the satellites eventually reach the end of their lives, Iridium engineers can carefully and safely de-boost and de-orbit each one from space, helping keep space clean and sustain it for future missions. Beyond maintenance, the Iridium network is overseen by an international team of experts in state-of-the-art facilities around the world.

This team provides 24/7 monitoring of the network, processes voice and data traffic, conducts systems integration testing, develops software upgrades for new technologies, and supports the network of terminals that communicate to and from the satellites.

On the ground, our network connects thousands of devices across the world from both Iridium and our partners. These industry leading companies leverage our unique network and technologies to manufacture, develop, and market Iridium Connected® devices to solve problems, maintain critical lifelines, and keep people connected.

Iridium IoT Services

Iridium Short Burst Data® (SBD®): Real-time, two-way messaging anywhere in the world. SBD is a simple, efficient packet-based service for frequent short data transmissions between equipment and centralized host computer systems.

Iridium Circuit Switched Data (CSD): CSD is an asynchronous, circuit-switched, 2400bps, bi-directional service that allows for dial-up services. It can be used for larger amounts of data, including files of dozens or hundreds of megabytes.

Iridium CloudConnect: This important Iridium IoT service is explored in Section 4 of this report

Iridium® Network Resilience

Iridium satellites are resilient to blockage, regardless of weather or terrain.

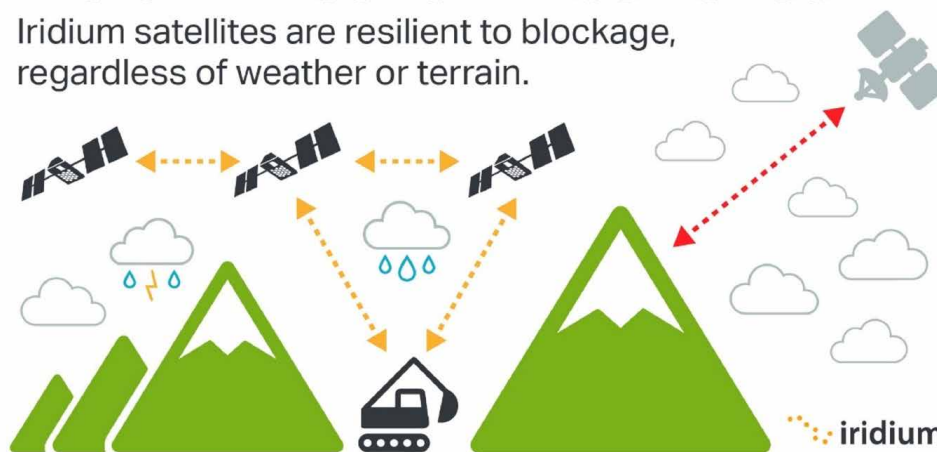


Figure. Advantages of Iridium LEO constellation vs GEO satellites

Iridium IoT Products

Using these services in L-band, Iridium has built a range of transceivers, chipsets and finished goods to make it easy for partners to integrate Iridium connectivity into their products. The main benefits these devices offer are:

- Form factor designed for board-on-board integration
- Small size
- Low latency
- Lower power consumption
- Low cost



WEBSITE

The current main Iridium devices are the Iridium 9602 and Iridium 9603 modems (measuring 41×45×13 mm and 31.5×29.6×8.1 mm respectively) which offer 2.4 kbps data speeds anywhere. These are most often used for applications like Personnel & Asset Tracking, Fleet Management, Environment & Safety Monitoring and Remote Automation & Control.

Antennas for these are very small and low cost – typically 25-35mm ceramic patch antennas which can easily be embedded into partner products alongside the Iridium hardware devices.

A new mid-band transceiver product – the Iridium Certus™ 9770 module – has recently been introduced to offer partners the same flexibility and ease of integration as the Iridium 9602 and Iridium 9603 modems but with a data rate of 88 kbps – 36 times higher. This is then suitable for applications like Fleet & Vessel Management, Lone Worker Communications, SCADA, and Remote Monitoring for high intensity operations.

This uses a new messaging service – Iridium Messaging TransportSM (IMTSM)

To these have been added a range of finished products that include the transceivers as above, plus antennas and power – Iridium's Edge® family of standalone terminals, designed specifically for IoT. These include the Iridium Edge, the Iridium Edge Pro and the Iridium Edge Solar. They are designed to work with Iridium's SBD and CloudConnect. The Iridium Edge Solar can also work with Iridium's Circuit Switched Data -- CSD -- service.

The Iridium Edge terminal can be added on to an existing IoT solution and works with Iridium's SBD and CloudConnect.

The Iridium Edge Pro is an intelligent, programmable stand-alone terminal with digital and analog I/O ports, Integrated GPS, an accelerometer, and temperature Sensors. A development kit and an online development platform with Java programming libraries are available.

The Iridium Edge Solar is a solar powered terminal that enables two-way communications with over-the-air configuration. It includes a Self-Charging Solar-Powered Battery with Lifespan up to 10 Years and Bluetooth capability for wireless sensor integration and local device connectivity.

Additional points

These products are all half-duplex, so that transmission either way is available.

This means that, should customers require it, Over-the-Air (OTA) update of remote product firmware is available.

Regarding security, customers may wish to do their own encryption. In addition, the Iridium network is Low Probability Intercept Low Probability Detect (LPILPD). SBD bursts are very short and difficult to detect. They are also straight up/straight down so cannot be easily intercepted. Iridium has long experience of military use of its satellite equipment and therefore is highly conscious of potential cyber security threats.

More information is available at <https://www.iridium.com>



psacertified™

WEBSITE

As connected technologies deploy in a multitude of industries, IoT security has never been more important. We must be able to trust devices and the data they generate in order to build people’s confidence in them and unlock new opportunities. However, a recent report revealed the number of attacks on IoT devices

has risen by 600%. That means we must do more to ensure products are not putting customers, citizens, critical infrastructure and assets at risk. PSA Certified was founded with mission to democratize security in the IoT, a global partnership, maintained by 9 security experts (Applus+ Laboratories, Arm, CAICT, ECSEC,

Riscure, SGS Brightsight, provenrun, TrustCB and UL). The founders created a comprehensive framework and independent, multi-level certification program that helps you overcome security challenges, quickly and cost-effectively.

Low cost with Minimum Risk

PSA Certified lowers business risk and the cost of security with a comprehensive framework and simple certification program.

Fast Alignment with Legislation and Standards

PSA Certified gives you access to global markets, because it aligns with major industry and government standards and IoT legislation.

Methodically Created and Independently Tested

The certification program was created methodically by industry-leading experts. Independent and unbiased assessment creates a comprehensive scheme.



WEBSITE



psacertified™

PSA Certified guides you through a step-by-step framework which helps you build security into a device in four easy steps:

ANALYZE

Threat models & security analyses

1. Analyze: understand the threats to your device and identify mitigations

ARCHITECT

Hardware & firmware architect specifications

2. Architect: identify the components that provide the right level of security for your product

IMPLEMENT

Firmware source code

3. Implement: bring together your system of trusted components and firmware

CERTIFY

Independently tested

4. Certify: evaluate your security and certify your device through third-party laboratory testing

The scheme is made possible by key research and fundamental principles including:

- PSA Certified 10 Security Goals that outline the security requirements that should be implemented in every connected device.

- The hardware-based Root of Trust (RoT), built into the silicon that provides a set of implicitly trusted functions the rest of the system can rely on.

The scheme has multiple levels to enable you to check your security implementation at varying levels of robustness from best practice, to software attacks and hardware attacks.

- PSA Certified is backed by over 50 leading companies who are all committed to raising the bar of security and giving the ecosystem the confidence to create. Join the fastest-growing security ecosystem and start your security journey at www.psacertified.org.



psacertified™

WEBSITE

**Case study: The first silicon certified to protect devices from complex hardware and software attacks**

Leading silicon, software, and solutions company, Silicon Labs, is strengthening its approach to security to protect its customers from the increasingly sophisticated attacks on Internet of Things (IoT) devices. It has become the first company in the world to be awarded PSA Certified Level 3 status, which it received for its implementation of Secure Vault™ technology. Silicon Labs say that their award-winning suite of state-of-the-art security features helps to protect connected products against remote scalable software attacks and attempts to compromise the hardware. In turn, that reduces the risk to the device makers, consumers, organizations, and industries that are relying on its technology.

“The continued growth of the IoT depends on trusting that devices are authentic and secure when they join ecosystems,” said Matt Johnson, President, Silicon Labs, in a media release that announced its most recent achievement. “Security certifications like PSA Certified Level 3 give IoT device makers and end users the assurances they need to know their IoT applications are protecting their secret identities used for authentication and prevent counterfeit or rogue devices from entering their supply chain, which can cause irreparable harm to brands and revenue.”

At the heart of Silicon Labs’ approach is an immutable hardware Root of Trust (RoT), which provides a foundation of security that device makers can build on. That means you do not have to be a security expert to build robust security into your device.

**Case study: Making security for Linux-based devices quicker and easier throughout the lifecycle**

Securing a Linux-based device can be challenging and time-consuming, which is why Foundries.io set out to make the task quicker and easier. Its cloud infrastructure service, FoundriesFactory, builds security into the device software from the outset. That means original equipment manufacturers (OEMs) can utilize it and adapt it to their own use case knowing they are not increasing their customers’ risk of cyberattack.

The company has achieved PSA Certified Level 1 certification to show that its platform has been developed in line with security best practices. That includes assessing the threats to the device, using threat modeling and security analysis; and addressing the PSA Certified 10 Security Goals - in particular, ensuring devices can be monitored and updated securely throughout their lifecycle.

Enabling secure over-the-air updates is critical to the longer-term security of the device, as George Grey, CEO, Foundries.io explains: “At Foundries.io we believe the most up-to-date software is the most secure. The PSA Certified Level 1 awarded to FoundriesFactory is the first given to a Linux-based solution and validates that we are working with the best-in-class approaches to security. Our customers continue to focus on their own business value-add in the knowledge that the security of their shipped devices is maintainable via FoundriesFactory.”

PSA Certified Level 1 certification also helps Foundries.io assure its customers the platform they are building on aligns with the latest baseline cybersecurity requirements and regulations, including EN 303 645, NIST 8259A, and Californian State Law SB-327.

[WEBSITE](#)

Simplify the Connected World

We live in a connected world. The connection of people, technology and processes creates the connected experiences that are expected by your employees, partners and customers. To deliver those experiences, you need a truly connected enterprise that turns your data into value through deeper analysis and insights that lead to new business models.

But the digital transformation required to meet those expectations is increasingly complex and more difficult to navigate with constantly changing needs. A misstep today can have a lasting impact on your ability to compete in the future.

Software AG can empower you to make smarter decisions faster to create experiences your customers, partners and employees expect so you can compete in this world of fast, always-evolving change.

We can help simplify the truly connected enterprise where systems integrate more seamlessly, technology connects more effectively, and processes run effortlessly enabling information and insights to flow more freely. But no two enterprises are alike; no two solutions identical. We have award-winning technology and expertise to be your partner. We will listen and understand your challenges and work side by side with you, anticipating the next challenge, to meet and exceed expected customer experiences so you can win against your competition.

With the digital backbone that simplifies the integration of applications, devices, data and clouds; empowers streamlined processes; and connects “things” like sensors, machines and robots, we provide the fundamental, structural support needed to enable digital transformation. Through this connection, communication, and collaboration, you can turn your data into value to grow, transform and compete.

Together, we can simplify the connected world by connecting people and technology for a smarter tomorrow.

Software AG's IoT offer

Cumulocity IoT is the #1 self-service, low-code IoT platform that enables businesses to build IoT solutions at low cost that can deliver value in as little as 90 days. Cumulocity IoT is an open platform that works with any device, Infrastructure as a Service or network (including Wi-Fi, mobile and LPWAN). Companies can connect and manage any asset and analyze any amount of data automatically and in real time in the cloud, at the edge, on-premises and also for hybrid environments.

Cumulocity IoT is designed to be extensible. Software AG believes IT and operations departments can work more effectively together. To support this, Cumulocity IoT offers ease of integration of its data with enterprise IT, operational systems and business processes, with no coding or API requirements.



WEBSITE

About Cumulocity IoT | Core Capabilities

1. Device connectivity and management

Quickly connect and manage any asset with self-service IoT.

With Cumulocity IoT you can connect to everything, run anywhere and integrate with any application. Innovate on the only completely open IoT platform and free your business from the constraints of any one technology stack. With Cumulocity IoT's device and connectivity management capability you can:

- Connect without coding
- Bulk register devices
- Centralize device management
- Secure many tenants
- Run a stand-alone edge solution

2. Self-Service Analytics

Act immediately on opportunities to market, sell, improve.

Point, click and analyze your data—with Cumulocity IoT, it's that simple. Business users and operational experts can build deep analytics on their own without writing code or needing support from IT or data scientists. With Cumulocity IoT's analytics capability you can:

- Analyze and act on IoT data in real time
- Predict and prevent problems
- Make decisions to optimize the production line in real-time
- Access and analyze historical data
- Take intelligence to the edge

3. Integration

Easily integrate the IoT with the core apps that run your business.

Integration is key to capitalize on all the data you're pulling in from IoT-enabled devices everywhere. With Cumulocity IoT, you can easily integrate your IoT application with your enterprise apps, whether they're in the cloud or on-premises. With Cumulocity IoT's integration capability you can:

- See the whole picture
- Integrate data across the enterprise without coding
- Connect your IoT and business processes

4. Application enablement

Differentiate your business faster with the IoT.

With Cumulocity IoT you can create your differentiating logic and applications. Beat your competition to market with innovations that leverage connected things and deliver your products as a service. Cumulocity IoT's application enablement capability is rated #1 by analysts and with it you can:

- Innovate faster
- Enrich and customize your solutions quickly
- Share innovations easily
- Bring groundbreaking new offerings to market

5. Professional services

Help at every step of your IoT journey.

Speed up your IoT journey with best practices from Software AG Professional Services. From getting your IoT project started by proving the value to providing end-to-end support, Software AG offers tailored professional services packages to ensure your IoT initiatives are a success. With Software AG's IoT professional services you can:

- DISCOVER your business motivation for IoT
- IDEATE your IoT vision from different perspectives
- PROVE the value, build a proof of concept and validate user acceptance
- GENERATE the final business model and roadmap
- IMPLEMENT the IoT project and support with mentoring and monitoring
- EXECUTE long-term support & maintenance up to Managed Services
- IMPROVE & SCALE your IoT solution

Beecham Research is a leading technology market research, analysis and consulting firm established in 1991. We have specialized in the development of the rapidly-growing Connected Devices market, often referred to as M2M and IoT, worldwide since 2001. We are internationally recognised as thought leaders in this market and have deep knowledge of the market dynamics at every level in the value chain.

Our clients include component and hardware vendors, major network/connectivity suppliers, system integrators, application developers, distributors and enterprise users in both B2B and B2C markets. We are experts in M2M/IoT services and platforms and also in IoT solution security, where we have extensive technical knowledge.



info@beechamresearch.com



beechamresearch.com



[@beechamresearch](https://twitter.com/beechamresearch)



facebook.com/BeechamResearch



linkedin.com/company/beecham-research



Shaping the IoT future